NDCBBSR_4th_gupta

Mar 28, 2023

sanjukta

Executive Summary

Issues Overview

On Mar 28, 2023, a source code review was performed over the ndcbbsrweb code base. 390 files, 2,439 LOC (Executable) were scanned and reviewed for defects that could lead to potential security vulnerabilities. A total of 206 reviewed findings were uncovered during the analysis.

Issues by Fortify Priority Order	
Low (17 Suppressed)	148
High (1 Suppressed)	34
Critical	18
Medium	6

Recommendations and Conclusions

The Issues Category section provides Fortify recommendations for addressing issues at a generic level. The recommendations for specific fixes can be extrapolated from those generic recommendations by the development group.

Project Summary

Code Base Summary

Code location: D:/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb
Number of Files: 390
Lines of Code: 2439
Build Label: <No Build Label>

Scan Information

Scan time: 00:57
SCA Engine version: 20.2.2.0003
Machine Name: DESKTOP-P8I04US
Username running scan: sanjukta

Results Certification

Results Certification Valid

Details:

Results Signature:

SCA Analysis Results has Valid signature

Rules Signature:

There were no custom rules used in this scan

Attack Surface

Attack Surface:
Command Line Arguments:
com.example.ndcbbsrweb.NdcbbsrwebApplication.main
com.example.ndcbbsrweb.util.AesCrypto.main
com.example.ndcbbsrweb.util.AesCryptobak.main

Environment Variables:
java.lang.System.getenv

File System:
org.apache.commons.io.FileUtils.readFileToByteArray

Private Information:
null.null.null
com.example.ndcbbsrweb.util.AesCrypto.decrypt
com.example.ndcbbsrweb.util.AesCryptobak.decrypt
java.lang.System.getenv
javax.crypto.KeyGenerator.generateKey

Java Properties:
java.lang.System.getProperty

System Information:
null.null.null
null.null.resolve
com.amazonaws.services.s3.AmazonS3.putObject
java.lang.System.getProperty
java.lang.System.getProperty
java.lang.System.getProperty
java.lang.Throwable.getMessage

Filter Set Summary

Current Enabled Filter Set:
Quick View

Filter Set Details:

Folder Filters:
If [fortify priority order] contains critical Then set folder to Critical
If [fortify priority order] contains high Then set folder to High
If [fortify priority order] contains medium Then set folder to Medium
If [fortify priority order] contains low Then set folder to Low
Visibility Filters:
(Disabled) If impact is not in range [2.5, 5.0] Then hide issue
(Disabled) If likelihood is not in range (1.0, 5.0] Then hide issue

Audit Guide Summary

Audit guide not enabled

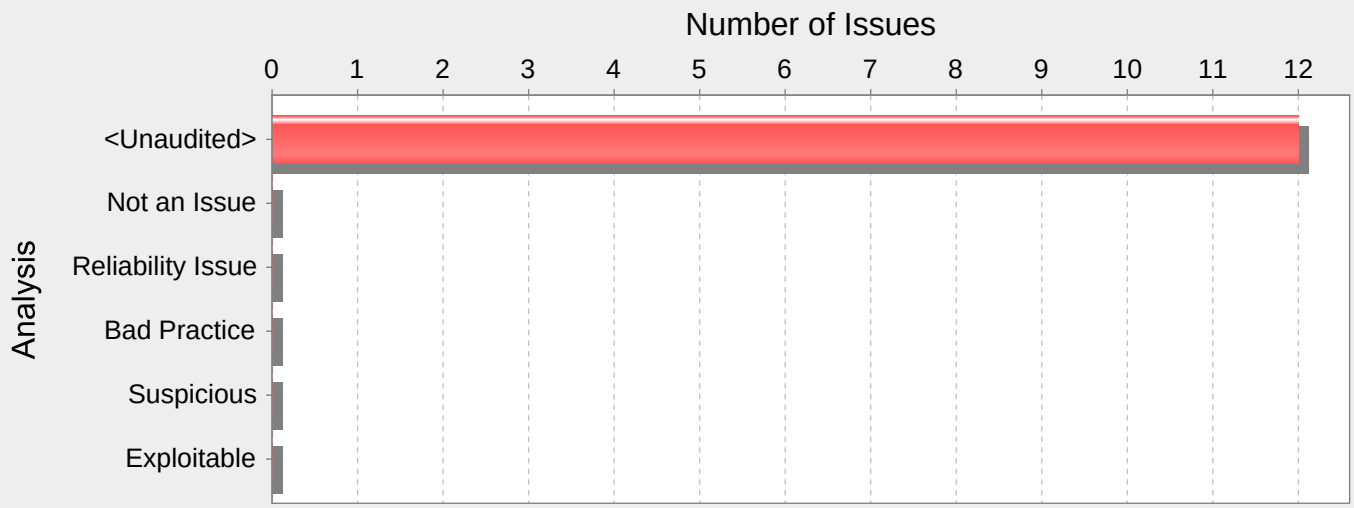
Results Outline

Overall number of results

The scan found 206 issues.

Vulnerability Examples by Category

Category: Path Manipulation (12 Issues)



Abstract:

Attackers can control the file system path argument to File() at AdminPanelController.java line 1278, which allows them to access or modify otherwise protected files.

Explanation:

Path manipulation errors occur when the following two conditions are met:

1. An attacker can specify a path used in an operation on the file system.

2. By specifying the resource, the attacker gains a capability that would not otherwise be permitted.

For example, the program might give the attacker the ability to overwrite the specified file or run with a configuration controlled by the attacker.

Example 1: The following code uses input from an HTTP request to create a file name. The programmer has not considered the possibility that an attacker could provide a file name such as "../../tomcat/conf/server.xml", which causes the application to delete one of its own configuration files.

```
String rName = request.getParameter("reportName");
File rFile = new File("/usr/local/apfr/reports/" + rName);
...
rFile.delete();
```

Example 2: The following code uses input from a configuration file to determine which file to open and echo back to the user. If the program runs with adequate privileges and malicious users can change the configuration file, they can use the program to read any file on the system that ends with the extension .txt.

```
fis = new FileInputStream(cfg.getProperty("sub")+".txt");
amt = fis.read(arr);
out.println(arr);
```

Some think that in the mobile environment, classic vulnerabilities, such as path manipulation, do not make sense -- why would the user attack themself? However, keep in mind that the essence of mobile platforms is applications that are downloaded from various sources and run alongside each other on the same device. The likelihood of running a piece of malware next to a banking application is high, which necessitates expanding the attack surface of mobile applications to include inter-process communication.

Example 3: The following code adapts Example 1 to the Android platform.

```
...
String rName = this.getIntent().getExtras().getString("reportName");
```

```
File rFile = getBaseContext().getFileStreamPath(rName);
...
rFile.delete();
...
```

Recommendations:

The best way to prevent path manipulation is with a level of indirection: create a list of legitimate values from which the user must select. With this approach, the user-provided input is never used directly to specify the resource name.

In some situations this approach is impractical because the set of legitimate resource names is too large or too hard to maintain. Programmers often resort to implementing a deny list in these situations. A deny list is used to selectively reject or escape potentially dangerous characters before using the input. However, any such list of unsafe characters is likely to be incomplete and will almost certainly become out of date. A better approach is to create a list of characters that are permitted to appear in the resource name and accept input composed exclusively of characters in the approved set.

Tips:

1. If the program performs custom input validation to your satisfaction, use the Fortify Custom Rules Editor to create a cleanse rule for the validation routine.

2. Implementation of an effective deny list is notoriously difficult. One should be skeptical if validation logic requires implementing a deny list. Consider different types of input encoding and different sets of metacharacters that might have special meaning when interpreted by different operating systems, databases, or other resources. Determine whether or not the deny list can be updated easily, correctly, and completely if these requirements ever change.

3. A number of modern web frameworks provide mechanisms to perform user input validation (including Struts and Spring MVC). To highlight the unvalidated sources of input, Fortify Secure Coding Rulepacks dynamically re-prioritize the issues Fortify Static Code Analyzer reports by lowering their probability of exploit and providing pointers to the supporting evidence whenever the framework validation mechanism is in use. We refer to this feature as Context-Sensitive Ranking. To further assist the Fortify user with the auditing process, the Fortify Software Security Research group makes available the Data Validation project template that groups the issues into folders based on the validation mechanism applied to their source of input.

AdminPanelController.java, line 1278 (Path Manipulation)

Fortify Priority:	Critical	**Folder**	Critical
Kingdom:	Input Validation and Representation		
Abstract:	Attackers can control the file system path argument to File() at AdminPanelController.java line 1278, which allows them to access or modify otherwise protected files.		

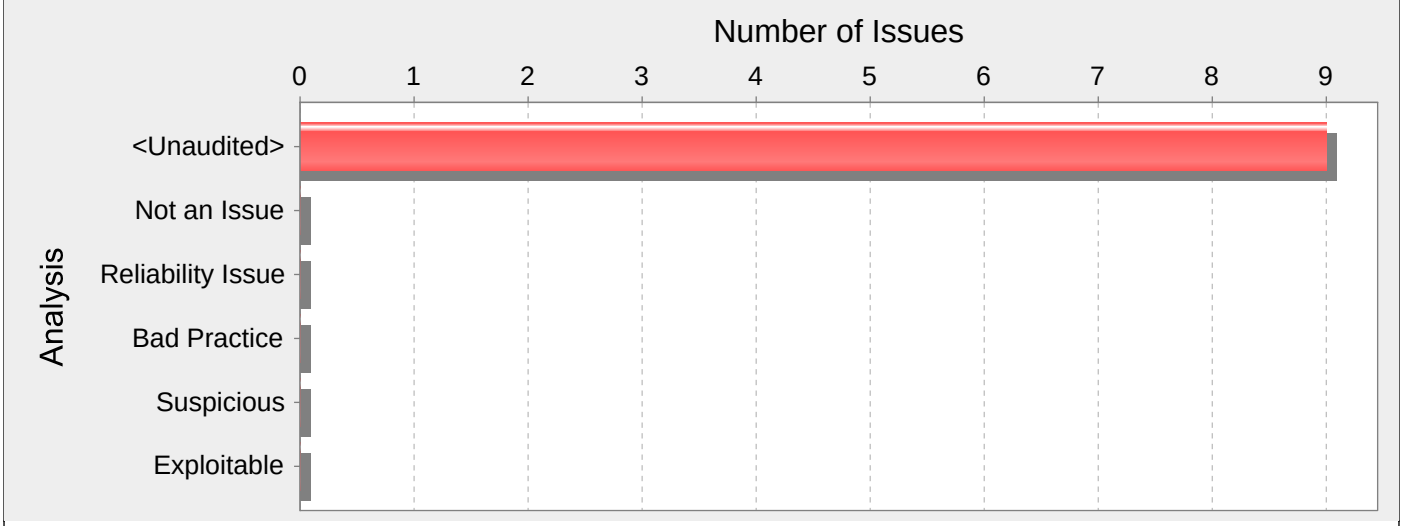
Source: AdminPanelController.java:949 saveHighlight(0)

```
947
948    @PostMapping("/saveHighlight")
949    public String saveHighlight(@RequestParam("image") MultipartFile file, boolean
       isImage, String content,
950        HttpServletRequest request) {
```

Sink: AdminPanelController.java:1278 java.io.File.File()

```
1276     Date d = new Date();
1277     String filename = d.getTime() + "." + extension;
1278     File convFile = new File(filename);
1279     FileOutputStream fos = null;
1280     try {
```

Category: Mass Assignment: Insecure Binder Configuration (9 Issues)



Abstract:

The framework binder used for binding the HTTP request parameters to the model class has not been explicitly configured to allow, or disallow certain attributes.

Explanation:

To ease development and increase productivity, most modern frameworks allow an object to be automatically instantiated and populated with the HTTP request parameters whose names match an attribute of the class to be bound. Automatic instantiation and population of objects speeds up development, but can lead to serious problems if implemented without caution. Any attribute in the bound classes, or nested classes, will be automatically bound to the HTTP request parameters. Therefore, malicious users will be able to assign a value to any attribute in bound or nested classes, even if they are not exposed to the client through web forms or API contracts.

Example 1: Using Spring MVC with no additional configuration, the following controller method will bind the HTTP request parameters to any attribute in the User or Details classes:

```
@RequestMapping(method = RequestMethod.POST)
public String registerUser(@ModelAttribute("user") User user, BindingResult result, SessionStatus status) {
if (db.save(user).hasErrors()) {
return "CustomerForm";
} else {
status.setComplete();
return "CustomerSuccess";
}
}
```

Where User class is defined as:

```
public class User {
private String name;
private String lastname;
private int age;
private Details details;
// Public Getters and Setters
...
}
```

and Details class is defined as:

```
public class Details {
private boolean is_admin;
private int id;
private Date login_date;
// Public Getters and Setters
...
```

```
}
```

Recommendations:

When using frameworks that provide automatic model binding capabilities, it is a best practice to control which attributes will be bound to the model object so that even if attackers figure out other non-exposed attributes of the model or nested classes, they will not be able to bind arbitrary values from HTTP request parameters.

Depending on the framework used there will be different ways to control the model binding process:

Spring MVC:

It is possible to control which HTTP request parameters will be used in the binding process and which ones will be ignored.

In Spring MVC applications using @ModelAttribute annotated parameters, the binder can be configured to control which attributes should be bound. In order to do so, a method can be annotated with @InitBinder so that the framework will inject a reference to the Spring Model Binder. The Spring Model Binder can be configured to control the attribute binding process with the setAllowedFields and setDisallowedFields methods. Spring MVC applications extending BaseCommandController can override the initBinder(HttpServletRequest request, ServletRequestDataBinder binder) method in order to get a reference to the Spring Model Binder.

Example 2: The Spring Model Binder (3.x) is configured to disallow the binding of sensitive attributes:

```
final String[] DISALLOWED_FIELDS = new String[]{"details.role", "details.age", "is_admin"};
@InitBinder
public void initBinder(WebDataBinder binder) {
binder.setDisallowedFields(DISALLOWED_FIELDS);
}
```

Example 3: The Spring Model Binder (2.x) is configured to disallow the binding of sensitive attributes:

```
@Override
protected void initBinder(HttpServletRequest request, ServletRequestDataBinder binder) throws Exception {
binder.setDisallowedFields(new String[]{"details.role", "details.age", "is_admin"});
}
```

In Spring MVC Applications using @RequestBody annotated parameters, the binding process is handled by HttpMessageConverter instances which will use libraries such as Jackson and JAXB to convert the HTTP request body into Java Objects. These libraries offer annotations to control which fields should be allowed or disallowed. For example, for the Jackson JSON library, the @JsonIgnore annotation can be used to prevent a field from being bound to the request.

Example 4: A controller method binds an HTTP request to an instance of the Employee class using the @RequestBody annotation.

```
@RequestMapping(value="/add/employee", method=RequestMethod.POST, consumes="text/html")
public void addEmployee(@RequestBody Employee employee){
// Do something with the employee object.
}
```

The application uses the default Jackson HttpMessageConverter to bind JSON HTTP requests to the Employee class. In order to prevent the binding of the is_admin sensitive field, use the @JsonIgnore annotation:

```
public class Employee {
@JsonIgnore
private boolean is_admin;
...
// Public Getters and Setters
...
}
```

Note: Check the following REST frameworks information for more details on how to configure Jackson and JAXB annotations.

Apache Struts:

Struts 1 and 2 will only bind HTTP request parameters to those Actions or ActionForms attributes which have an associated public setter accessor. If an attribute should not be bound to the request, its setter should be made private.

Example 5: Configure a private setter so that Struts framework will not automatically bind any HTTP request parameter:

```
private String role;
```

```
private void setRole(String role)  {
this.role = role;
}
```

REST frameworks:

Most REST frameworks will automatically bind any HTTP request bodies with content type JSON or XML to a model object. Depending on the libraries used for JSON and XML processing, there will be different ways of controlling the binding process. The following are some examples for JAXB (XML) and Jackson (JSON):

Example 6: Models bound from XML documents using Oracle's JAXB library can control the binding process using different annotations such as @XmlAccessorType, @XmlAttribute, @XmlElement and @XmlTransient. The binder can be told not to bind any attributes by default, by annotating the models using the @XmlAccessorType annotation with the value XmlAccessType.NONE and then selecting which fields should be bound using @XmlAttribute and @XmlElement annotations:

```
@XmlRootElement
@XmlAccessorType(XmlAccessType.NONE)
public class User {
private String role;
private String name;
@XmlAttribute
public String getName() {
return name;
}
public void setName(String name) {
this.name = name;
}
public String getRole() {
return role;
}
public void setRole(String role) {
this.role = role;
}
```

Example 7: Models bound from JSON documents using the Jackson library can control the binding process using different annotations such as @JsonIgnore, @JsonIgnoreProperties, @JsonIgnoreType and @JsonInclude. The binder can be told to ignore certain attributes by annotating them with @JsonIgnore annotation:

```
public class User {
@JsonIgnore
private String role;
private String name;
public String getName() {
return name;
}
public void setName(String name) {
this.name = name;
}
public String getRole() {
return role;
}
public void setRole(String role) {
this.role = role;
}
```

A different approach to protecting against mass assignment vulnerabilities is using a layered architecture where the HTTP request parameters are bound to DTO objects. The DTO objects are only used for that purpose, exposing only those attributes defined in the web forms or API contracts, and then mapping these DTO objects to Domain Objects where the rest of the private attributes can be defined.

Tips:

1. This vulnerability category can be classified as a design flaw since accurately finding these issues requires understanding of the application architecture which is beyond the capabilities of static analysis. Therefore, it is possible that if the application is designed to use specific DTO objects for HTTP request binding, there will not be any need to configure the binder to exclude any attributes.

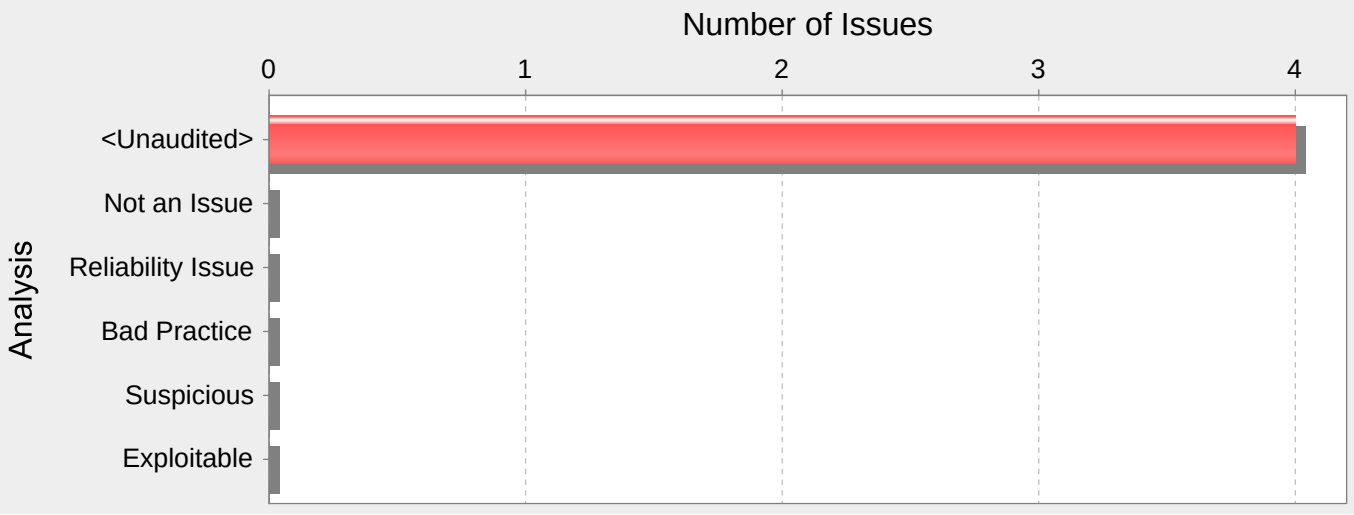
AdminPanelController.java, line 374 (Mass Assignment: Insecure Binder Configuration)

Fortify Priority:	High	**Folder**	High
Kingdom:	API Abuse		
Abstract:	The framework binder used for binding the HTTP request parameters to the model class has not been explicitly configured to allow, or disallow certain attributes.		

Sink: AdminPanelController.java:374 Function: saveTeam()

```
372
373  @PostMapping("/saveTeam")
374  public String saveTeam(@ModelAttribute("team") teamModal team) {
375
376   if (PriviledgeCheckAdmin() == false) {
```

Category: Cookie Security: Overly Broad Domain (4 Issues)



Abstract:

A cookie with an overly broad domain opens an application to attack through other applications.

Explanation:

Developers often set cookies to be active across a base domain such as ".example.com". This exposes the cookie to all web applications on the base domain and any sub-domains. Because cookies often carry sensitive information such as session identifiers, sharing cookies across applications can cause a vulnerability in one application to compromise another application.

Example 1:

Imagine you have a secure application deployed at http://secure.example.com/ and the application sets a session ID cookie with domain ".example.com" when a user logs in.

For example:

Cookie cookie = new Cookie("sessionID", sessionID);
cookie.setDomain(".example.com");

Suppose you have another, less secure, application at http://insecure.example.com/, and it contains a cross-site scripting vulnerability. Any user authenticated to http://secure.example.com that browses to http://insecure.example.com risks exposing their session cookie from http://secure.example.com.

In addition to reading a cookie, it might be possible for attackers to perform a Cookie Poisoning attack by using insecure.example.com to create its own overly broad cookie that overwrites the cookie from secure.example.com.

Recommendations:

Set cookie domains to be as restrictive as possible.

Example 2: The following code shows how to set the cookie domain to "secure.example.com" for the example in the Explanation section.

Cookie cookie = new Cookie("sessionID", sessionID);
cookie.setDomain("secure.example.com");

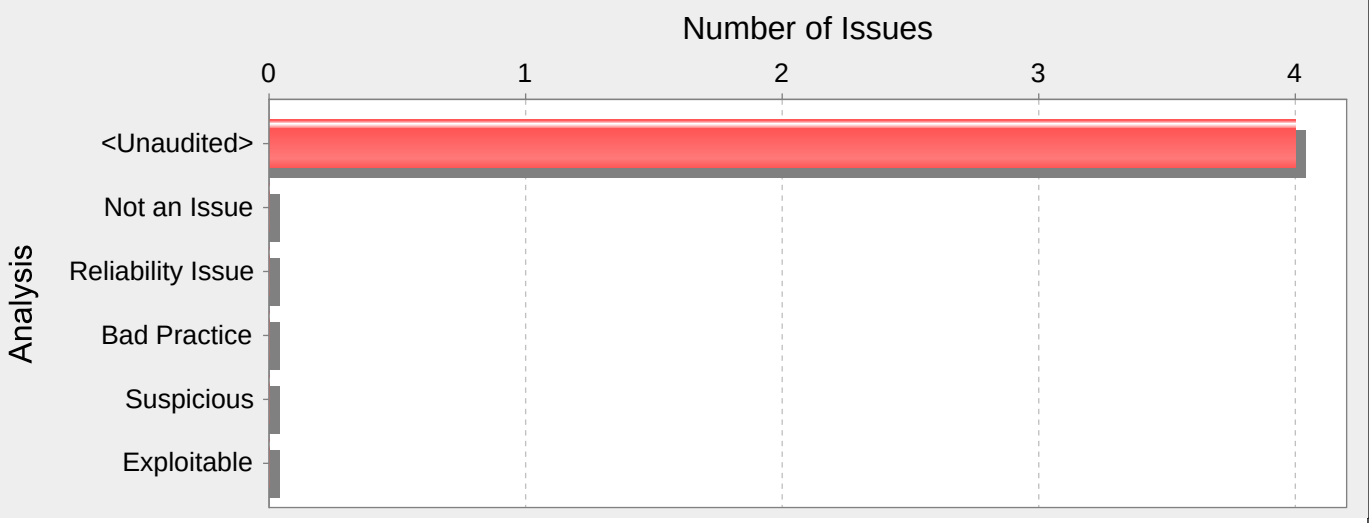
AdminPanelController.java, line 256 (Cookie Security: Overly Broad Domain)

Fortify Priority:	High	**Folder**	High
Kingdom:	Security Features		
Abstract:	A cookie with an overly broad domain opens an application to attack through other applications.		

Sink: AdminPanelController.java:256 setDomain()

```
254
255                 cookie1.setPath("/");
256                 cookie1.setDomain("ndcbbsr.nic.in");
257
258                 cookie2.setPath("/");
```

Category: Cookie Security: Overly Broad Path (4 Issues)



Abstract:

A cookie with an overly broad path can be accessed through other applications on the same domain.

Explanation:

Developers often set cookies to be accessible from the root context path ("/"). This exposes the cookie to all web applications on the domain. Because cookies often carry sensitive information such as session identifiers, sharing cookies across applications can cause a vulnerability in one application to compromise another application.

Example 1:

Imagine you have a forum application deployed at http://communitypages.example.com/MyForum and the application sets a session ID cookie with path "/" when users log in to the forum.

For example:

```
Cookie cookie = new Cookie("sessionID", sessionID);
cookie.setPath("/");
```

Suppose an attacker creates another application at http://communitypages.example.com/EvilSite and posts a link to this site on the forum. When a user of the forum clicks this link, the browser will send the cookie set by /MyForum to the application running at /EvilSite. By stealing the session ID, the attacker can compromise the account of any forum user that browsed to /EvilSite.

In addition to reading a cookie, it might be possible for attackers to perform a Cookie Poisoning attack by using /EvilSite to create its own overly broad cookie that overwrites the cookie from /MyForum.

Recommendations:

Make sure to set cookie paths to be as restrictive as possible.

Example 2: The following code shows how to set the cookie path to "/MyForum" for the example in the Explanation section.

```
Cookie cookie = new Cookie("sessionID", sessionID);
cookie.setPath("/MyForum");
```

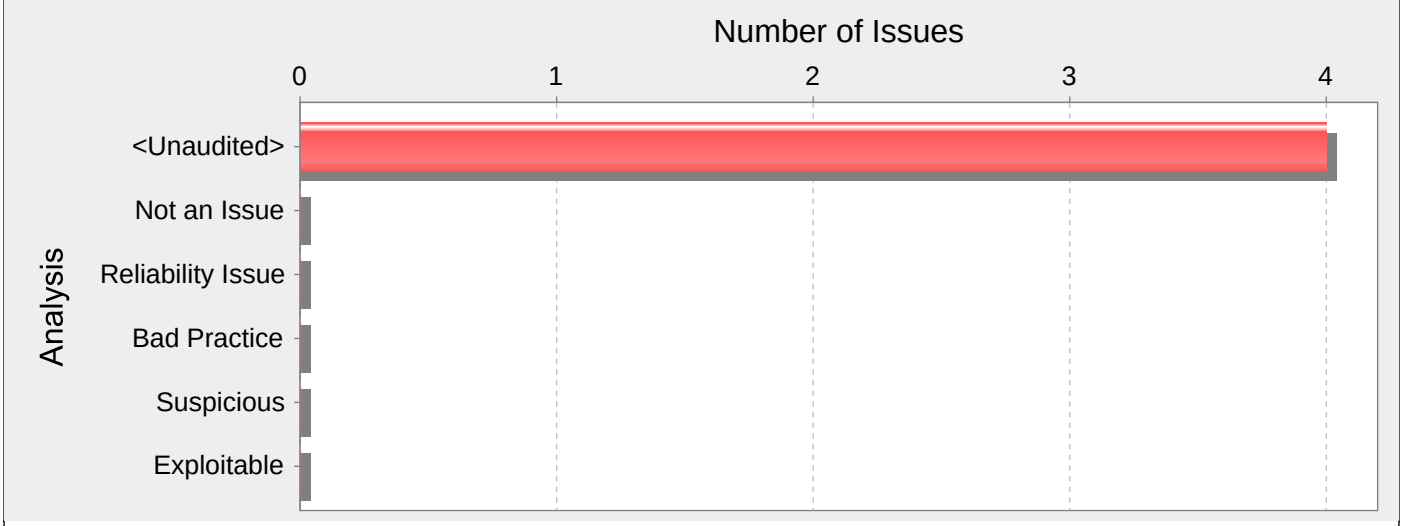
AdminPanelController.java, line 255 (Cookie Security: Overly Broad Path)

Fortify Priority:	High	**Folder**	High
Kingdom:	Security Features		
Abstract:	A cookie with an overly broad path can be accessed through other applications on the same domain.		

Sink: AdminPanelController.java:255 setPath()

```
253                 StandardCharsets.UTF_8));
254
255             cookie1.setPath("/");
256             cookie1.setDomain("ndcbbsr.nic.in");
```

Category: Open Redirect (4 Issues)



Abstract:

The file AdminPanelController.java passes unvalidated data to an HTTP redirect function on line 1412. Allowing unvalidated input to control the URL used in a redirect can aid phishing attacks.

Explanation:

Redirects allow web applications to direct users to different pages within the same application or to external sites. Applications utilize redirects to aid in site navigation and, in some cases, to track how users exit the site. Open redirect vulnerabilities occur when a web application redirects clients to any arbitrary URL that can be controlled by an attacker.

Attackers may utilize open redirects to trick users into visiting a URL to a trusted site and redirecting them to a malicious site. By encoding the URL, an attacker is able to make it more difficult for end-users to notice the malicious destination of the redirect, even when it is passed as a URL parameter to the trusted site. Open redirects are often abused as part of phishing scams to harvest sensitive end-user data.

Example 1: The following JSP code instructs the user's browser to open a URL parsed from the dest request parameter when a user clicks the link.

```
<%
...
String strDest = request.getParameter("dest");
pageContext.forward(strDest);
...
%>
```

If a victim received an email instructing them to follow a link to "http://trusted.example.com/ecommerce/redirect.asp?dest=www.wilyhacker.com", the user would likely click on the link believing they would be transferred to the trusted site. However, when the victim clicks the link, the code in Example 1 will redirect the browser to "http://www.wilyhacker.com".

Many users have been educated to always inspect URLs they receive in emails to make sure the link specifies a trusted site they know. However, if the attacker Hex encoded the destination url as follows:

"http://trusted.example.com/ecommerce/redirect.asp?dest=%77%69%6C%79%68%61%63%6B%65%72%2E%63%6F%6D"

then even a savvy end-user may be fooled into following the link.

Recommendations:

Unvalidated user input should not be allowed to control the destination URL in a redirect. Instead, use a level of indirection: create a list of legitimate URLs that users are allowed to specify and only allow users to select from the list. With this approach, input provided by users is never used directly to specify a URL for redirects.

Example 2: The following code references an array populated with valid URLs. The link the user clicks passes in the array index that corresponds to the desired URL.

```
<%
...
try {
int strDest = Integer.parseInt(request.getParameter("dest"));
if((strDest >= 0) && (strDest <= strURLArray.length -1 ))
{
```

```
strFinalURL = strURLArray[strDest];
pageContext.forward(strFinalURL);
}
}
catch (NumberFormatException nfe) {
// Handle exception
...
}
...
%>
```

In some situations this approach is impractical because the set of legitimate URLs is too large or too hard to keep track of. In such cases, use a similar approach to restrict the domains that users can be redirected to, which can at least prevent attackers from sending users to malicious external sites.

Tips:

1. A number of modern web frameworks provide mechanisms to perform user input validation (including Struts and Spring MVC). To highlight the unvalidated sources of input, Fortify Secure Coding Rulepacks dynamically re-prioritize the issues Fortify Static Code Analyzer reports by lowering their probability of exploit and providing pointers to the supporting evidence whenever the framework validation mechanism is in use. We refer to this feature as Context-Sensitive Ranking. To further assist the Fortify user with the auditing process, the Fortify Software Security Research group makes available the Data Validation project template that groups the issues into folders based on the validation mechanism applied to their source of input.

2. Fortify AppDefender adds protection against this category.

AdminPanelController.java, line 1412 (Open Redirect)

Fortify Priority:	Critical	**Folder**	Critical
Kingdom:	Input Validation and Representation		
Abstract:	The file AdminPanelController.java passes unvalidated data to an HTTP redirect function on line 1412. Allowing unvalidated input to control the URL used in a redirect can aid phishing attacks.		

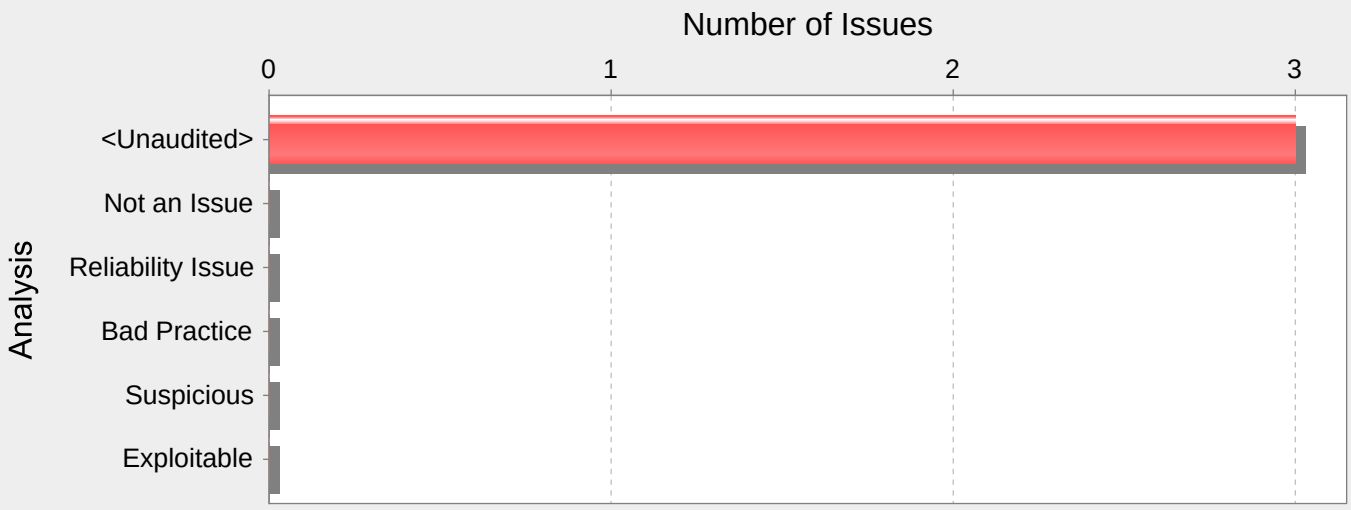
Source: NdcServiceImpl.java:357 com.example.ndcbbsrweb.dao.PortalRepository.findByshortname()

```
355  @Override
356  public Portal findPortal(String url) {
357   return portals.findByshortname(url);
358  }
359
```

Sink: AdminPanelController.java:1412 Return()

```
1410     if (portal.getShort_name().equals(target) &&
portal.getPortal_url().contains(".ndcbbsr.nic.in")) {
1411      if (urlValidator.isValid(portal.getPortal_url())) {
1412       return "redirect:" + portal.getPortal_url() + "?mode=parichay";
1413      }else {
1414       return "redirect:/error?errcode=1006";
```

Category: Cookie Security: Overly Broad Session Cookie Domain (3 Issues)



Abstract:

A session cookie with an overly broad domain can be accessed by applications sharing the same base domain.

Explanation:

Developers often set session cookies to be a base domain such as ".example.com". However, doing so exposes the session cookie to all web applications on the base domain name and any sub-domains. Leaking session cookies can lead to account compromises.

Example 1: Imagine you have a secure application deployed at http://secure.example.com/ and the application sets a session cookie with domain ".example.com" when users log in.

The application's configuration file would have the following entry:

server.servlet.session.cookie.domain=.example.com

Suppose you have another less secure application at http://insecure.example.com/ and it contains a cross-site scripting vulnerability. Any user authenticated to http://secure.example.com that browses to http://insecure.example.com risks exposing their session cookie from http://secure.example.com.

Recommendations:

Make sure to set cookie domains to be as restrictive as possible.

Example 2: The following configuration option in application.properties shows how to set the session cookie domain to "secure.example.com" for the Example 1 example.

server.servlet.session.cookie.domain=secure.example.com

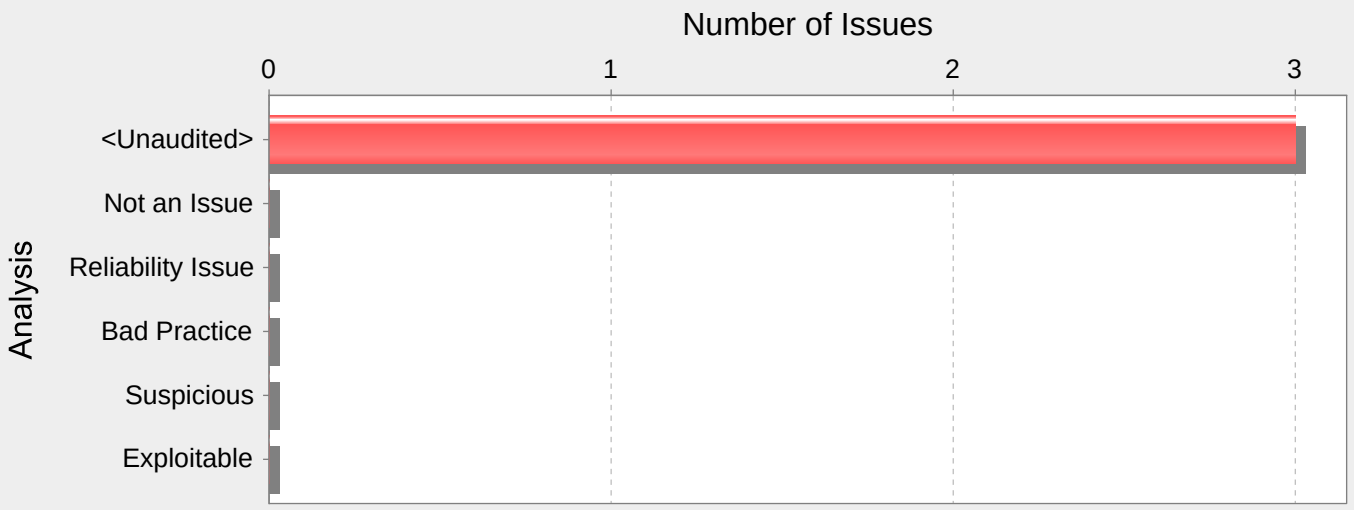
application.properties, line 32 (Cookie Security: Overly Broad Session Cookie Domain)

Fortify Priority:	High	**Folder**	High
Kingdom:	Security Features		
Abstract:	A session cookie with an overly broad domain can be accessed by applications sharing the same base domain.		

Sink: application.properties:32 server.servlet.session.cookie.domain()

```
30  #spring.datasource.password=******
31
32  server.servlet.session.cookie.domain=.ndcbbsr.nic.in
33  server.servlet.session.cookie.http-only=true
34  server.servlet.session.cookie.path=/
```

Category: Cookie Security: Overly Broad Session Cookie Path (3 Issues)



Abstract:

A session cookie with an overly broad path can be compromised through applications sharing the same domain.

Explanation:

Developers often set session cookies to be the root context path ("/"). This exposes the cookie to all web applications on the same domain name. Leaking session cookies can lead to account compromises because an attacker may steal the session cookie using a vulnerability in any of the applications on the domain.

Example 1: Imagine you have a forum application deployed at http://communitypages.example.com/MyForum and the application sets a session cookie with path "/" when users log in to the forum. For example:

server.servlet.session.cookie.path=/

Suppose an attacker creates another application at http://communitypages.example.com/EvilSite and posts a link to this site on the forum. When a user of the forum clicks this link, his browser will send the session cookie set by /MyForum to the application running at /EvilSite. By using the session cookie provided from the user on /MyForum, the attacker can compromise the account of any forum user that browses to /EvilSite.

Recommendations:

Set session cookie paths to be as restrictive as possible.

Example 2: The following code shows how to set the session cookie path to "/MyForum" for Example 1.

server.servlet.session.cookie.path=/MyForum

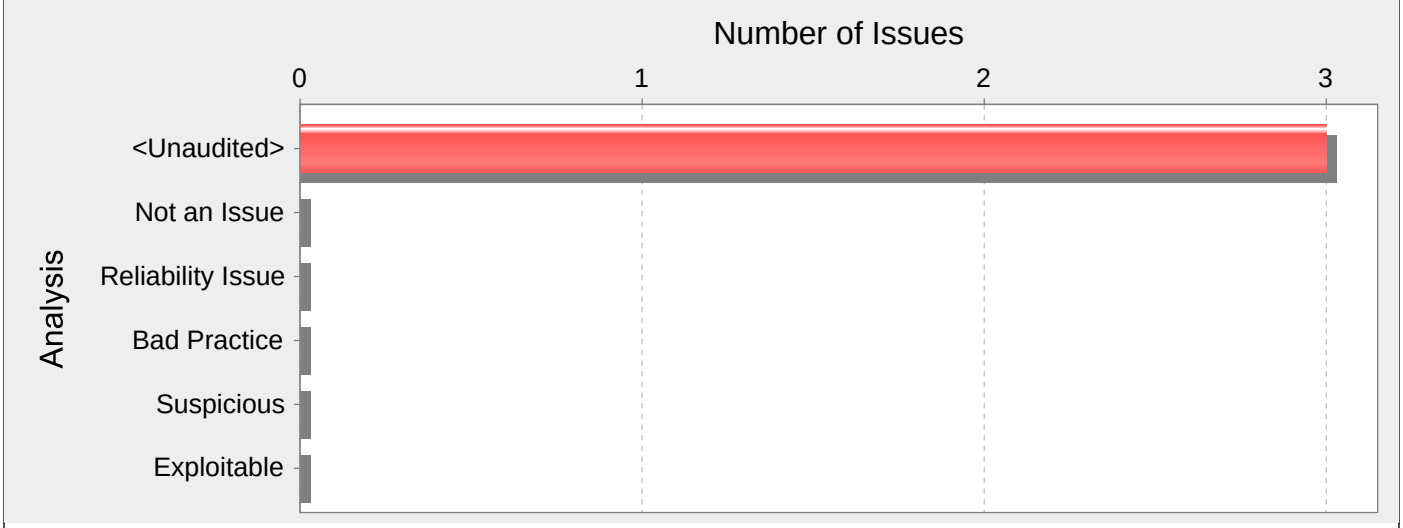
application.properties, line 34 (Cookie Security: Overly Broad Session Cookie Path)

Fortify Priority:	High	**Folder**	High
Kingdom:	Security Features		
Abstract:	A session cookie with an overly broad path can be compromised through applications sharing the same domain.		

Sink: application.properties:34 server.servlet.session.cookie.path()

```
32  server.servlet.session.cookie.domain=.ndcbbsr.nic.in
33  server.servlet.session.cookie.http-only=true
34  server.servlet.session.cookie.path=/
35
36  server.servlet.session.timeout=30m
```

Category: Password Management: Password in Configuration File (3 Issues)



Abstract:

Storing a plain text password in a configuration file may result in a system compromise.

Explanation:

Storing a plain text password in a configuration file allows anyone who can read the file access to the password-protected resource. Developers sometimes believe that they cannot defend the application from someone who has access to the configuration, but this attitude makes an attacker's job easier. Good password management guidelines require that a password never be stored in plain text.

Recommendations:

A password should never be stored in plain text. An administrator should be required to enter the password when the system starts. If that approach is impractical, a less secure but often adequate solution is to obfuscate the password and scatter the de-obfuscation material around the system so that an attacker has to obtain and correctly combine multiple system resources to decipher the password.

Some third-party products claim the ability to manage passwords in a more secure way. For example, WebSphere Application Server 4.x uses a simple XOR encryption algorithm for obfuscating values, but be skeptical about such facilities. WebSphere and other application servers offer outdated and relatively weak encryption mechanisms that are insufficient for security-sensitive environments. For a secure solution the only viable option is a proprietary one.

Tips:

1. Fortify Static Code Analyzer searches configuration files for common names used for password properties. Audit these issues by verifying that the flagged entry is used as a password and that the password entry contains plain text.

2. If the entry in the configuration file is a default password, require that it be changed in addition to requiring that it be obfuscated in the configuration file.

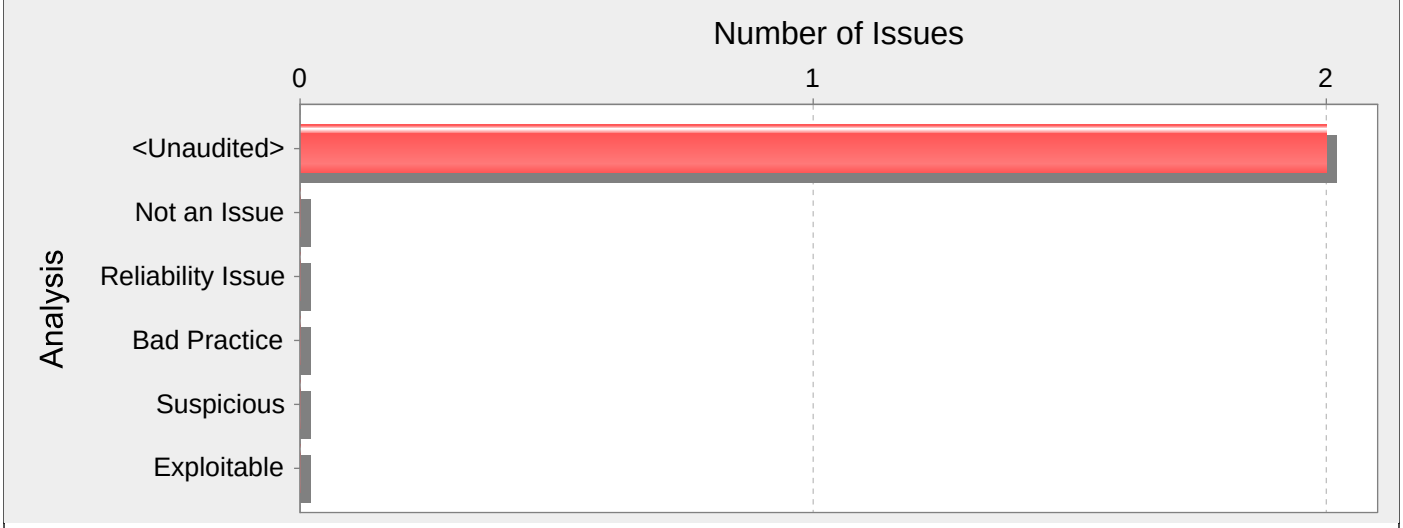
application.properties, line 24 (Password Management: Password in Configuration File)

Fortify Priority:	High	**Folder**	High
Kingdom:	Environment		
Abstract:	Storing a plain text password in a configuration file may result in a system compromise.		

Sink: application.properties:24 spring.datasource.password()

```
22  spring.datasource.url =
    jdbc:postgresql://127.0.0.1:5432/ndcbbsr?useSSL=false&serverTimezone=UTC
23  spring.datasource.username=postgres
24  spring.datasource.password=******
25
26  #production
```

Category: Null Dereference (2 Issues)



Abstract:

The method isTokenValid() in Home.java can crash the program by dereferencing a null-pointer on line 75.

Explanation:

Null-pointer exceptions usually occur when one or more of the programmer's assumptions is violated. A dereference-after-store error occurs when a program explicitly sets an object to null and dereferences it later. This error is often the result of a programmer initializing a variable to null when it is declared.

Most null-pointer issues result in general software reliability problems, but if attackers can intentionally trigger a null-pointer dereference, they can use the resulting exception to bypass security logic or to cause the application to reveal debugging information that will be valuable in planning subsequent attacks.

Example: In the following code, the programmer explicitly sets the variable foo to null. Later, the programmer dereferences foo before checking the object for a null value.

Foo foo = null;
...
foo.setBar(val);
...
}

Recommendations:

Implement careful checks before dereferencing objects that might be null. When possible, abstract null checks into wrappers around code that manipulates resources to ensure that they are applied in all cases and to minimize the places where mistakes can occur.

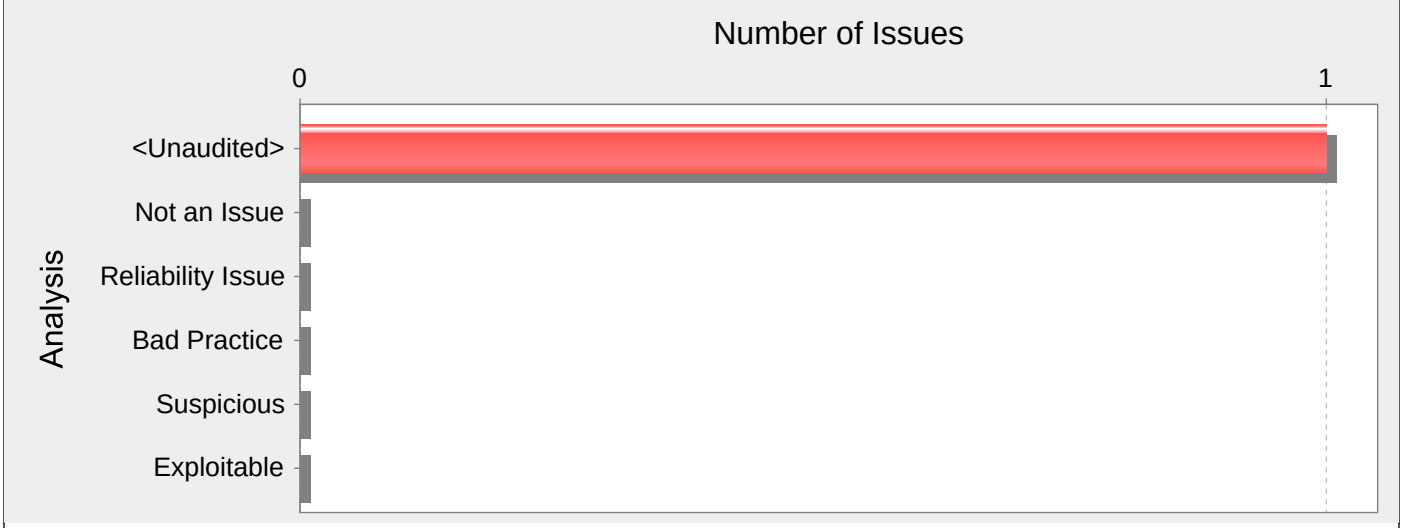
Home.java, line 75 (Null Dereference)

Fortify Priority:	High	**Folder**	High
Kingdom:	Code Quality		
Abstract:	The method isTokenValid() in Home.java can crash the program by dereferencing a null-pointer on line 75.		

Sink: Home.java:75 Dereferenced : responseMap()

```
73                LOGGER.debug("parichay response fetching error");
74               }
75               if (responseMap.get("status").equals("success")) {
76                if (responseMap.get("tokenValid").equals("true"))
```

Category: Access Control: Database (1 Issues)



Abstract:

Without proper access control, the method findNews() in NdcServiceImpl.java can execute a SQL statement on line 231 that contains an attacker-controlled primary key, thereby allowing the attacker to access unauthorized records.

Explanation:

Database access control errors occur when:

1. Data enters a program from an untrusted source.

2. The data is used to specify the value of a primary key in a SQL query.

Example 1: The following code uses a parameterized statement, which escapes metacharacters and prevents SQL injection vulnerabilities, to construct and execute a SQL query that searches for an invoice matching the specified identifier [1]. The identifier is selected from a list of all invoices associated with the current authenticated user.

```
...
id = Integer.decode(request.getParameter("invoiceID"));
String query = "SELECT * FROM invoices WHERE id = ?";
PreparedStatement stmt = conn.prepareStatement(query);
stmt.setInt(1, id);
ResultSet results = stmt.execute();
...
```

The problem is that the developer has failed to consider all of the possible values of id. Although the interface generates a list of invoice identifiers that belong to the current user, an attacker might bypass this interface to request any desired invoice. Because the code in this example does not check to ensure that the user has permission to access the requested invoice, it will display any invoice, even if it does not belong to the current user.

Some think that in the mobile world, classic web application vulnerabilities, such as database access control errors, do not make sense -- why would the user attack themself? However, keep in mind that the essence of mobile platforms is applications that are downloaded from various sources and run alongside each other on the same device. The likelihood of running a piece of malware next to a banking application is high, which necessitates expanding the attack surface of mobile applications to include inter-process communication.

Example 2: The following code adapts Example 1 to the Android platform.

```
...
String id = this.getIntent().getExtras().getString("invoiceID");
String query = "SELECT * FROM invoices WHERE id = ?";
SQLiteDatabase db = this.openOrCreateDatabase("DB", MODE_PRIVATE, null);
Cursor c = db.rawQuery(query, new Object[]{id});
...
```

A number of modern web frameworks provide mechanisms to perform user input validation (including Struts and Spring MVC). To highlight the unvalidated sources of input, Fortify Secure Coding Rulepacks dynamically re-prioritize the issues Fortify Static Code Analyzer reports by lowering their probability of exploit and providing pointers to the supporting evidence whenever the framework validation mechanism is in use. We refer to this feature as Context-Sensitive Ranking. To further assist the Fortify user with the auditing process, the Fortify Software Security Research group makes available the Data Validation project template that groups the issues into folders based on the validation mechanism applied to their source of input.

Recommendations:

Rather than relying on the presentation layer to restrict values submitted by the user, access control should be handled by the application and database layers. Under no circumstances should a user be allowed to retrieve or modify a row in the database without the appropriate permissions. Every query that accesses the database should enforce this policy, which can often be accomplished by simply including the current authenticated username as part of the query.

Example 3: The following code implements the same functionality as Example 1 but imposes an additional constraint to verify that the invoice belongs to the currently authenticated user.

```
...
userName = ctx.getAuthenticatedUserName();
id = Integer.decode(request.getParameter("invoiceID"));
String query =
"SELECT * FROM invoices WHERE id = ? AND user = ?";
PreparedStatement stmt = conn.prepareStatement(query);
stmt.setInt(1, id);
stmt.setString(2, userName);
ResultSet results = stmt.execute();
...
```

And here is an Android equivalent:

```
...
PasswordAuthentication pa = authenticator.getPasswordAuthentication();
String userName = pa.getUserName();
String id = this.getIntent().getExtras().getString("invoiceID");
String query = "SELECT * FROM invoices WHERE id = ? AND user = ?";
SQLiteDatabase db = this.openOrCreateDatabase("DB", MODE_PRIVATE, null);
Cursor c = db.rawQuery(query, new Object[]{id, userName});
...
```

NdcServiceImpl.java, line 231 (Access Control: Database)

Fortify Priority:	High	**Folder**	High
Kingdom:	Security Features		
Abstract:	Without proper access control, the method findNews() in NdcServiceImpl.java can execute a SQL statement on line 231 that contains an attacker-controlled primary key, thereby allowing the attacker to access unauthorized records.		

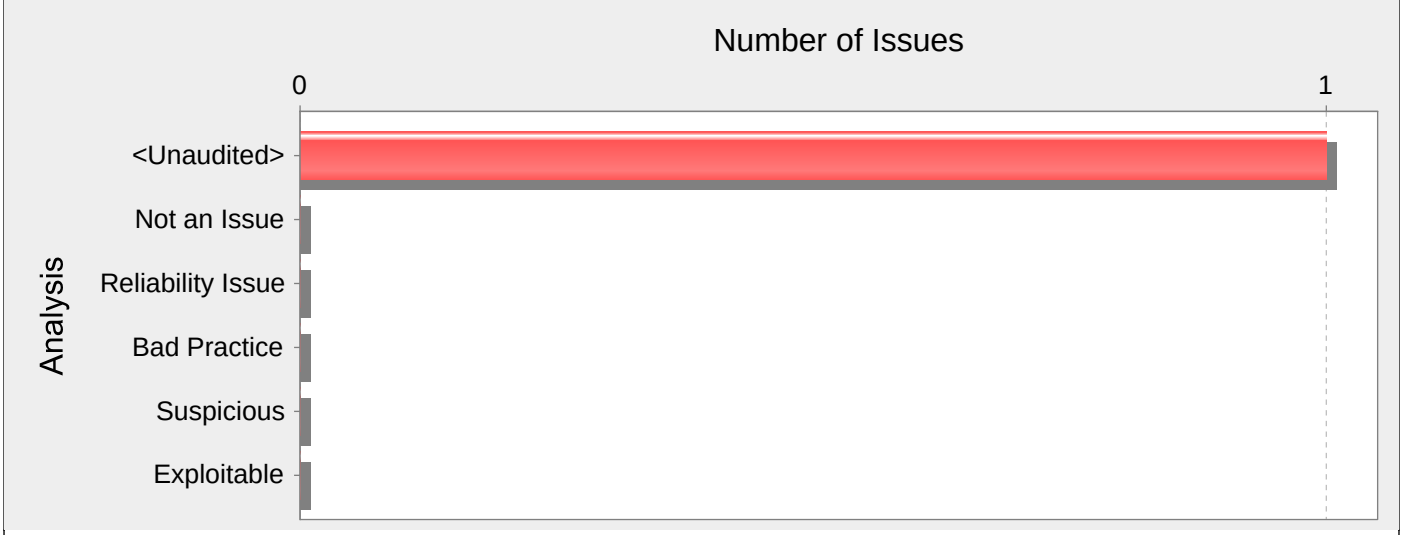
Source: AdminPanelController.java:859 updateNews(1)

```
857  @PostMapping("/updateNews")
858  public String updateNews(@RequestParam(value = "file", required = false) MultipartFile
file,
859     LatestNewsModal newsmodal, HttpServletRequest request) {
860
861   if (!IpLoginCheck()) {
```

Sink: NdcServiceImpl.java:231 org.springframework.data.jpa.repository.JpaRepository.getById()

```
229
230  public LatestNews findNews(int id) {
231   return latestNewsdao.getById(id);
232  }
```

Category: Header Manipulation (1 Issues: 1 Suppressed)



Abstract:

The method getResources() in HomeController.java includes unvalidated data in an HTTP response header on line 143. This enables attacks such as cache-poisoning, cross-site scripting, cross-user defacement, page hijacking, cookie manipulation or open redirect.

Explanation:

Header Manipulation vulnerabilities occur when:

1. Data enters a web application through an untrusted source, most frequently an HTTP request.

2. The data is included in an HTTP response header sent to a web user without being validated.

As with many software security vulnerabilities, Header Manipulation is a means to an end, not an end in itself. At its root, the vulnerability is straightforward: an attacker passes malicious data to a vulnerable application, and the application includes the data in an HTTP response header.

One of the most common Header Manipulation attacks is HTTP Response Splitting. To mount a successful HTTP Response Splitting exploit, the application must allow input that contains CR (carriage return, also given by %0d or \r) and LF (line feed, also given by %0a or \n)characters into the header. These characters not only give attackers control of the remaining headers and body of the response the application intends to send, but also allows them to create additional responses entirely under their control.

Many of today's modern application servers will prevent the injection of malicious characters into HTTP headers. For example, recent versions of Apache Tomcat will throw an IllegalArgumentException if you attempt to set a header with prohibited characters. If your application server prevents setting headers with new line characters, then your application is not vulnerable to HTTP Response Splitting. However, solely filtering for new line characters can leave an application vulnerable to Cookie Manipulation or Open Redirects, so care must still be taken when setting HTTP headers with user input.

Example: The following code segment reads the name of the author of a weblog entry, author, from an HTTP request and sets it in a cookie header of an HTTP response.

String author = request.getParameter(AUTHOR_PARAM);

...

Cookie cookie = new Cookie("author", author);

cookie.setMaxAge(cookieExpiration);

response.addCookie(cookie);

Assuming a string consisting of standard alphanumeric characters, such as "Jane Smith", is submitted in the request the HTTP response including this cookie might take the following form:

HTTP/1.1 200 OK

...

Set-Cookie: author=Jane Smith

...

However, because the value of the cookie is formed of unvalidated user input the response will only maintain this form if the value submitted for AUTHOR_PARAM does not contain any CR and LF characters. If an attacker submits a malicious string, such as "Wiley Hacker\r\nHTTP/1.1 200 OK\r\n...", then the HTTP response would be split into two responses of the following form:

HTTP/1.1 200 OK

...
Set-Cookie: author=Wiley Hacker

HTTP/1.1 200 OK

...

Clearly, the second response is completely controlled by the attacker and can be constructed with any header and body content desired. The ability of attacker to construct arbitrary HTTP responses permits a variety of resulting attacks, including: cross-user defacement, web and browser cache poisoning, cross-site scripting, and page hijacking.

Cross-User Defacement: An attacker will be able to make a single request to a vulnerable server that will cause the server to create two responses, the second of which may be misinterpreted as a response to a different request, possibly one made by another user sharing the same TCP connection with the server. This can be accomplished by convincing the user to submit the malicious request themselves, or remotely in situations where the attacker and the user share a common TCP connection to the server, such as a shared proxy server. In the best case, an attacker may leverage this ability to convince users that the application has been hacked, causing users to lose confidence in the security of the application. In the worst case, an attacker may provide specially crafted content designed to mimic the behavior of the application but redirect private information, such as account numbers and passwords, back to the attacker.

Cache Poisoning: The impact of a maliciously constructed response can be magnified if it is cached either by a web cache used by multiple users or even the browser cache of a single user. If a response is cached in a shared web cache, such as those commonly found in proxy servers, then all users of that cache will continue receive the malicious content until the cache entry is purged. Similarly, if the response is cached in the browser of an individual user, then that user will continue to receive the malicious content until the cache entry is purged, although only the user of the local browser instance will be affected.

Cross-Site Scripting: Once attackers have control of the responses sent by an application, they have a choice of a variety of malicious content to provide users. Cross-site scripting is common form of attack where malicious JavaScript or other code included in a response is executed in the user's browser. The variety of attacks based on XSS is almost limitless, but they commonly include transmitting private data like cookies or other session information to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site. The most common and dangerous attack vector against users of a vulnerable application uses JavaScript to transmit session and authentication information back to the attacker who can then take complete control of the victim's account.

Page Hijacking: In addition to using a vulnerable application to send malicious content to a user, the same root vulnerability can also be leveraged to redirect sensitive content generated by the server and intended for the user to the attacker instead. By submitting a request that results in two responses, the intended response from the server and the response generated by the attacker, an attacker may cause an intermediate node, such as a shared proxy server, to misdirect a response generated by the server for the user to the attacker. Because the request made by the attacker generates two responses, the first is interpreted as a response to the attacker's request, while the second remains in limbo. When the user makes a legitimate request through the same TCP connection, the attacker's request is already waiting and is interpreted as a response to the victim's request. The attacker then sends a second request to the server, to which the proxy server responds with the server generated request intended for the victim, thereby compromising any sensitive information in the headers or body of the response intended for the victim.

Cookie Manipulation: When combined with attacks like Cross-Site Request Forgery, attackers may change, add to, or even overwrite a legitimate user's cookies.

Open Redirect: Allowing unvalidated input to control the URL used in a redirect can aid phishing attacks.

Recommendations:

The solution to Header Manipulation is to ensure that input validation occurs in the correct places and checks for the correct properties.

Since Header Manipulation vulnerabilities occur when an application includes malicious data in its output, one logical approach is to validate data immediately before it leaves the application. However, because web applications often have complex and intricate code for generating responses dynamically, this method is prone to errors of omission (missing validation). An effective way to mitigate this risk is to also perform input validation for Header Manipulation.

Web applications must validate their input to prevent other vulnerabilities, such as SQL injection, so augmenting an application's existing input validation mechanism to include checks for Header Manipulation is generally relatively easy. Despite its value, input validation for Header Manipulation does not take the place of rigorous output validation. An application might accept input through a shared data store or other trusted source, and that data store might accept input from a source that does not perform adequate input validation. Therefore, the application cannot implicitly rely on the safety of this or any other data. This means that the best way to prevent Header Manipulation vulnerabilities is to validate everything that enters the application or leaves the application destined for the user.

The most secure approach to validation for Header Manipulation is to create an allow list of safe characters that are permitted to appear in HTTP response headers and accept input composed exclusively of characters in the approved set. For example, a valid name might only include alphanumeric characters or an account number might only include digits 0-9.

A more flexible, but less secure approach is to implement a deny list, which selectively rejects or escapes potentially dangerous characters before using the input. To form such a list, you first need to understand the set of characters that hold special meaning in HTTP response headers. Although the CR and LF characters are at the heart of an HTTP response splitting attack, other characters, such as ':' (colon) and '=' (equal), have special meaning in response headers as well.

After you identify the correct points in an application to perform validation for Header Manipulation attacks and what special characters the validation should consider, the next challenge is to identify how your validation handles special characters. The application should reject any input destined to be included in HTTP response headers that contains special characters, particularly CR and LF, as invalid.

Many application servers attempt to limit an application's exposure to HTTP response splitting vulnerabilities by providing implementations for the functions responsible for setting HTTP headers and cookies that perform validation for the characters essential to an HTTP response splitting attack. Do not rely on the server running your application to make it secure. For any developed application, there are no guarantees about which application servers it will run on during its lifetime. As standards and known exploits evolve, there are no guarantees that application servers will continue to stay in sync.

Tips:

1. Many HttpServletRequest implementations return a URL-encoded string from getHeader(), will not cause a HTTP response splitting issue unless it is decoded first because the CR and LF characters will not carry a meta-meaning in their encoded form. However, this behavior is not specified in the J2EE standard and varies by implementation. Furthermore, even encoded user input returned from getHeader() can lead to other vulnerabilities, including open redirects and other HTTP header tampering.

2. A number of modern web frameworks provide mechanisms to perform user input validation (including Struts and Spring MVC). To highlight the unvalidated sources of input, Fortify Secure Coding Rulepacks dynamically re-prioritize the issues Fortify Static Code Analyzer reports by lowering their probability of exploit and providing pointers to the supporting evidence whenever the framework validation mechanism is in use. We refer to this feature as Context-Sensitive Ranking. To further assist the Fortify user with the auditing process, the Fortify Software Security Research group makes available the Data Validation project template that groups the issues into folders based on the validation mechanism applied to their source of input.

3. Fortify AppDefender adds protection against this category.

HomeController.java, line 143 (Header Manipulation) [Suppressed]

Fortify Priority:	High	**Folder**	High
Kingdom:	Input Validation and Representation		
Abstract:	The method getResources() in HomeController.java includes unvalidated data in an HTTP response header on line 143. This enables attacks such as cache-poisoning, cross-site scripting, cross-user defacement, page hijacking, cookie manipulation or open redirect.		

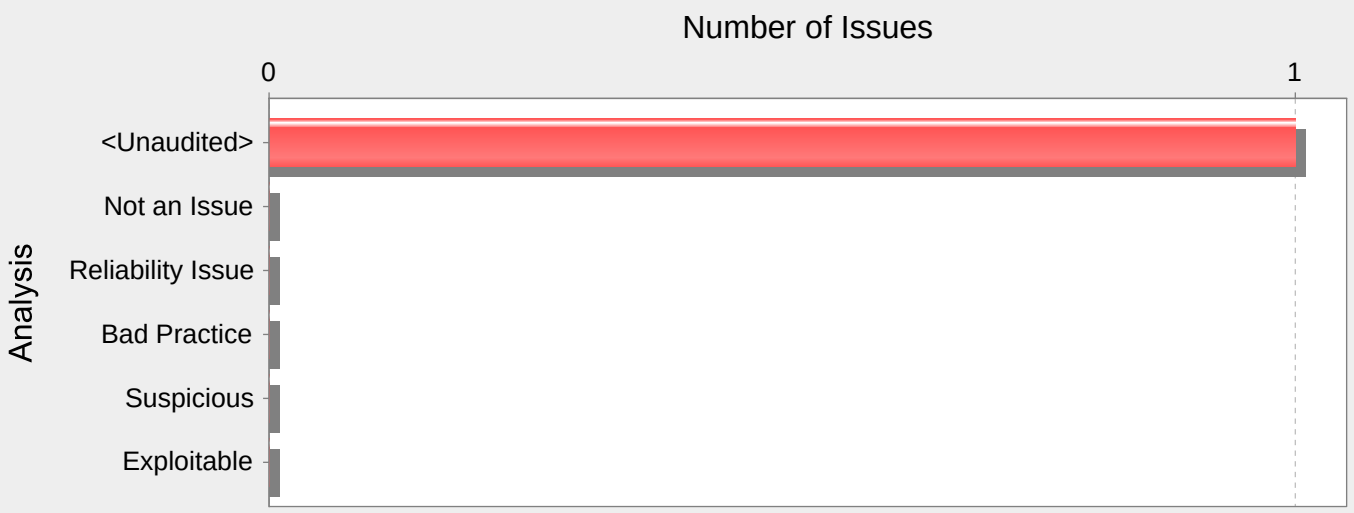
Source: HomeController.java:126 getResources(0)

```
124
125     @RequestMapping(value={"/getdata"}, method = RequestMethod.GET)
126     public ModelAndView getResources(@RequestParam("rid") String rid,@RequestParam("dir") String dir,
127       HttpServletResponse response,Model model)
128     {
```

Sink: HomeController.java:143 javax.servlet.http.HttpServletResponse.setHeader()

```
141       }
142
143       response.setHeader("Content-Disposition", "attachment;filename=".concat(String.valueOf(rid)));
144       OutputStream os = response.getOutputStream();
145       os.write(byteArr);
```

Category: Header Manipulation: SMTP (1 Issues)



Abstract:

The method SendMail() in MailAuthSMTP.java includes unvalidated data in an SMTP header on line 43. This enables attackers to add arbitrary headers such as CC or BCC that they can use to leak the mail contents to themselves or use the mail server as a spam bot.

Explanation:

SMTP Header Manipulation vulnerabilities occur when:

1. Data enters an application through an untrusted source, most frequently an HTTP request in a web application.

2. The data is included in an SMTP header sent to a mail server without being validated.

As with many software security vulnerabilities, SMTP Header Manipulation is a means to an end, not an end in itself. At its root, the vulnerability is straightforward: an attacker passes malicious data to a vulnerable application, and the application includes the data in an SMTP header.

One of the most common SMTP Header Manipulation attacks is used for distributing spam emails. If an application contains a vulnerable "Contact us" form that allows setting the subject and the body of the email, an attacker will be able to set any arbitrary content and inject a CC header with a list of email addresses to spam anonymously since the email will be sent from the victim server.

Example: The following code segment reads the subject and body of a "Contact us" form:

```
String subject = request.getParameter("subject");
String body = request.getParameter("body");
MimeMessage message = new MimeMessage(session);
message.setFrom(new InternetAddress("webform@acme.com"));
message.setRecipients(Message.RecipientType.TO, InternetAddress.parse("support@acme.com"));
message.setSubject("[Contact us query] " + subject);
message.setText(body);
Transport.send(message);
```

Assuming a string consisting of standard alphanumeric characters, such as "Page not working" is submitted in the request, the SMTP headers might take the following form:

```
...
subject: [Contact us query] Page not working
...
```

However, because the value of the header is constructed from unvalidated user input the response will only maintain this form if the value submitted for subject does not contain any CR and LF characters. If an attacker submits a malicious string, such as "Congratulations!! You won the lottery!!!\r\ncc:victim1@mail.com,victim2@mail.com ...", then the SMTP headers would be of the following form:

```
...
subject: [Contact us query] Congratulations!! You won the lottery
cc: victim1@mail.com,victim2@mail.com
...
```

This will effectively allow an attacker to craft spam messages or to send anonymous emails amongst other attacks.

Recommendations:

The solution to SMTP Header Manipulation is to ensure that input validation occurs in the correct places and checks for the correct properties.

Since SMTP Header Manipulation vulnerabilities occur when an application includes malicious data in its output, one logical approach is to validate data immediately before it is used in the header context and make sure there are no illegal CRLF characters that can break the header structure.

MailAuthSMTP.java, line 43 (Header Manipulation: SMTP)

Fortify Priority:	High	**Folder**	High
Kingdom:	Input Validation and Representation		
Abstract:	The method SendMail() in MailAuthSMTP.java includes unvalidated data in an SMTP header on line 43. This enables attackers to add arbitrary headers such as CC or BCC that they can use to leak the mail contents to themselves or use the mail server as a spam bot.		

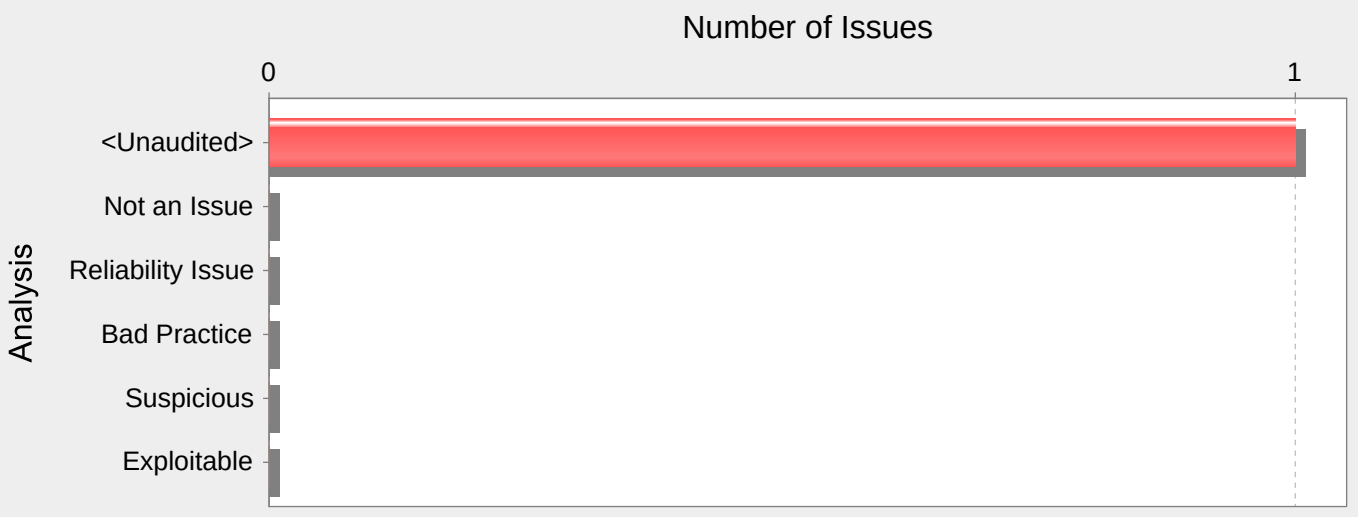
Source: TokenAuth.java:81 MailPush(3)

```
79
80                 @GetMapping("/mailpush")
81                 public Map<String, String> MailPush(String url, String mailid, String content, String
                   subject, String sender, String token) throws JsonProcessingException  {
82
83
```

Sink: MailAuthSMTP.java:43 javax.mail.internet.MimeMessage.setSubject()

```
41                   MimeMessage message = new MimeMessage(mailSession);
42                   message.setContent(msg, "text/html; charset=utf-8");
43                   message.setSubject(subject);
44                   message.setFrom(new InternetAddress("noreply-ndcbbsr@nic.in")); // from address
45                   message.addRecipient(Message.RecipientType.TO, new InternetAddress(email));
```

Category: HTML5: Missing Content Security Policy (1 Issues)



Abstract:

Content Security Policy (CSP) is not configured.

Explanation:

Content Security Policy (CSP) is a declarative security header that enables developers to dictate which domains the site is allowed to load content from or initiate connections to when rendered in the web browser. It provides an additional layer of security from critical vulnerabilities such as cross-site scripting, clickjacking, cross-origin access and the like, on top of input validation and checking an allow list in code.

Spring Security and other frameworks do not add Content Security Policy headers by default. The web application author must declare the security policy/policies to enforce or monitor for the protected resources to benefit from this additional layer of security.

Recommendations:

Configure a Content Security Policy to mitigate possible injection vulnerabilities.

Example: The following code sets a Content Security Policy in a Spring Security protected application:

```
@Override
protected void configure(HttpSecurity http) throws Exception {
...
String policy = getCSPolicy();
http.headers().contentSecurityPolicy(policy);
...
}
```

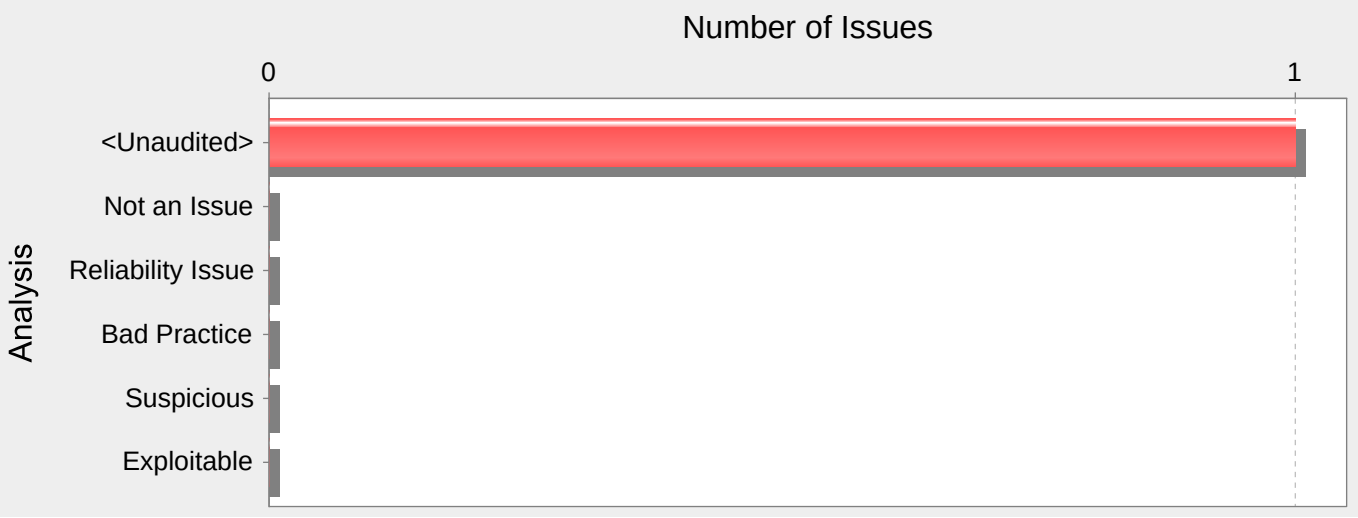
Content Security Policy is not intended to solve all content injection vulnerabilities. Instead, you can leverage CSP to help reduce the harm caused by content injection attacks. Use regular defensive coding,above, current such as input validation and output encoding.

SecSecurityConfig.java, line 20 (HTML5: Missing Content Security Policy)

Fortify Priority:	Critical	**Folder**	Critical
Kingdom:	Encapsulation		
Abstract:	Content Security Policy (CSP) is not configured.		
Sink:	SecSecurityConfig.java:20 Function: configure()		

```
18
19                      @Override
20                      protected void configure(HttpSecurity http)  {
21
22                       try {
```

Category: Key Management: Empty Encryption Key (1 Issues)



Abstract:

Empty encryption keys can compromise security in a way that cannot be easily remedied.

Explanation:

It is never a good idea to use an empty encryption key because it significantly reduces the protection afforded by a good encryption algorithm, and it also makes fixing the problem extremely difficult. After the offending code is in production, the empty encryption key cannot be changed without patching the software. If an account that is protected by the empty encryption key is compromised, the owners of the system must choose between security and availability.

Example 1: The following code performs AES encryption using an empty encryption key:

```
...
private static String encryptionKey = "";
byte[] keyBytes = encryptionKey.getBytes();
SecretKeySpec key = new SecretKeySpec(keyBytes, "AES");
Cipher encryptCipher = Cipher.getInstance("AES");
encryptCipher.init(Cipher.ENCRYPT_MODE, key);
...
```

Not only will anyone who has access to the code be able to determine that it uses an empty encryption key, but anyone with even basic cracking techniques is much more likely to successfully decrypt any encrypted data. After the application has shipped, a software patch is required to change the empty encryption key. An employee with access to this information can use it to break into the system. Even if attackers only had access to the application's executable, they could extract evidence of the use of an empty encryption key.

Recommendations:

Encryption keys should never be empty and should be obfuscated and managed in an external source. Storing encryption keys in plain text, empty or otherwise, anywhere on the system allows anyone with sufficient permissions to read and potentially misuse the encryption key.

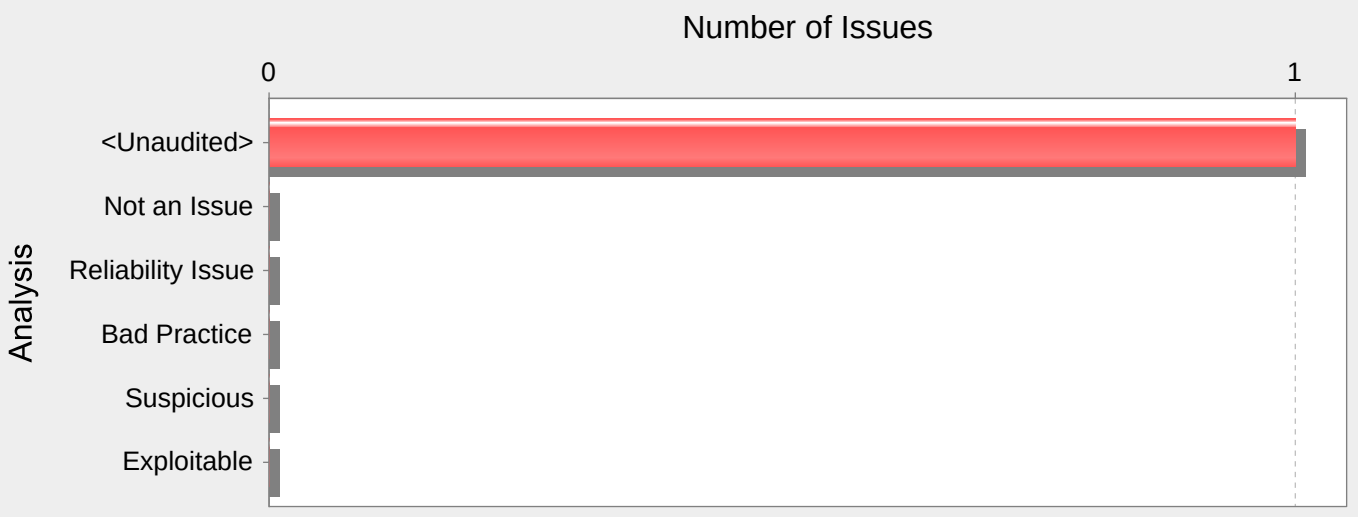
AdminPanelController.java, line 143 (Key Management: Empty Encryption Key)

Fortify Priority:	High	**Folder**	High
Kingdom:	Security Features		
Abstract:	Empty encryption keys can compromise security in a way that cannot be easily remedied.		

Sink: AdminPanelController.java:143 VariableAccess: key()

```
141  public String TokenAppGetter(String app) {
142
143    String key = "";
144
145    List<Keytable> list = ndcservice.findAllKeytable();
```

Category: Key Management: Hardcoded Encryption Key (1 Issues)



Abstract:

Hardcoded encryption keys can compromise security in a way that cannot be easily remedied.

Explanation:

It is never a good idea to hardcode an encryption key because it allows all of the project's developers to view the encryption key, and makes fixing the problem extremely difficult. After the code is in production, a software patch is required to change the encryption key. If the account that is protected by the encryption key is compromised, the owners of the system must choose between security and availability.

Example 1: The following code uses a hardcoded encryption key:

```
...
private static final String encryptionKey = "lakdsljkalkjlksdfkl";
byte[] keyBytes = encryptionKey.getBytes();
SecretKeySpec key = new SecretKeySpec(keyBytes, "AES");
Cipher encryptCipher = Cipher.getInstance("AES");
encryptCipher.init(Cipher.ENCRYPT_MODE, key);
...
```

Anyone with access to the code has access to the encryption key. After the application has shipped, there is no way to change the encryption key unless the program is patched. An employee with access to this information can use it to break into the system. If attackers had access to the executable for the application, they could extract the encryption key value.

Recommendations:

Encryption keys should never be hardcoded and should be obfuscated and managed in an external source. Storing encryption keys in plain text anywhere on the system allows anyone with sufficient permissions to read and potentially misuse the encryption key.

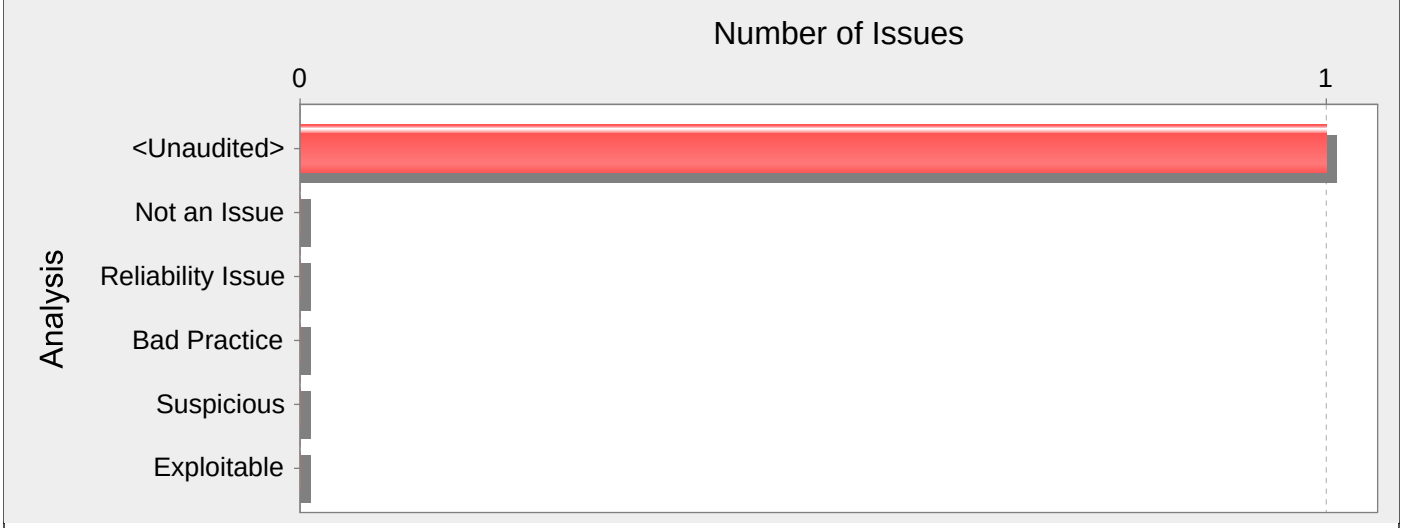
AesCryptobak.java, line 97 (Key Management: Hardcoded Encryption Key)

Fortify Priority:	Critical	**Folder**	Critical
Kingdom:	Security Features		
Abstract:	Hardcoded encryption keys can compromise security in a way that cannot be easily remedied.		

Sink: AesCryptobak.java:97 VariableAccess: key()

```
95    public static void main(String[] args) {
96
97       String key = "0123456789abcdef"; // 128 bit key
98       String initVector = "abcdef9876543210"; // 16 bytes IV, it is recommended to use a
different random IV for every message!
```

Category: Privacy Violation (1 Issues)



Abstract:

The method testEncryption() in AesCrypto.java mishandles confidential information, which can compromise user privacy and is often illegal.

Explanation:

Privacy violations occur when:

1. Private user information enters the program.

2. The data is written to an external location, such as the console, file system, or network.

Example 1: The following code contains a logging statement that tracks the records added to a database by storing the contents in a log file.

```
pass = getPassword();
...
dbmsLog.println(id+":"+pass+":"+type+":"+tstamp);
```

The code in Example 1 logs a plain text password to the file system. Although many developers trust the file system as a safe storage location for data, it should not be trusted implicitly, particularly when privacy is a concern.

Privacy is one of the biggest concerns in the mobile world for a couple of reasons. One of them is a much higher chance of device loss. The other has to do with inter-process communication between mobile applications. With mobile platforms, applications are downloaded from various sources and are run alongside each other on the same device. The likelihood of running a piece of malware next to a banking application is high, which is why application authors need to be careful about what information they include in messages addressed to other applications running on the device. Sensitive information should never be part of inter-process communication between mobile applications.

Example 2: The following code reads username and password for a given site from an Android WebView store and broadcasts them to all the registered receivers.

```
...
webview.setWebViewClient(new WebViewClient() {
public void onReceivedHttpAuthRequest(WebView view,
HttpAuthHandler handler, String host, String realm) {
String[] credentials = view.getHttpAuthUsernamePassword(host, realm);
String username = credentials[0];
String password = credentials[1];
Intent i = new Intent();
i.setAction("SEND_CREDENTIALS");
i.putExtra("username", username);
i.putExtra("password", password);
view.getContext().sendBroadcast(i);
}
});
...
```

This example demonstrates several problems. First of all, by default, WebView credentials are stored in plain text and are not hashed. If a user has a rooted device (or uses an emulator), they can read stored passwords for given sites. Second, plain text credentials are broadcast to all the registered receivers, which means that any receiver registered to listen to intents with the SEND_CREDENTIALS action will receive the message. The broadcast is not even protected with a permission to limit the number of recipients, although in this case we do not recommend using permissions as a fix.

Private data can enter a program in a variety of ways:

- Directly from the user in the form of a password or personal information

- Accessed from a database or other data store by the application

- Indirectly from a partner or other third party

Typically, in the context of the mobile environment, this private information includes (along with passwords, SSNs, and other general personal information):

- Location

- Cell phone number

- Serial numbers and device IDs

- Network Operator information

- Voicemail information

Sometimes data that is not labeled as private can have a privacy implication in a different context. For example, student identification numbers are usually not considered private because there is no explicit and publicly-available mapping to an individual student's personal information. However, if a school generates identification numbers based on student social security numbers, then the identification numbers should be considered private.

Security and privacy concerns often seem to compete with each other. From a security perspective, you should record all important operations so that any anomalous activity can later be identified. However, when private data is involved, this practice can create risk.

Although there are many ways in which private data can be handled unsafely, a common risk stems from misplaced trust. Programmers often trust the operating environment in which a program runs, and therefore believe that it is acceptable to store private information on the file system, in the registry, or in other locally-controlled resources. However, even if access to certain resources is restricted, this does not guarantee that the individuals who do have access can be trusted. For example, in 2004, an unscrupulous employee at AOL sold approximately 92 million private customer email addresses to a spammer marketing an offshore gambling web site [1].

In response to such high-profile exploits, the collection and management of private data is becoming increasingly regulated. Depending on its location, the type of business it conducts, and the nature of any private data it handles, an organization may be required to comply with one or more of the following federal and state regulations:

- Safe Harbor Privacy Framework [3]

- Gramm-Leach Bliley Act (GLBA) [4]

- Health Insurance Portability and Accountability Act (HIPAA) [5]

- California SB-1386 [6]

Despite these regulations, privacy violations continue to occur with alarming frequency.

Recommendations:

When security and privacy demands clash, privacy should usually be given the higher priority. To accomplish this and still maintain required security information, cleanse any private information before it exits the program.

To enforce good privacy management, develop and strictly adhere to internal privacy guidelines. The guidelines should specifically describe how an application should handle private data. If your organization is regulated by federal or state law, ensure that your privacy guidelines are sufficiently strenuous to meet the legal requirements. Even if your organization is not regulated, you must protect private information or risk losing customer confidence.

The best policy with respect to private data is to minimize its exposure. Applications, processes, and employees should not be granted access to any private data unless the access is required for the tasks that they are to perform. Just as the principle of least privilege dictates that no operation should be performed with more than the necessary privileges, access to private data should be restricted to the smallest possible group.

For mobile applications, make sure they never communicate any sensitive data to other applications running on the device. When private data needs to be stored, it should always be encrypted. For Android, as well as any other platform that uses SQLite database, SQLCipher is a good alternative. SQLCipher is an extension to the SQLite database that provides transparent 256-bit AES encryption of database files. Thus, credentials can be stored in an encrypted database.

Example 3: The following code demonstrates how to integrate SQLCipher into an Android application after downloading the necessary binaries, and store credentials into the database file.

```
import net.sqlcipher.database.SQLiteDatabase;
```

...
SQLiteDatabase.loadLibs(this);
File dbFile = getDatabasePath("credentials.db");
dbFile.mkdirs();
dbFile.delete();
SQLiteDatabase db = SQLiteDatabase.openOrCreateDatabase(dbFile, "credentials", null);
db.execSQL("create table credentials(u, p)");
db.execSQL("insert into credentials(u, p) values(?, ?)", new Object[]{username, password});
...

Note that references to android.database.sqlite.SQLiteDatabase are substituted with those of net.sqlcipher.database.SQLiteDatabase.

To enable encryption on the WebView store, you must recompile WebKit with the sqlcipher.so library.

Example 4: The following code reads username and password for a given site from an Android WebView store and instead of broadcasting them to all the registered receivers, it only broadcasts internally so that the broadcast is only seen by other parts of the same application.

...
webview.setWebViewClient(new WebViewClient() {
public void onReceivedHttpAuthRequest(WebView view,
HttpAuthHandler handler, String host, String realm) {
String[] credentials = view.getHttpAuthUsernamePassword(host, realm);
String username = credentials[0];
String password = credentials[1];
Intent i = new Intent();
i.setAction("SEND_CREDENTIALS");
i.putExtra("username", username);
i.putExtra("password", password);
LocalBroadcastManager.getInstance(view.getContext()).sendBroadcast(i);
}
});
...

Tips:

1. As part of any thorough audit for privacy violations, ensure that custom rules are written to identify all sources of private or otherwise sensitive information entering the program. Most sources of private data cannot be identified automatically. Without custom rules, your check for privacy violations is likely to be substantially incomplete.

2. You can use the Fortify Java Annotations FortifyPassword, FortifyNotPassword, FortifyPrivate, and FortifyNotPrivate to indicate which fields and variables represent passwords and private data.

3. A number of modern web frameworks provide mechanisms to perform user input validation (including Struts and Spring MVC). To highlight the unvalidated sources of input, Fortify Secure Coding Rulepacks dynamically re-prioritize the issues Fortify Static Code Analyzer reports by lowering their probability of exploit and providing pointers to the supporting evidence whenever the framework validation mechanism is in use. We refer to this feature as Context-Sensitive Ranking. To further assist the Fortify user with the auditing process, the Fortify Software Security Research group makes available the Data Validation project template that groups the issues into folders based on the validation mechanism applied to their source of input.

AesCrypto.java, line 31 (Privacy Violation)

Fortify Priority:	Critical	**Folder**	Critical
Kingdom:	Security Features		
Abstract:	The method testEncryption() in AesCrypto.java mishandles confidential information, which can compromise user privacy and is often illegal.		
Source:	AesCrypto.java:29 com.example.ndcbbsrweb.util.AesCrypto.decrypt()		

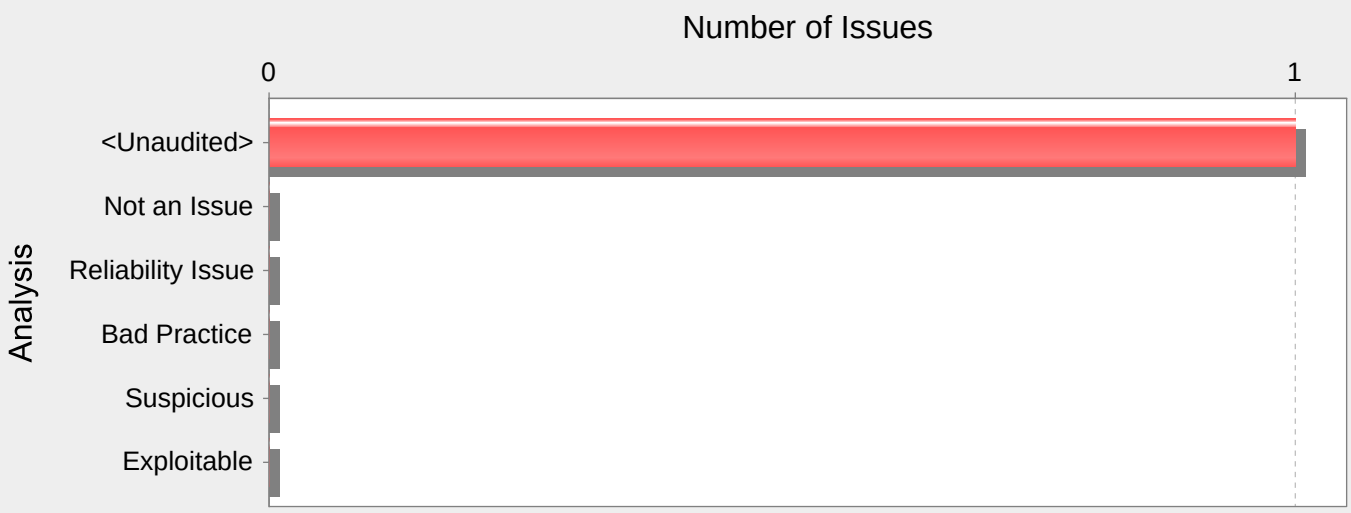
```
27
28              byte[] cipherText = encrypt( secretKey, associatedData,message);
29              String decrypted = decrypt(cipherText, secretKey, associatedData);
30
31              System.out.println(message+","+ decrypted);
```

Sink: AesCrypto.java:31 java.io.PrintStream.println()

```
29              String decrypted = decrypt(cipherText, secretKey, associatedData);
```

```
30
31                          System.out.println(message+","+ decrypted);
32                      }
```

Category: Unreleased Resource: Streams (1 Issues)



Abstract:

The function uploadFile() in UnusedMethods.java sometimes fails to release a system resource allocated by FileOutputStream() on line 24.

Explanation:

The program can potentially fail to release a system resource.

Resource leaks have at least two common causes:

- Error conditions and other exceptional circumstances.

- Confusion over which part of the program is responsible for releasing the resource.

Most unreleased resource issues result in general software reliability problems. However, if an attacker can intentionally trigger a resource leak, the attacker may be able to launch a denial of service attack by depleting the resource pool.

Example: The following method never closes the file handle it opens. The finalize() method for FileInputStream eventually calls close(), but there is no guarantee as to how long it will take before the finalize() method will be invoked. In a busy environment, this can result in the JVM using up all of its file handles.

```
private void processFile(String fName) throws FileNotFoundException, IOException {
FileInputStream fis = new FileInputStream(fName);
int sz;
byte[] byteArray = new byte[BLOCK_SIZE];
while ((sz = fis.read(byteArray)) != -1) {
processBytes(byteArray, sz);
}
}
```

Recommendations:

1. Never rely on finalize() to reclaim resources. In order for an object's finalize() method to be invoked, the garbage collector must determine that the object is eligible for garbage collection. Because the garbage collector is not required to run unless the JVM is low on memory, there is no guarantee that an object's finalize() method will be invoked in an expedient fashion. When the garbage collector finally does run, it may cause a large number of resources to be reclaimed in a short period of time, which can lead to "bursty" performance and lower overall system throughput. This effect becomes more pronounced as the load on the system increases.

Finally, if it is possible for a resource reclamation operation to hang (if it requires communicating over a network to a database, for example), then the thread that is executing the finalize() method will hang.

2. Release resources in a finally block. The code for the Example should be rewritten as follows:

```
public void processFile(String fName) throws FileNotFoundException, IOException {
FileInputStream fis;
try {
fis = new FileInputStream(fName);
int sz;
byte[] byteArray = new byte[BLOCK_SIZE];
while ((sz = fis.read(byteArray)) != -1) {
```

```
processBytes(byteArray, sz);
}
}
finally {
if (fis != null) {
safeClose(fis);
}
}
}
public static void safeClose(FileInputStream fis) {
if (fis != null) {
try {
fis.close();
} catch (IOException e) {
log(e);
}
}
}
```

This solution uses a helper function to log the exceptions that might occur when trying to close the stream. Presumably this helper function will be reused whenever a stream needs to be closed.

Also, the processFile method does not initialize the fis object to null. Instead, it checks to ensure that fis is not null before calling safeClose(). Without the null check, the Java compiler reports that fis might not be initialized. This choice takes advantage of Java's ability to detect uninitialized variables. If fis is initialized to null in a more complex method, cases in which fis is used without being initialized will not be detected by the compiler.

UnusedMethods.java, line 24 (Unreleased Resource: Streams)

Fortify Priority:	High	**Folder**	High
Kingdom:	Code Quality		
Abstract:	The function uploadFile() in UnusedMethods.java sometimes fails to release a system resource allocated by FileOutputStream() on line 24.		
Sink:	UnusedMethods.java:24 bout = new BufferedOutputStream(new java.io.FileOutputStream())		

```
22
23                  byte barr[] = file.getBytes();
24                  BufferedOutputStream bout = new BufferedOutputStream(new FileOutputStream(uploadDir +
"/" + filename));
25                  bout.write(barr);
26                  bout.flush();
```

Detailed Project Summary

Files Scanned

Code base location: D:/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb

Files Scanned:

.mvn/wrapper/maven-wrapper.properties java_properties May 12, 2022 7:41:32 AM

C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/static/index.html.js secondary Mar 28, 2023 4:57:18 PM

C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/aboutus.html.js secondary Mar 28, 2023 4:57:18 PM

C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/admin/Admin-Home.html.js secondary Mar 28, 2023 4:57:18 PM

C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/admin/addBanner.html.js secondary Mar 28, 2023 4:57:18 PM

C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/admin/addGallery.html.js secondary Mar 28, 2023 4:57:18 PM

C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/admin/addHighlight.html.js secondary Mar 28, 2023 4:57:18 PM

C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/admin/addNews.html.js secondary Mar 28, 2023 4:57:18 PM

C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/admin/addPricing.html.js secondary Mar 28, 2023 4:57:18 PM

C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/admin/addTeam.html.js secondary Mar 28, 2023 4:57:18 PM

C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/admin/addTender.html.js secondary Mar 28, 2023 4:57:18 PM

C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/admin/bannerView.html.js secondary Mar 28, 2023 4:57:18 PM

C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/admin/contactus.html.js secondary Mar 28, 2023 4:57:18 PM

C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/admin/editNews.html.js secondary Mar 28, 2023 4:57:18 PM

C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/admin/editTeam.html.js secondary Mar 28, 2023 4:57:18 PM

C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/admin/editcontact.html.js secondary Mar 28, 2023 4:57:18 PM

C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/admin/ipgetter.html.js secondary Mar 28, 2023 4:57:18

PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/admin/login.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/admin/ndc_home.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/admin/other_home.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/admin/portals.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/admin/teamView.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/admin/viewGallery.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/admin/viewHighlights.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/admin/viewNews.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/admin/viewPricing.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/admin/viewTender.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/basictemplate.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/colocation.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/contactus.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/error/400.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/error/404.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/error/500.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/error/error.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/feedback.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/gallery.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB

SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/highlights.html.js secondary Mar 28, 2023 4:57:18 PM C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/index.html.js secondary Mar 28, 2023 4:57:18 PM C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/list-team.html.js secondary Mar 28, 2023 4:57:18 PM C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/pricing.html.js secondary Mar 28, 2023 4:57:18 PM C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/services.html.js secondary Mar 28, 2023 4:57:18 PM C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/welcome.html.js secondary Mar 28, 2023 4:57:18 PM C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/webapp/400.html.js secondary Mar 28, 2023 4:57:18 PM C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/webapp/404.html.js secondary Mar 28, 2023 4:57:18 PM C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/webapp/error.html.js secondary Mar 28, 2023 4:57:18 PM C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/webapp/errorpage.html.js secondary Mar 28, 2023 4:57:18 PM C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/webapp/homeip.html.js secondary Mar 28, 2023 4:57:18 PM C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/webapp/index.html.js secondary Mar 28, 2023 4:57:18 PM C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/webapp/ipgetter.html.js secondary Mar 28, 2023 4:57:18 PM C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/webapp/ndc_official.html.js secondary Mar 28, 2023 4:57:18 PM C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/webapp/unauth.html.js secondary Mar 28, 2023 4:57:18 PM C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/400.html.js secondary Mar 28, 2023 4:57:18 PM C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/404.html.js secondary Mar 28, 2023 4:57:18 PM C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/static/index.html.js secondary Mar 28, 2023 4:57:18 PM C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/aboutus.html.js secondary Mar 28, 2023 4:57:18 PM C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/admin/Admin-Home.html.js secondary Mar 28, 2023 4:57:18 PM C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/admin/addBanner.html.js secondary Mar 28, 2023 4:57:18 PM C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/admin/addGallery.html.js secondary Mar 28, 2023 4:57:18 PM C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/admin/addHighlight.html.js secondary Mar 28, 2023 4:57:18 PM

C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/admin/addNews.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/admin/addPricing.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/admin/addTeam.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/admin/addTender.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/admin/bannerView.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/admin/contactus.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/admin/editNews.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/admin/editTeam.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/admin/editcontact.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/admin/ipgetter.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/admin/login.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/admin/ndc_home.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/admin/other_home.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/admin/portals.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/admin/teamView.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/admin/viewGallery.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/admin/viewHighlights.html.js secondary Mar 28, 2023 4:57:18 PM

C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/admin/viewNews.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/admin/viewPricing.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/admin/viewTender.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/basictemplate.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/colocation.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/contactus.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/error/400.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/error/404.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/error/500.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/error/error.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/feedback.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/gallery.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/highlights.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/index.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/list-team.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/pricing.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/services.html.js secondary Mar 28, 2023 4:57:18 PM

C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/welcome.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/error.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/errorpage.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/homeip.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/index.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/ipgetter.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/ndc_official.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/unauth.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/static/index.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/aboutus.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/admin/Admin-Home.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/admin/addBanner.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/admin/addGallery.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/admin/addHighlight.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/admin/addNews.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/admin/addPricing.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/admin/addTeam.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/admin/addTender.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/admin/bannerView.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/admin/contactus.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/admin/editNews.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB

SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/admin/editTeam.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/admin/editcontact.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/admin/ipgetter.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/admin/login.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/admin/ndc_home.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/admin/other_home.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/admin/portals.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/admin/teamView.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/admin/viewGallery.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/admin/viewHighlights.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/admin/viewNews.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/admin/viewPricing.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/admin/viewTender.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/basictemplate.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/colocation.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/contactus.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/error/400.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/error/404.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/error/500.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/error/error.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/feedback.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/gallery.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB

SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/highlights.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/index.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/list-team.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/pricing.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/services.html.js secondary Mar 28, 2023 4:57:18 PM
C:/Users/sanjukta/AppData/Local/Fortify/sca20.2/build/ndcbbsrweb/extracted/javascript/D/SCA/Year_2023/NDCBBSR/NDCBB
SR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/welcome.html.js secondary Mar 28, 2023 4:57:18 PM
pom.xml xml 4.2 KB Mar 24, 2023 5:14:20 PM
src/main/java/com/example/ndcbbsrweb/NdcbbsrwebApplication.java java 3 Lines May 12, 2022 1:19:38 PM
src/main/java/com/example/ndcbbsrweb/Security/SecSecurityConfig.java java 19 Lines 1.5 KB Mar 24, 2023 12:12:12 PM
src/main/java/com/example/ndcbbsrweb/ServletInitializer.java java 2 Lines May 12, 2022 7:41:32 AM
src/main/java/com/example/ndcbbsrweb/controller/AdminPanelController.java java 491 Lines 39 KB Mar 24, 2023 5:19:04 PM
src/main/java/com/example/ndcbbsrweb/controller/ErrController.java java 8 Lines 1.1 KB Mar 23, 2023 3:53:40 PM
src/main/java/com/example/ndcbbsrweb/controller/GlobalDefaultExceptionHandler.java java 11 Lines 1.5 KB Jan 30, 2023
12:42:00 PM
src/main/java/com/example/ndcbbsrweb/controller/Helper.java java 5 Lines Nov 19, 2022 11:33:56 AM
src/main/java/com/example/ndcbbsrweb/controller/Home.java java 100 Lines 8.7 KB Feb 1, 2023 12:36:42 PM
src/main/java/com/example/ndcbbsrweb/controller/HomeController.java java 45 Lines 4 KB Mar 23, 2023 3:55:36 PM
src/main/java/com/example/ndcbbsrweb/controller/InitController.java java 2 Lines Nov 19, 2022 11:40:20 AM
src/main/java/com/example/ndcbbsrweb/controller/LoginPage.java java 43 Lines 3.6 KB Mar 24, 2023 12:54:56 PM
src/main/java/com/example/ndcbbsrweb/controller/Logout.java java 2 Lines Sep 27, 2022 12:45:22 PM
src/main/java/com/example/ndcbbsrweb/controller/NdcTeamController.java java 12 Lines 1.3 KB May 17, 2022 12:37:52 PM
src/main/java/com/example/ndcbbsrweb/controller/ObjStoreConfig.java java 35 Lines 3.6 KB Feb 3, 2023 4:26:04 PM
src/main/java/com/example/ndcbbsrweb/controller/ParichayHelper.java java 28 Lines 2.8 KB Nov 19, 2022 11:42:42 AM
src/main/java/com/example/ndcbbsrweb/controller/TokenAuth.java java 40 Lines 4 KB Mar 23, 2023 3:57:14 PM
src/main/java/com/example/ndcbbsrweb/controller/TransactionFilter.java java 13 Lines 1.7 KB Jan 30, 2023 12:29:50 PM
src/main/java/com/example/ndcbbsrweb/controller/UnusedMethods.java java 14 Lines Feb 1, 2023 12:32:28 PM
src/main/java/com/example/ndcbbsrweb/dao/BannerImageRepository.java java May 12, 2022 1:27:42 PM
src/main/java/com/example/ndcbbsrweb/dao/ContactUSRepository.java java May 12, 2022 1:27:42 PM
src/main/java/com/example/ndcbbsrweb/dao/FeedbackRepository.java java Jun 2, 2022 4:54:40 PM
src/main/java/com/example/ndcbbsrweb/dao/Feedback_typeRepository.java java Jun 3, 2022 12:52:56 PM
src/main/java/com/example/ndcbbsrweb/dao/HighlightsRepository.java java May 12, 2022 1:27:42 PM
src/main/java/com/example/ndcbbsrweb/dao/IptableRepository.java java Nov 19, 2022 11:42:54 AM
src/main/java/com/example/ndcbbsrweb/dao/KeytableRepository.java java Nov 5, 2022 12:43:10 PM
src/main/java/com/example/ndcbbsrweb/dao/LatestNewsRepository.java java May 12, 2022 1:27:42 PM
src/main/java/com/example/ndcbbsrweb/dao/NdcTeamRepository.java java May 12, 2022 1:27:42 PM
src/main/java/com/example/ndcbbsrweb/dao/PortalRepository.java java Mar 23, 2023 3:58:00 PM
src/main/java/com/example/ndcbbsrweb/dao/PricingDao.java java May 12, 2022 1:27:42 PM
src/main/java/com/example/ndcbbsrweb/dao/ServicesRepository.java java May 12, 2022 1:27:42 PM
src/main/java/com/example/ndcbbsrweb/dao/TenderRepository.java java May 12, 2022 1:27:42 PM
src/main/java/com/example/ndcbbsrweb/dao/UserdetailsRepository.java java Jul 15, 2022 12:55:18 PM
src/main/java/com/example/ndcbbsrweb/dao/Usrdao.java java Aug 10, 2022 3:17:36 PM
src/main/java/com/example/ndcbbsrweb/entity/Banner.java java 12 Lines 1.2 KB Feb 28, 2023 10:31:28 AM
src/main/java/com/example/ndcbbsrweb/entity/ContactUS.java java 18 Lines 1.7 KB Feb 28, 2023 10:32:10 AM
src/main/java/com/example/ndcbbsrweb/entity/Feedback.java java 18 Lines 1.8 KB Nov 18, 2022 5:33:40 PM
src/main/java/com/example/ndcbbsrweb/entity/FeedbackModal.java java 1 Lines Jun 3, 2022 12:50:24 PM
src/main/java/com/example/ndcbbsrweb/entity/Feedback_type.java java 7 Lines Jun 3, 2022 3:51:18 PM

src/main/java/com/example/ndcbbsrweb/entity/HighLights.java java 12 Lines 1.2 KB Nov 18, 2022 5:33:40 PM
src/main/java/com/example/ndcbbsrweb/entity/HomePageModal.java java 1 Lines May 12, 2022 1:27:42 PM
src/main/java/com/example/ndcbbsrweb/entity/Iptable.java java 13 Lines 1.2 KB Nov 18, 2022 5:34:14 PM
src/main/java/com/example/ndcbbsrweb/entity/Keytable.java java 9 Lines Nov 19, 2022 11:43:12 AM
src/main/java/com/example/ndcbbsrweb/entity/LatestNews.java java 15 Lines 1.7 KB Feb 28, 2023 10:33:10 AM
src/main/java/com/example/ndcbbsrweb/entity/Ndcteam.java java 15 Lines 1.5 KB Feb 28, 2023 10:30:48 AM
src/main/java/com/example/ndcbbsrweb/entity/Portal.java java 15 Lines 1.8 KB Mar 23, 2023 3:58:28 PM
src/main/java/com/example/ndcbbsrweb/entity/Pricing.java java 18 Lines 1.8 KB Feb 28, 2023 10:53:14 AM
src/main/java/com/example/ndcbbsrweb/entity/Services.java java 1 Lines May 12, 2022 1:27:42 PM
src/main/java/com/example/ndcbbsrweb/entity/TenderAndNotification.java java 15 Lines 1.7 KB Feb 28, 2023 10:53:14 AM
src/main/java/com/example/ndcbbsrweb/entity/Userdetails.java java 23 Lines 1.9 KB Nov 19, 2022 11:43:20 AM
src/main/java/com/example/ndcbbsrweb/entity/Usr.java java 15 Lines 1.5 KB Nov 18, 2022 5:37:34 PM
src/main/java/com/example/ndcbbsrweb/modal/BannerModal.java java 9 Lines Mar 23, 2023 3:46:22 PM
src/main/java/com/example/ndcbbsrweb/modal/ContactUSModal.java java 13 Lines Mar 23, 2023 3:46:22 PM
src/main/java/com/example/ndcbbsrweb/modal/FeedbackModal.java java 13 Lines 1.1 KB Mar 23, 2023 3:46:22 PM
src/main/java/com/example/ndcbbsrweb/modal/LatestNewsModal.java java 15 Lines 1 KB Mar 23, 2023 3:46:22 PM
src/main/java/com/example/ndcbbsrweb/modal/PricingModal.java java 13 Lines Mar 23, 2023 3:46:22 PM
src/main/java/com/example/ndcbbsrweb/modal/TenderAndNotificationModal.java java 11 Lines Mar 23, 2023 3:46:22 PM
src/main/java/com/example/ndcbbsrweb/modal/teamModal.java java 11 Lines Mar 23, 2023 3:46:22 PM
src/main/java/com/example/ndcbbsrweb/service/NdcService.java java 3 KB Mar 23, 2023 3:59:10 PM
src/main/java/com/example/ndcbbsrweb/service/NdcServiceImpl.java java 92 Lines 9.9 KB Mar 24, 2023 12:18:20 PM
src/main/java/com/example/ndcbbsrweb/util/AESEncryption.java java 49 Lines 4.3 KB Mar 24, 2023 12:08:26 PM
src/main/java/com/example/ndcbbsrweb/util/AesCrypto.java java 30 Lines 3.7 KB Mar 24, 2023 4:01:08 PM
src/main/java/com/example/ndcbbsrweb/util/AesCryptobak.java java 37 Lines 3.5 KB Mar 24, 2023 3:40:36 PM
src/main/java/com/example/ndcbbsrweb/util/CheckImage.java java 9 Lines Jan 30, 2023 12:01:00 PM
src/main/java/com/example/ndcbbsrweb/util/MailAuthSMTP.java java 29 Lines 2.3 KB Mar 24, 2023 1:09:38 PM
src/main/java/com/example/ndcbbsrweb/util/UtkalUtil.java java 81 Lines 5.2 KB Mar 23, 2023 4:03:00 PM
src/main/resources/application.properties java_properties 2.2 KB Mar 24, 2023 12:32:14 PM
src/main/resources/log4j2.properties java_properties Jan 7, 2023 3:49:24 PM
src/main/resources/static/index.html html Nov 3, 2022 2:45:28 PM
src/main/resources/static/js/clock.js typescript 17 Lines May 12, 2022 3:13:46 PM
src/main/resources/static/js/popper.min.js typescript 1 Lines 20.5 KB May 12, 2022 3:13:46 PM
src/main/resources/static/js/sha256.js typescript 73 Lines 4.2 KB May 12, 2022 3:13:46 PM
src/main/resources/static/js/zoomer.js typescript 184 Lines 10.1 KB May 12, 2022 3:13:46 PM
src/main/resources/templates/aboutus.html html 4.6 KB May 12, 2022 1:28:30 PM
src/main/resources/templates/admin/Admin-Home.html html 2.8 KB Sep 27, 2022 10:34:36 AM
src/main/resources/templates/admin/addBanner.html html 1.1 KB Sep 14, 2022 6:19:34 PM
src/main/resources/templates/admin/addGallery.html html 1.1 KB Sep 14, 2022 6:19:32 PM
src/main/resources/templates/admin/addHighlight.html html 6 Lines 1.8 KB Sep 14, 2022 6:19:42 PM
src/main/resources/templates/admin/addNews.html html 1.3 KB Sep 14, 2022 6:19:48 PM
src/main/resources/templates/admin/addPricing.html html 1.4 KB Sep 14, 2022 6:19:56 PM
src/main/resources/templates/admin/addTeam.html html 1.4 KB Sep 14, 2022 6:20:04 PM
src/main/resources/templates/admin/addTender.html html 1.3 KB Sep 14, 2022 6:20:14 PM
src/main/resources/templates/admin/bannerView.html html 3 Lines 2.2 KB Sep 15, 2022 1:07:24 PM
src/main/resources/templates/admin/contactus.html html 5.6 KB Sep 14, 2022 6:20:30 PM
src/main/resources/templates/admin/editNews.html html 1.3 KB Sep 14, 2022 6:20:40 PM
src/main/resources/templates/admin/editTeam.html html 1.4 KB Sep 14, 2022 6:20:48 PM
src/main/resources/templates/admin/editcontact.html html 1.4 KB Sep 14, 2022 6:20:36 PM
src/main/resources/templates/admin/ipgetter.html html Nov 10, 2022 3:53:06 PM
src/main/resources/templates/admin/login.html html 1.2 KB Jun 29, 2022 11:55:26 AM
src/main/resources/templates/admin/ndc_home.html html 1.2 KB Sep 27, 2022 11:09:34 AM

src/main/resources/templates/admin/other_home.html html 1.2 KB Sep 28, 2022 12:05:44 PM
src/main/resources/templates/admin/portals.html html 2.2 KB Oct 13, 2022 4:29:52 PM
src/main/resources/templates/admin/teamView.html html 3 Lines 2.9 KB Sep 15, 2022 1:30:46 PM
src/main/resources/templates/admin/viewGallery.html html 3 Lines 1.8 KB Sep 14, 2022 6:21:16 PM
src/main/resources/templates/admin/viewHighlights.html html 3 Lines 2.5 KB Sep 14, 2022 6:21:22 PM
src/main/resources/templates/admin/viewNews.html html 3 Lines 2.5 KB Sep 14, 2022 6:21:28 PM
src/main/resources/templates/admin/viewPricing.html html 3 Lines 2.8 KB Sep 14, 2022 6:21:34 PM
src/main/resources/templates/admin/viewTender.html html 3 Lines 2.6 KB Sep 14, 2022 6:21:40 PM
src/main/resources/templates/basictemplate.html html May 12, 2022 1:28:30 PM
src/main/resources/templates/colocation.html html 7.8 KB May 12, 2022 1:28:30 PM
src/main/resources/templates/contactus.html html 6 KB May 12, 2022 1:28:30 PM
src/main/resources/templates/error.html html Jul 14, 2022 9:54:26 AM
src/main/resources/templates/error/400.html html Jan 5, 2023 1:01:06 PM
src/main/resources/templates/error/404.html html Nov 17, 2022 3:32:56 PM
src/main/resources/templates/error/500.html html Nov 17, 2022 3:34:22 PM
src/main/resources/templates/error/error.html html Mar 24, 2023 4:49:46 PM
src/main/resources/templates/feedback.html html 1.1 KB Sep 27, 2022 5:57:08 PM
src/main/resources/templates/gallery.html html 1.7 KB Sep 13, 2022 5:57:30 PM
src/main/resources/templates/highlights.html html Sep 14, 2022 12:21:08 PM
src/main/resources/templates/includes/addEditTeamView.html html 1.1 KB May 12, 2022 1:28:30 PM
src/main/resources/templates/includes/adminheader.html html 3.1 KB Sep 27, 2022 10:44:40 AM
src/main/resources/templates/includes/footer.html html 6.4 KB May 12, 2022 1:28:30 PM
src/main/resources/templates/includes/header.html html 4.7 KB Jul 15, 2022 11:30:10 AM
src/main/resources/templates/includes/innerBanner.html html May 12, 2022 1:28:30 PM
src/main/resources/templates/includes/otheruserheader.html html 3 KB Sep 28, 2022 12:02:28 PM
src/main/resources/templates/index.html html 10.3 KB Sep 13, 2022 5:48:30 PM
src/main/resources/templates/list-team.html html 1.4 KB May 12, 2022 1:28:30 PM
src/main/resources/templates/pricing.html html 1.3 KB May 12, 2022 1:28:30 PM
src/main/resources/templates/services.html html 13 Lines 2.8 KB May 17, 2022 1:05:52 PM
src/main/resources/templates/welcome.html html May 12, 2022 1:23:24 PM
src/main/webapp/400.html html Jan 5, 2023 1:00:32 PM
src/main/webapp/404.html html Nov 17, 2022 2:28:20 PM
src/main/webapp/error.html html Jul 12, 2022 6:53:00 PM
src/main/webapp/errorpage.html html Jul 14, 2022 9:53:58 AM
src/main/webapp/homeip.html html Nov 10, 2022 12:49:56 PM
src/main/webapp/index.html html Nov 3, 2022 1:11:30 PM
src/main/webapp/ipgetter.html html Nov 10, 2022 12:28:12 PM
src/main/webapp/ndc_official.html html Sep 27, 2022 10:25:48 AM
src/main/webapp/unauth.html html Jul 12, 2022 3:25:38 PM
src/test/java/com/example/ndcbbsrweb/NdcbbsrwebApplicationTests.java java 1 Lines May 12, 2022 7:41:32 AM
target/Ndcbbsrweb/400.html html Jan 5, 2023 1:00:32 PM
target/Ndcbbsrweb/404.html html Nov 17, 2022 2:28:20 PM
target/Ndcbbsrweb/WEB-INF/classes/application.properties java_properties 2.2 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/log4j2.properties java_properties Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/static/index.html html Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/static/js/clock.js typescript 17 Lines Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/static/js/popper.min.js typescript 1 Lines 20.5 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/static/js/sha256.js typescript 73 Lines 4.2 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/static/js/zoomer.js typescript 184 Lines 10.1 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/aboutus.html html 4.6 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/admin/Admin-Home.html html 2.8 KB Mar 24, 2023 5:19:16 PM

target/Ndcbbsrweb/WEB-INF/classes/templates/admin/addBanner.html html 1.1 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/admin/addGallery.html html 1.1 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/admin/addHighlight.html html 6 Lines 1.8 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/admin/addNews.html html 1.3 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/admin/addPricing.html html 1.4 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/admin/addTeam.html html 1.4 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/admin/addTender.html html 1.3 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/admin/bannerView.html html 3 Lines 2.2 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/admin/contactus.html html 5.6 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/admin/editNews.html html 1.3 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/admin/editTeam.html html 1.4 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/admin/editcontact.html html 1.4 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/admin/ipgetter.html html Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/admin/login.html html 1.2 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/admin/ndc_home.html html 1.2 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/admin/other_home.html html 1.2 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/admin/portals.html html 2.2 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/admin/teamView.html html 3 Lines 2.9 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/admin/viewGallery.html html 3 Lines 1.8 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/admin/viewHighlights.html html 3 Lines 2.5 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/admin/viewNews.html html 3 Lines 2.5 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/admin/viewPricing.html html 3 Lines 2.8 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/admin/viewTender.html html 3 Lines 2.6 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/basictemplate.html html Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/colocation.html html 7.8 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/contactus.html html 6 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/error.html html Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/error/400.html html Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/error/404.html html Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/error/500.html html Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/error/error.html html Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/feedback.html html 1.1 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/gallery.html html 1.7 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/highlights.html html Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/includes/addEditTeamView.html html 1.1 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/includes/adminheader.html html 3.1 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/includes/footer.html html 6.4 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/includes/header.html html 4.7 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/includes/innerBanner.html html Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/includes/otheruserheader.html html 3 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/index.html html 10.3 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/list-team.html html 1.4 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/pricing.html html 1.3 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/services.html html 13 Lines 2.8 KB Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/WEB-INF/classes/templates/welcome.html html Mar 24, 2023 5:19:16 PM
target/Ndcbbsrweb/error.html html Jul 12, 2022 6:53:00 PM
target/Ndcbbsrweb/errorpage.html html Jul 14, 2022 9:53:58 AM
target/Ndcbbsrweb/homeip.html html Nov 10, 2022 12:49:56 PM
target/Ndcbbsrweb/index.html html Nov 3, 2022 1:11:30 PM
target/Ndcbbsrweb/ipgetter.html html Nov 10, 2022 12:28:12 PM
target/Ndcbbsrweb/ndc_official.html html Sep 27, 2022 10:25:48 AM

target/Ndcbbsrweb/unauth.html html Jul 12, 2022 3:25:38 PM
target/classes/application.properties java_properties 2.2 KB Mar 24, 2023 5:19:16 PM
target/classes/log4j2.properties java_properties Mar 24, 2023 5:19:16 PM
target/classes/static/index.html html Mar 24, 2023 5:19:16 PM
target/classes/static/js/clock.js typescript 17 Lines Mar 24, 2023 5:19:16 PM
target/classes/static/js/popper.min.js typescript 1 Lines 20.5 KB Mar 24, 2023 5:19:16 PM
target/classes/static/js/sha256.js typescript 73 Lines 4.2 KB Mar 24, 2023 5:19:16 PM
target/classes/static/js/zoomer.js typescript 184 Lines 10.1 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/aboutus.html html 4.6 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/admin/Admin-Home.html html 2.8 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/admin/addBanner.html html 1.1 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/admin/addGallery.html html 1.1 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/admin/addHighlight.html html 6 Lines 1.8 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/admin/addNews.html html 1.3 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/admin/addPricing.html html 1.4 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/admin/addTeam.html html 1.4 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/admin/addTender.html html 1.3 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/admin/bannerView.html html 3 Lines 2.2 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/admin/contactus.html html 5.6 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/admin/editNews.html html 1.3 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/admin/editTeam.html html 1.4 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/admin/editcontact.html html 1.4 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/admin/ipgetter.html html Mar 24, 2023 5:19:16 PM
target/classes/templates/admin/login.html html 1.2 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/admin/ndc_home.html html 1.2 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/admin/other_home.html html 1.2 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/admin/portals.html html 2.2 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/admin/teamView.html html 3 Lines 2.9 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/admin/viewGallery.html html 3 Lines 1.8 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/admin/viewHighlights.html html 3 Lines 2.5 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/admin/viewNews.html html 3 Lines 2.5 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/admin/viewPricing.html html 3 Lines 2.8 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/admin/viewTender.html html 3 Lines 2.6 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/basictemplate.html html Mar 24, 2023 5:19:16 PM
target/classes/templates/colocation.html html 7.8 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/contactus.html html 6 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/error.html html Mar 24, 2023 5:19:16 PM
target/classes/templates/error/400.html html Mar 24, 2023 5:19:16 PM
target/classes/templates/error/404.html html Mar 24, 2023 5:19:16 PM
target/classes/templates/error/500.html html Mar 24, 2023 5:19:16 PM
target/classes/templates/error/error.html html Mar 24, 2023 5:19:16 PM
target/classes/templates/feedback.html html 1.1 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/gallery.html html 1.7 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/highlights.html html Mar 24, 2023 5:19:16 PM
target/classes/templates/includes/addEditTeamView.html html 1.1 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/includes/adminheader.html html 3.1 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/includes/footer.html html 6.4 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/includes/header.html html 4.7 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/includes/innerBanner.html html Mar 24, 2023 5:19:16 PM
target/classes/templates/includes/otheruserheader.html html 3 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/index.html html 10.3 KB Mar 24, 2023 5:19:16 PM

target/classes/templates/list-team.html html 1.4 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/pricing.html html 1.3 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/services.html html 13 Lines 2.8 KB Mar 24, 2023 5:19:16 PM
target/classes/templates/welcome.html html Mar 24, 2023 5:19:16 PM
target/maven-archiver/pom.properties java_properties Mar 24, 2023 5:19:22 PM

Reference Elements

Classpath:

D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\.mvn\wrapper\maven-wrapper.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\HikariCP-4.0.3.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\activation-1.1.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\antlr-2.7.7.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\aspectjweaver-1.9.7.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\attoparser-2.0.5.RELEASE.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\aws-java-sdk-core-1.12.317.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\aws-java-sdk-kms-1.12.317.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\aws-java-sdk-s3-1.12.317.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\bcprov-jdk15on-1.47.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\byte-buddy-1.12.17.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\checker-qual-3.5.0.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\classmate-1.5.1.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\commons-beanutils-1.9.4.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\commons-codec-1.15.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\commons-collections-3.2.2.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\commons-digester-2.1.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\commons-io-2.11.0.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\commons-logging-1.2.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\commons-validator-1.7.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\hibernate-commons-annotations-5.1.2.Final.jar

D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\hibernate-core-5.6.11.Final.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\httpclient-4.5.13.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\httpcore-4.4.15.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\ion-java-1.0.2.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\istack-commons-runtime-3.0.12.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\jackson-annotations-2.13.4.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\jackson-core-2.13.4.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\jackson-databind-2.13.4.2.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\jackson-dataformat-cbor-2.13.4.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\jackson-datatype-jdk8-2.13.4.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\jackson-datatype-jsr310-2.13.4.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\jackson-module-parameter-names-2.13.4.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\jakarta.activation-1.2.2.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\jakarta.activation-api-1.2.2.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\jakarta.annotation-api-1.3.5.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\jakarta.persistence-api-2.2.3.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\jakarta.transaction-api-1.3.3.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\jakarta.xml.bind-api-2.3.3.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\jandex-2.4.2.Final.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\jaxb-runtime-2.3.6.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\jboss-logging-3.4.3.Final.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\jmespath-java-1.12.317.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\joda-time-2.8.1.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\json-simple-1.1.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\jul-to-slf4j-1.7.36.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\log4j-

api-2.17.2.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\log4j-to-slf4j-2.17.2.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\logback-classic-1.2.11.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\logback-core-1.2.11.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\mail-1.4.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\postgresql-42.5.0.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\slf4j-api-1.7.36.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\snakeyaml-1.30.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-aop-5.3.23.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-aspects-5.3.23.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-beans-5.3.23.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-boot-2.7.4.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-boot-autoconfigure-2.7.4.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-boot-starter-2.7.4.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-boot-starter-aop-2.7.4.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-boot-starter-data-jpa-2.7.4.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-boot-starter-jdbc-2.7.4.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-boot-starter-json-2.7.4.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-boot-starter-logging-2.7.4.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-boot-starter-security-2.7.4.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-boot-starter-thymeleaf-2.7.4.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-boot-starter-web-2.7.4.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-context-5.3.23.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-core-5.3.23.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-data-commons-2.7.3.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-data-jpa-2.7.3.jar

D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-expression-5.3.23.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-jcl-5.3.23.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-jdbc-5.3.23.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-orm-5.3.23.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-security-config-5.7.3.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-security-core-5.7.3.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-security-crypto-5.7.3.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-security-web-5.7.3.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-tx-5.3.23.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-web-5.3.23.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\spring-webmvc-5.3.23.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\thymeleaf-3.0.15.RELEASE.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\thymeleaf-extras-java8time-3.0.4.RELEASE.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\thymeleaf-spring5-3.0.15.RELEASE.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\txw2-2.3.6.jar
D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb\ndcbbsrweb\target\Ndcbbsrweb\WEB-INF\lib\unbescape-1.1.6.RELEASE.jar

Libdirs:

No libdirs specified during translation

Rulepacks

Valid Rulepacks:

Name: Fortify Secure Coding Rules, Community, Cloud
Version: 2021.4.0.0008
ID: 686C4B2F-0321-4025-B9F4-6E26094B4746
SKU: RUL13242

Name: Fortify Secure Coding Rules, Community, Universal
Version: 2021.4.0.0008
ID: 97b8b0e6-618b-47cf-a7fb-8636faea6b75
SKU: RUL13240

Name: Fortify Secure Coding Rules, Core, Android
Version: 2021.4.0.0008
ID: FF9890E6-D119-4EE8-A591-83DCF4CA6952
SKU: RUL13093

Name: Fortify Secure Coding Rules, Core, Annotations
Version: 2021.4.0.0008
ID: 14EE50EB-FA1C-4AE8-8B59-39F952E21E3B
SKU: RUL13078

Name: Fortify Secure Coding Rules, Core, Java
Version: 2021.4.0.0008
ID: 06A6CC97-8C3F-4E73-9093-3E74C64A2AAF
SKU: RUL13003

Name: Fortify Secure Coding Rules, Core, JavaScript
Version: 2021.4.0.0008
ID: BD292C4E-4216-4DB8-96C7-9B607BFD9584
SKU: RUL13059

Name: Fortify Secure Coding Rules, Core, Universal
Version: 2021.4.0.0008
ID: 88D39959-D322-499A-87F3-BC9E1193B07A
SKU: RUL13241

Name: Fortify Secure Coding Rules, Extended, Configuration
Version: 2021.4.0.0008
ID: CD6959FC-0C37-45BE-9637-BAA43C3A4D56
SKU: RUL13005

Name: Fortify Secure Coding Rules, Extended, Content
Version: 2021.4.0.0008
ID: 9C48678C-09B6-474D-B86D-97EE94D38F17
SKU: RUL13067

Name: Fortify Secure Coding Rules, Extended, Java
Version: 2021.4.0.0008
ID: AAAC0B10-79E7-4FE5-9921-F4903A79D317
SKU: RUL13007

Name: Fortify Secure Coding Rules, Extended, JavaScript
Version: 2021.4.0.0008
ID: C4D1969E-B734-47D3-87D4-73962C1D32E2
SKU: RUL13141

Name: Fortify Secure Coding Rules, Extended, JSP
Version: 2021.4.0.0008
ID: 00403342-15D0-48C9-8E67-4B1CFBDEFCD2
SKU: RUL13026

External Metadata:
Version: 2021.4.0.0008

Name: CWE
ID: 3ADB9EE4-5761-4289-8BD3-CBFCC593EBBC
The Common Weakness Enumeration (CWE), co-sponsored and maintained by MITRE, is international in scope and free for public use. CWE provides a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design.

Name: CWE Top 25 2019
ID: 7AF935C9-15AA-45B2-8EEC-0EAE4194ACDE
The 2019 CWE Top 25 Most Dangerous Software Errors lists the most widespread and critical weaknesses that can lead to serious vulnerabilities in software (as demonstrated by the National Vulnerability Database). These weaknesses occur frequently, are often easy to find, and easy to exploit. They are dangerous because they will frequently enable attackers to completely take over the software, steal data, or prevent the software from working at all. The list is the result of heuristic formula that the CWE Team used with a data-driven approach that leveraged the Common Vulnerabilities and Exposure (CVE), National Vulnerability Database (NVD), and Common Vulnerability Scoring System (CVSS). Due to the hierarchical nature of the CWE taxonomy, Fortify considers all CWE IDs which are children of a Top 25 entry, as included within the context of the entry due to the "CHILD-OF" relationship within the hierarchy. Exercise caution if using only this Top 25 list to prioritize auditing efforts because the software under analysis might not align with the assumptions of the heuristic used to define the Top 25. For example, many of these weaknesses are related to C-like languages and the software under analysis might not be within the C-family of languages - thus, many CWEs would not be in scope.

Name: CWE Top 25 2020
ID: E4C1DC51-45BD-469E-BA5D-BABF690F09F4
The 2020 CWE Top 25 Most Dangerous Software Errors lists the most widespread and critical weaknesses that can lead to serious vulnerabilities in software (as demonstrated by the National Vulnerability Database). These weaknesses occur frequently, are often easy to find, and easy to exploit. They are dangerous because they will frequently enable attackers to completely take over the software, steal data, or prevent the software from working at all. The list is the result of heuristic formula that the CWE Team used with a data-driven approach that leveraged the Common Vulnerabilities and Exposure (CVE), National Vulnerability Database (NVD), and Common Vulnerability Scoring System (CVSS). Due to the hierarchical nature of the CWE taxonomy, Fortify considers all CWE IDs which are children of a Top 25 entry, as included within the context of the entry due to the "CHILD-OF" relationship within the hierarchy. Exercise caution if using only this Top 25 list to prioritize auditing efforts because the software under analysis might not align with the assumptions of the heuristic used to define the Top 25. For example, many of these weaknesses are related to C-like languages and the software under analysis might not be within the C-family of languages - thus, many CWEs would not be in scope.

Name: CWE Top 25 2021
ID: FDA85EBD-56E5-4698-86FD-DD52E2F8F32B
The 2021 CWE Top 25 Most Dangerous Software Errors lists the most widespread and critical weaknesses that can lead to serious vulnerabilities in software (as demonstrated by the National Vulnerability Database). These weaknesses occur frequently, are often easy to find, and easy to exploit. They are dangerous because they will frequently enable attackers to completely take over the software, steal data, or prevent the software from working at all. The list is the result of heuristic formula that the CWE Team used with a data-driven approach that leveraged the Common Vulnerabilities and Exposure (CVE), National Vulnerability Database (NVD), and Common Vulnerability Scoring System (CVSS). Due to the hierarchical nature of the CWE taxonomy, Fortify considers all CWE IDs which are children of a Top 25 entry, as included within the context of the entry due to the "CHILD-OF" relationship within the hierarchy. Exercise caution if using only this Top 25 list to prioritize auditing efforts because the software under analysis might not align with the assumptions of the heuristic used to define the Top 25. For example, many of these weaknesses are related to C-like languages and the software under analysis might not be within the C-family of languages - thus, many CWEs would not be in scope.

Name: DISA CCI 2
ID: 7F037130-41E5-40F0-B653-7819A4B3E241
The purpose of a Defense Information Systems Agency (DISA) Control Correlation Identifier (CCI) is to provide a standard identifier for policy based requirements which connect high-level policy expressions and low-level technical implementations. Associated with each CCI is a description for each of the singular, actionable, statements compromising an information assurance (IA) control or IA best practice. Using CCI allows high-level policy framework security requirements to be decomposed and explicitly associated with low-level implementations, thus enabling the assessment of related compliance assessment results spanning heterogeneous technologies. The current IA controls and best practices associated with each CCI, that are specified in NIST SP 800-53 Revision 4, can be viewed using the DISA STIG Viewer.
The following table summarizes the number of issues identified across the different CCIs broken down by Fortify Priority Order. The status of a CCI is considered "In Place" when there are no issues reported for a given CCI.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, CCI-003187 is not considered "In Place". Similarly, if the project is missing a Micro Focus Fortify WebInspect scan, or the scan contains any critical findings, CCI-000366 and CCI-000256 are not considered "In Place".

Name: FISMA
ID: B40F9EE0-3824-4879-B9FE-7A789C89307C
The Federal Information Processing Standard (FIPS) 200 document is part of the official series of publications, issued by the National Institute of Standards and Technology (NIST), relating to standards and guidelines adopted and promulgated under the provisions of the Federal Information Security Management Act (FISMA). Specifically, FIPS Publication 200 specifies the "Minimum Security Requirements for Federal Information and Information Systems."

Name: GDPR
ID: 771C470C-9274-4580-8556-C12F5E4BEC51
The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. Going into effect on May 25, 2018, GDPR provides a framework for organizations on how to handle personal data. According to GDPR regulation personal data "means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." GDPR articles that pertain to application security and require businesses to protect personal data during design and development of its product and services are:

- Article 25, Data protection by design and by default - which requires "The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed."
- Article 32, Security of processing - which requires businesses to protect its systems and applications "from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data". This report may be used by organizations as a framework to help identify and protect personal data as it relates to application security.

Name: MISRA C 2012
ID: 555A3A66-A0E1-47AF-910C-3F19A6FB2506
Now in its third edition, the Motor Industry Software Reliability Association (MISRA) C Guidelines describe a subset of the C programming language in which there is reduced risk of introducing mistakes in critical systems. While the MISRA C Guidelines focus upon safety-related software development, a subset of the rules reflects security properties. Fortify interprets the MISRA C Guidelines under the context of security and provides correlation of security vulnerability categories to the rules defined by MISRA. Fortify provides these security focused detection mechanisms with the standard rulepacks, however, further support of the MISRA C Guidelines related to safety can be added through the use of custom rules. The results in this report can assist in the

creation of a compliance matrix for MISRA.

Name: MISRA C++ 2008
ID: 5D4B75A1-FC91-4B4B-BD4D-C81BBE9604FA
The Motor Industry Software Reliability Association (MISRA) C++ Guidelines describe a subset of the C++ programming language in which there is reduced risk of introducing mistakes in critical systems. While the MISRA C++ Guidelines focus upon safety-related software development, a subset of the rules reflects security properties. Fortify interprets the MISRA C++ Guidelines under the context of security and provides correlation of security vulnerability categories to the rules defined by MISRA. Fortify provides these security focused detection mechanisms with the standard rulepacks, however, further support of the MISRA C++ Guidelines related to safety can be added through the use of custom rules. The results in this report can assist in the creation of a compliance matrix for MISRA.

Name: NIST SP 800-53 Rev.4
ID: 1114583B-EA24-45BE-B7F8-B61201BACDD0
NIST Special Publication 800-53 Revision 4 provides a list of security and privacy controls designed to protect federal organizations and information systems from security threats. The following table summarizes the number of issues identified across the different controls and broken down by Fortify Priority Order.

Name: NIST SP 800-53 Rev.5
ID: 32434089-54F3-49F8-93F8-688B6B2FE8ED
NIST Special Publication 800-53 Revision 5 provides a list of security and privacy controls designed to protect federal organizations and information systems from security threats. The following table summarizes the number of issues identified across the different controls and broken down by Fortify Priority Order.

Name: OWASP ASVS 4.0
ID: 28083E33-760F-4A1A-AADA-738CC60082AD
The OWASP Application Security Verification Standard establishes a framework of security requirements and controls that focus on functional and non-functional security controls for the software development lifecycle based upon a community-driven effort. OWASP ASVS identifies several application security verification levels, with each level increasing depth:

<LI>ASVS Level 1 (L1): for low assurance levels and is completely penetration testable.</LI>
<LI>ASVS Level 2 (L2): for applications that contain sensitive data, which requires protection, and is the recommended level for most apps.</LI>
<LI>ASVS Level 3 (L3): for the most critical applications - applications that perform high value transactions, contain sensitive medical data, or any application that requires the highest level of trust.</LI> </UL>

Name: OWASP Mobile 2014
ID: EEE3F9E7-28D6-4456-8761-3DA56C36F4EE
The OWASP Mobile Top 10 Risks 2014 provides a powerful awareness document for mobile application security. The OWASP Mobile Top 10 represents a broad consensus about what the most critical mobile application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2004
ID: 771C470C-9274-4580-8556-C023E4D3ADB4
The OWASP Top Ten 2004 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2007

ID: 1EB1EC0E-74E6-49A0-BCE5-E6603802987A
The OWASP Top Ten 2007 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2010
ID: FDCECA5E-C2A8-4BE8-BB26-76A8ECD0ED59
The OWASP Top Ten 2010 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2013
ID: 1A2B4C7E-93B0-4502-878A-9BE40D2A25C4
The OWASP Top Ten 2013 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2017
ID: 3C6ECB67-BBD9-4259-A8DB-B49328927248
The OWASP Top Ten 2017 provides a powerful awareness document for web application security focused on informing the community about the consequences of the most common and most important web application security weaknesses. The OWASP Top Ten represents a broad agreement about what the most critical web application security flaws are with consensus being drawn from data collection and survey results. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2021
ID: 1887A283-3C0D-453C-AD10-0B451EAF096D0
The OWASP Top 10 2021 provides a powerful awareness document for web application security focused on informing the community about the consequences of the most common and most important web application security weaknesses. The OWASP Top 10 represents a broad agreement about what the most critical web application security flaws are with consensus drawn from data collection and survey results. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: PCI 1.1
ID: CBDB9D4D-FC20-4C04-AD58-575901CAB531
The Payment Card Industry (PCI) Data Security Standard (DSS) 1.1 compliance standard describes 12 requirements which are organized into 6 logically related groups, which are "control objectives". PCI DSS requirements are applicable if Primary Account Number (PAN) is stored, processed, or transmitted by the system.

Name: PCI 1.2
ID: 57940BDB-99F0-48BF-BF2E-CFC42BA035E5
Payment Card Industry Data Security Standard Version 1.2 description

Name: PCI 2.0
ID: 8970556D-7F9F-4EA7-8033-9DF39D68FF3E
The PCI DSS 2.0 compliance standard, particularly sections 6.3, 6.5, and 6.6, references the OWASP Top 10 vulnerability categories as the core categories that must be tested for and remediated. The following table summarizes the number of issues identified across the different PCI DSS requirements and broken down by Fortify Priority Order.

Name: PCI 3.0
ID: E2FB0D38-0192-4F03-8E01-FE2A12680CA3

The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.0. Fortify tests for 32 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.0 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI 3.1
ID: AC0D18CF-C1DA-47CF-9F1A-E8EC0A4A717E
The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.1. Fortify tests for 31 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.1 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI 3.2
ID: 4E8431F9-1BA1-41A8-BDBD-087D5826751A
The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.2. Fortify tests for 31 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.2 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI 3.2.1
ID: EADE255F-6561-4EFE-AD31-2914F6BFA329
The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.2.1. Fortify tests for 31 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.2.1 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI SSF 1.0
ID: 0F551543-AF0E-4334-BEDF-1DDCD5F4BF74
The following is a summary of the application security portions of the Secure Software Requirements and Assessment Procedures defined in the Payment Card Industry (PCI) Software Security Framework (SSF) v1.0. Fortify tests for 23 application security related control objectives across Control Objective sections 2, 3, 4, 5, 6, 7, 8, and A.2 of PCI SSF and reports whether each control objective is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI SSF 1.0 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI SSF 1.1
ID: 601EA2F3-5EDC-411C-818C-10DC5B29467D
The following is a summary of the application security portions of the Secure Software Requirements and Assessment Procedures defined in the Payment Card Industry (PCI) Software Security Framework (SSF) v1.1. Fortify tests for 31 application security related control objectives across Control Objective sections 2, 3, 4, 5, 6, 7, 8, A.2, B.2, and B.3 of PCI SSF and reports whether each control objective is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI SSF 1.1 compliance and is not intended

to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: SANS Top 25 2009
ID: 939EF193-507A-44E2-ABB7-C00B2168B6D8
The 2009 CWE/SANS Top 25 Programming Errors lists the most significant programming errors that can lead to serious software vulnerabilities. They occur frequently, are often easy to find, and easy to exploit. They are dangerous because they will frequently allow attackers to completely take over the software, steal data, or prevent the software from working at all. The list is the result of collaboration between the SANS Institute, MITRE, and many top software security experts.

Name: SANS Top 25 2010
ID: 72688795-4F7B-484C-88A6-D4757A6121CA
SANS Top 25 2010 Most Dangerous Software Errors provides an enumeration of the most widespread and critical errors, categorized by Common Weakness Enumeration (CWE) identifiers, that lead to serious vulnerabilities in software (http://cwe.mitre.org/). These software errors are often easy to find and exploit. The inherent danger in these errors is that they can allow an attacker to completely take over the software, steal data, or prevent the software from working at all.

Name: SANS Top 25 2011
ID: 92EB4481-1FD9-4165-8E16-F2DE6CB0BD63
SANS Top 25 2011 Most Dangerous Software Errors provides an enumeration of the most widespread and critical errors, categorized by Common Weakness Enumeration (CWE) identifiers, that lead to serious vulnerabilities in software (http://cwe.mitre.org/). These software errors are often easy to find and exploit. The inherent danger in these errors is that they can allow an attacker to completely take over the software, steal data, or prevent the software from working at all.

Name: STIG 3.1
ID: F2FA57EA-5AAA-4DDE-90A5-480BE65CE7E7
Security Technical Implementation Guide Version 3.1 description

Name: STIG 3.10
ID: 788A87FE-C9F9-4533-9095-0379A9B35B12
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 3.4
ID: 58E2C21D-C70F-4314-8994-B859E24CF855
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

<LI>CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.</LI>
<LI>CAT II: provide information that have a high potential of giving access to an intruder.</LI>
<LI>CAT III: provide information that potentially could lead to compromise.</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

Name: STIG 3.5
ID: DD18E81F-3507-41FA-9DFA-2A9A15B5479F
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

<LI>CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.</LI>
<LI>CAT II: provide information that have a high potential of giving access to an intruder.</LI>
<LI>CAT III: provide information that potentially could lead to compromise.</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

Name: STIG 3.6
ID: 000CA760-0FED-4374-8AA2-6FA3968A07B1
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

<LI>CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.</LI>
<LI>CAT II: provide information that have a high potential of giving access to an intruder.</LI>
<LI>CAT III: provide information that potentially could lead to compromise.</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 3.7
ID: E69C07C0-81D8-4B04-9233-F3E74167C3D2
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

<LI>CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.</LI>
<LI>CAT II: provide information that have a high potential of giving access to an intruder.</LI>
<LI>CAT III: provide information that potentially could lead to compromise.</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden

or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 3.9
ID: 1A9D736B-2D4A-49D1-88CA-DF464B40D732
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 4.1
ID: 95227C50-A9E4-4C9D-A8AF-FD98ABAE1F3C
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.10
ID: EF1FF442-1673-4CF1-B7C4-920F1A96A8150
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.11
ID: D9F6C005-1ED5-4685-8A69-79A87A1A9431
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.2
ID: 672C15F8-8822-4E05-8C9E-1A4BAAA7A373
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.3
ID: A0B313F0-29BD-430B-9E34-6D10F1178506
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.4
ID: ECEC5CA2-7ACA-4B70-BF44-3248B9C6F4F8
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.5
ID: E6010E0A-7F71-4388-B8B7-EE9A02143474
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.6
ID: EFB9B012-44D6-456D-B197-03D2FD7C7AD6
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>

<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.7
ID: B04A1E01-F1C1-48D3-A827-0F70872182D7
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.8
ID: E6805D9F-D5B5-4192-962C-46828FF68507
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.9
ID: 7B9F7B3B-07FC-4B61-99A1-70E3BB23A6A0
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>].

DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 5.1
ID: 1E2530B5-61C5-45D0-B479-79CB82DAFF83
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>].
DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: WASC 2.00
ID: 74f8081d-dd49-49da-880f-6830cebe9777
The Web Application Security Consortium (WASC) was created as a cooperative effort to standardize, clarify, and organize the threats to the security of a web site. Version 2.00 of their Threat Classification outlines the attacks and weaknesses that can commonly lead to a website being compromised.

Name: WASC 24 + 2
ID: 9DC61E7F-1A48-4711-BBFD-E9DFF537871F
The Web Application Security Consortium (WASC) was created as a cooperative effort to standardize, clarify, and organize the threats to the security of a web site.

Properties

WinForms.CollectionMutationMonitor.Label=WinFormsDataSource
awt.toolkit=sun.awt.windows.WToolkit
com.fortify.AuthenticationKey=C:\Users\sanjukta\AppData\Local/Fortify/config/tools
com.fortify.Core=C:\Fortify\Fortify_SCA_and_Apps_20.2.2\Core
com.fortify.InstallRoot=C:\Fortify\Fortify_SCA_and_Apps_20.2.2

com.fortify.InstallationUserName=sanjukta
com.fortify.SCAExecutablePath=C:/Fortify/Fortify_SCA_and_Apps_20.2.2/bin/sourceanalyzer.exe
com.fortify.TotalPhysicalMemory=16883982336
com.fortify.VS.RequireASPPrecompilation=true
com.fortify.WorkingDirectory=C:\Users\sanjukta\AppData\Local/Fortify
com.fortify.locale=en
com.fortify.log.console=true
com.fortify.sca.AddImpliedMethods=true
com.fortify.sca.AntCompilerClass=com.fortify.dev.ant.SCACompiler
com.fortify.sca.AppendLogFile=true
com.fortify.sca.AspnetTranslator=C:\Fortify\Fortify_SCA_and_Apps_20.2.2\Core/private-bin/sca/aspcodegen.exe
com.fortify.sca.BuildID=ndcbbsrweb
com.fortify.sca.BuildOptions=-pid-file C:\Users\sanjukta\AppData\Local\Temp\PID7211307274715415658.tmp -b ndcbbsrweb -machine-output -cp D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb/**/*.jar -source 1.8 D:\SCA\Year_2023\NDCBBSR\NDCBBSR_4th_Lvl_gupta\ndcbbsrweb
com.fortify.sca.BundleControlflowIssues=true
com.fortify.sca.BytecodePreview=true
com.fortify.sca.CollectPerformanceData=true
com.fortify.sca.CustomRulesDir=C:\Fortify\Fortify_SCA_and_Apps_20.2.2\Core\config\customrules
com.fortify.sca.DaemonCompilers=com.fortify.sca.util.compilers.GppCompiler,com.fortify.sca.util.compilers.GccCompiler,com.fortify.sca.util.compilers.AppleGppCompiler,com.fortify.sca.util.compilers.AppleGccCompiler,com.fortify.sca.util.compilers.MicrosoftCompiler,com.fortify.sca.util.compilers.MicrosoftLinker,com.fortify.sca.util.compilers.LdCompiler,com.fortify.sca.util.compilers.ArUtil,com.fortify.sca.util.compilers.SunCCompiler,com.fortify.sca.util.compilers.SunCppCompiler,com.fortify.sca.util.compilers.IntelCompiler,com.fortify.sca.util.compilers.ExternalCppAdapter,com.fortify.sca.util.compilers.ClangCompiler
com.fortify.sca.DeadCodeFilter=true
com.fortify.sca.DeadCodeIgnoreTrivialPredicates=true
com.fortify.sca.DefaultAnalyzers=semantic:dataflow:controlflow:nullptr:configuration:content:structural:buffer
com.fortify.sca.DefaultFileTypes=java,rb,erb,jsp,jspx,jspf,tag,tagx,tld,sql,cfm,php,phtml,ctp,pks,pkh,pkb,xml,config,Config,settings,properties,dll,exe,winmd,cs,vb,asax,ascx,ashx,asmx,aspx,master,Master,xaml,baml,cshtml,vbhtml,inc,asp,vbscript,js,jsx,ini,bas,cls,vbs,frm,ctl,html,htm,xsd,wsdd,xmi,py,cfml,cfc,abap,xhtml,cpx,xcfg,jsff,as,mxml,cbl,cscfg,csdef,wadcfg,wadcfgx,appxmanifest,wsdl,plist,bsp,ABAP,BSP,swift,page,trigger,scala,ts,tsx,conf,json,yaml,yml,go,kt,kts,Dockerfile,dockerfile
com.fortify.sca.DefaultJarsDirs=default_jars
com.fortify.sca.DefaultRulesDir=C:\Fortify\Fortify_SCA_and_Apps_20.2.2\Core\config\rules
com.fortify.sca.DisableCFRules=19EF0414-88CD-4882-82FC-BF3A89865666,4E28CEFE-1B94-4711-BF5A-EDA5D1B3E6BF,A2D33B21-FE55-4C53-86C6-2AB5BF343738,7F4CC818-7525-440B-9C68-02267A80179A,7F80BA1C-82E9-4F2A-BBB4-ADFDFB27B215,E650C773-2BB6-42AA-BC29-370AAF0C53ED
com.fortify.sca.DisableDeadCodeElimination=false
com.fortify.sca.DisableFunctionPointers=false
com.fortify.sca.DisableGlobals=false
com.fortify.sca.DisableInferredConstants=false
com.fortify.sca.DotnetDecompiler=C:\Fortify\Fortify_SCA_and_Apps_20.2.2\Core/private-bin/sca/dotnet-decompiler.exe
com.fortify.sca.DotnetTranslator=C:\Fortify\Fortify_SCA_and_Apps_20.2.2\Core/private-bin/sca/dotnet-translator.exe
com.fortify.sca.EnableInterproceduralConstantResolution=true
com.fortify.sca.EnableNestedWrappers=true
com.fortify.sca.EnableStructuralMatchCache=true
com.fortify.sca.EnableWrapperDetection=true
com.fortify.sca.FVDLDisableDescriptions=false
com.fortify.sca.FVDLDisableProgramData=false
com.fortify.sca.FVDLDisableSnippets=false
com.fortify.sca.FVDLStylesheet=C:\Fortify\Fortify_SCA_and_Apps_20.2.2\Core/resources/sca/fvdl2html.xsl
com.fortify.sca.GoTranslator=C:\Fortify\Fortify_SCA_and_Apps_20.2.2\Core/private-bin/sca/golang.exe

com.fortify.sca.IndirectCallGraphBuilders=WinFormsAdHocFunctionBuilder,VirtualCGBuilder,J2EEIndirectCGBuilder,JNICGBuilder,StoredProcedureResolver,JavaWSCGBuilder,StrutsCGBuilder,DotNetWSCGBuilder,SqlServerSPResolver,ASPCGBuilder,ScriptedCGBuilder,NewJspCustomTagCGBuilder,DotNetCABCGBuilder,StateInjectionCGBuilder,SqlServerSPResolver2,PHPLambdaResolver,JavaWebCGBuilder
com.fortify.sca.JVMArgs=-XX:SoftRefLRUPolicyMSPerMB=3000 -Xmx14736498688 -Xss16M
com.fortify.sca.JavaSourcepathSearch=true
com.fortify.sca.JdkVersion=1.8
com.fortify.sca.LogFile=C:\Users\sanjukta\AppData\Local\Fortify\sca20.2\log\sca
com.fortify.sca.LogFileDir=C:\Users\sanjukta\AppData\Local\Fortify\sca20.2\log
com.fortify.sca.LogFileExt=.log
com.fortify.sca.LogFileName=sca.log
com.fortify.sca.LogFileNameNoExt=sca
com.fortify.sca.LogFilePath=C:\Users\sanjukta\AppData\Local\Fortify\sca20.2\log\sca.log
com.fortify.sca.LogLevel=INFO
com.fortify.sca.LowSeverityCutoff=1.0
com.fortify.sca.MachineOutputMode=
com.fortify.sca.MultithreadedAnalysis=true
com.fortify.sca.NoNestedOutTagOutput=org.apache.taglibs.standard.tag.rt.core.RemoveTag,org.apache.taglibs.standard.tag.rt.core.SetTag
com.fortify.sca.OldVbNetExcludeFileTypes=vb,asax,ascx,ashx,asmx,aspx,xaml,cshtml,vbhtml
com.fortify.sca.PHPVersion=7.0
com.fortify.sca.PID=24144
com.fortify.sca.Phase0HigherOrder.Languages=python,ruby,swift,javascript,typescript
com.fortify.sca.Phase0HigherOrder.Level=1
com.fortify.sca.PidFile=C:\Users\sanjukta\AppData\Local\Temp\PID643306302670714532.tmp
com.fortify.sca.PrintPerformanceDataAfterScan=false
com.fortify.sca.ProjectRoot=C:\Users\sanjukta\AppData\Local/Fortify
com.fortify.sca.ProjectRoot=C:\Users\sanjukta\AppData\Local/Fortify
com.fortify.sca.PythonVersion=2
com.fortify.sca.Renderer=fpr
com.fortify.sca.RequireMapKeys=classrule
com.fortify.sca.ResultsFile=C:\Users\sanjukta\AppData\Local/Fortify\AWB-20.2.2\ndcbbsrweb\ndcbbsrweb.fpr
com.fortify.sca.ScaMSBuild=C:\Fortify\Fortify_SCA_and_Apps_20.2.2\Core/private-bin/sca/msbuild/current/bin/msbuild.exe
com.fortify.sca.SolverTimeout=15
com.fortify.sca.SqlLanguage=TSQL
com.fortify.sca.SuppressLowSeverity=true
com.fortify.sca.ThreadCount.NameTableLoading=1
com.fortify.sca.TypeInferenceFunctionTimeout=60
com.fortify.sca.TypeInferenceLanguages=javascript,typescript,python,ruby
com.fortify.sca.TypeInferencePhase0Timeout=300
com.fortify.sca.UnicodeInputFile=true
com.fortify.sca.UniversalBlacklist=.*yyparse.*
com.fortify.sca.alias.mode.csharp=fs
com.fortify.sca.alias.mode.javascript=fi
com.fortify.sca.alias.mode.scala=fi
com.fortify.sca.alias.mode.swift=fs
com.fortify.sca.alias.mode.typescript=fi
com.fortify.sca.alias.mode.vb=fs
com.fortify.sca.analyzer.controlflow.EnableLivenessOptimization=false
com.fortify.sca.analyzer.controlflow.EnableMachineFiltering=false
com.fortify.sca.analyzer.controlflow.EnableRefRuleOptimization=false

com.fortify.sca.analyzer.controlflow.EnableTimeOut=true
com.fortify.sca.compilers.ant=com.fortify.sca.util.compilers.AntAdapter
com.fortify.sca.compilers.ar=com.fortify.sca.util.compilers.ArUtil
com.fortify.sca.compilers.armcc=com.fortify.sca.util.compilers.ArmCcCompiler
com.fortify.sca.compilers.armcpp=com.fortify.sca.util.compilers.ArmCppCompiler
com.fortify.sca.compilers.c++=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.c89=com.fortify.sca.util.compilers.C89Compiler
com.fortify.sca.compilers.cc=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.cl=com.fortify.sca.util.compilers.MicrosoftCompiler
com.fortify.sca.compilers.clearmake=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.devenv=com.fortify.sca.util.compilers.DevenvAdapter
com.fortify.sca.compilers.fortify=com.fortify.sca.util.compilers.FortifyCompiler
com.fortify.sca.compilers.g++=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++-*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++2*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++3*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++4*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.gcc=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc-*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc2*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc3*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc4*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gmake=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.gradle=com.fortify.sca.util.compilers.GradleAdapter
com.fortify.sca.compilers.gradlew=com.fortify.sca.util.compilers.GradleAdapter
com.fortify.sca.compilers.icc=com.fortify.sca.util.compilers.IntelCompiler
com.fortify.sca.compilers.icl=com.fortify.sca.util.compilers.MicrosoftCompiler
com.fortify.sca.compilers.icpc=com.fortify.sca.util.compilers.IntelCompiler
com.fortify.sca.compilers.jam=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.javac=com.fortify.sca.util.compilers.JavacCompiler
com.fortify.sca.compilers.ld=com.fortify.sca.util.compilers.LdCompiler
com.fortify.sca.compilers.link=com.fortify.sca.util.compilers.MicrosoftLinker
com.fortify.sca.compilers.make=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.msbuild=com.fortify.sca.util.compilers.MSBuildAdapter
com.fortify.sca.compilers.msdev=com.fortify.sca.util.compilers.MSDevAdapter
com.fortify.sca.compilers.mvn=com.fortify.sca.util.compilers.MavenAdapter
com.fortify.sca.compilers.nmake=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.scalac=com.fortify.sca.util.compilers.ScalacCompiler
com.fortify.sca.compilers.tcc=com.fortify.sca.util.compilers.ArmCcCompiler
com.fortify.sca.compilers.tcpp=com.fortify.sca.util.compilers.ArmCppCompiler
com.fortify.sca.compilers.touchless=com.fortify.sca.util.compilers.FortifyCompiler
com.fortify.sca.compilers.xilink=com.fortify.sca.util.compilers.MicrosoftLinker
com.fortify.sca.cpfe.441.command=C:\Fortify\Fortify_SCA_and_Apps_20.2.2\Core/private-bin/sca/cpfe441.rfct
com.fortify.sca.cpfe.command=C:\Fortify\Fortify_SCA_and_Apps_20.2.2\Core/private-bin/sca/cpfe48.exe
com.fortify.sca.cpfe.file.option=--gen_c_file_name
com.fortify.sca.cpfe.options=--remove_unneeded_entities --suppress_vtbl -tused
com.fortify.sca.cpfe.options=--remove_unneeded_entities --suppress_vtbl -tused
com.fortify.sca.env.exesearchpath=C:\Fortify\Fortify_SCA_and_Apps_20.2.2\bin;C:\Program Files\Microsoft\jdk-11.0.12.7-hotspot\bin;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\WINDOWS\System32\WindowsPowerShell\v1.0\;C:\WINDOWS\System32\OpenSSH\;C:\Program Files\Microsoft SQL Server\150\Tools\Binn\;C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\170\Tools\Binn\;C:\Program

Files\dotnet\;C:\Fortify\Fortify_SCA_and_Apps_20.2.2\bin;C:\Users\sanjukta\AppData\Local\Microsoft\WindowsApps;;C:\Fortify\Fortify_SCA_and_Apps_20.2.2\bin\..\Core\lib
com.fortify.sca.fileextensions.ABAP=ABAP
com.fortify.sca.fileextensions.BSP=ABAP
com.fortify.sca.fileextensions.Config=XML
com.fortify.sca.fileextensions.Dockerfile=DOCKERFILE
com.fortify.sca.fileextensions.Master=ASPNET
com.fortify.sca.fileextensions.abap=ABAP
com.fortify.sca.fileextensions.appxmanifest=XML
com.fortify.sca.fileextensions.as=ACTIONSCRIPT
com.fortify.sca.fileextensions.asax=ASPNET
com.fortify.sca.fileextensions.ascx=ASPNET
com.fortify.sca.fileextensions.ashx=ASPNET
com.fortify.sca.fileextensions.asmx=ASPNET
com.fortify.sca.fileextensions.asp=ASP
com.fortify.sca.fileextensions.aspx=ASPNET
com.fortify.sca.fileextensions.axml=ASPNET
com.fortify.sca.fileextensions.baml=MSIL
com.fortify.sca.fileextensions.bas=VB6
com.fortify.sca.fileextensions.bsp=ABAP
com.fortify.sca.fileextensions.cbl=COBOL
com.fortify.sca.fileextensions.cfc=CFML
com.fortify.sca.fileextensions.cfm=CFML
com.fortify.sca.fileextensions.cfml=CFML
com.fortify.sca.fileextensions.cls=VB6
com.fortify.sca.fileextensions.conf=HOCON
com.fortify.sca.fileextensions.config=XML
com.fortify.sca.fileextensions.cpx=XML
com.fortify.sca.fileextensions.cs=CSHARP
com.fortify.sca.fileextensions.cscfg=XML
com.fortify.sca.fileextensions.csdef=XML
com.fortify.sca.fileextensions.cshtml=ASPNET
com.fortify.sca.fileextensions.ctl=VB6
com.fortify.sca.fileextensions.ctp=PHP
com.fortify.sca.fileextensions.dll=MSIL
com.fortify.sca.fileextensions.dockerfile=DOCKERFILE
com.fortify.sca.fileextensions.erb=RUBY_ERB
com.fortify.sca.fileextensions.exe=MSIL
com.fortify.sca.fileextensions.faces=JSPX
com.fortify.sca.fileextensions.frm=VB6
com.fortify.sca.fileextensions.go=GO
com.fortify.sca.fileextensions.htm=HTML
com.fortify.sca.fileextensions.html=HTML
com.fortify.sca.fileextensions.ini=JAVA_PROPERTIES
com.fortify.sca.fileextensions.java=JAVA
com.fortify.sca.fileextensions.js=TYPESCRIPT
com.fortify.sca.fileextensions.jsff=JSPX
com.fortify.sca.fileextensions.json=JSON
com.fortify.sca.fileextensions.jsp=JSP
com.fortify.sca.fileextensions.jspf=JSP
com.fortify.sca.fileextensions.jspx=JSPX

com.fortify.sca.fileextensions.jsx=TYPESCRIPT
com.fortify.sca.fileextensions.kt=KOTLIN
com.fortify.sca.fileextensions.kts=KOTLIN
com.fortify.sca.fileextensions.master=ASPNET
com.fortify.sca.fileextensions.mdl=MSIL
com.fortify.sca.fileextensions.mod=MSIL
com.fortify.sca.fileextensions.mxml=MXML
com.fortify.sca.fileextensions.page=VISUAL_FORCE
com.fortify.sca.fileextensions.php=PHP
com.fortify.sca.fileextensions.phtml=PHP
com.fortify.sca.fileextensions.pkb=PLSQL
com.fortify.sca.fileextensions.pkh=PLSQL
com.fortify.sca.fileextensions.pks=PLSQL
com.fortify.sca.fileextensions.plist=XML
com.fortify.sca.fileextensions.properties=JAVA_PROPERTIES
com.fortify.sca.fileextensions.py=PYTHON
com.fortify.sca.fileextensions.rb=RUBY
com.fortify.sca.fileextensions.scala=SCALA
com.fortify.sca.fileextensions.settings=XML
com.fortify.sca.fileextensions.sql=SQL
com.fortify.sca.fileextensions.swift=SWIFT
com.fortify.sca.fileextensions.tag=JSP
com.fortify.sca.fileextensions.tagx=JSP
com.fortify.sca.fileextensions.tld=TLD
com.fortify.sca.fileextensions.trigger=APEX_TRIGGER
com.fortify.sca.fileextensions.ts=TYPESCRIPT
com.fortify.sca.fileextensions.tsx=TYPESCRIPT
com.fortify.sca.fileextensions.vb=VB
com.fortify.sca.fileextensions.vbhtml=ASPNET
com.fortify.sca.fileextensions.vbs=VBSCRIPT
com.fortify.sca.fileextensions.vbscript=VBSCRIPT
com.fortify.sca.fileextensions.wadcfg=XML
com.fortify.sca.fileextensions.wadcfgx=XML
com.fortify.sca.fileextensions.winmd=MSIL
com.fortify.sca.fileextensions.wsdd=XML
com.fortify.sca.fileextensions.wsdl=XML
com.fortify.sca.fileextensions.xaml=ASPNET
com.fortify.sca.fileextensions.xcfg=XML
com.fortify.sca.fileextensions.xhtml=JSPX
com.fortify.sca.fileextensions.xmi=XML
com.fortify.sca.fileextensions.xml=XML
com.fortify.sca.fileextensions.xsd=XML
com.fortify.sca.fileextensions.yaml=YAML
com.fortify.sca.fileextensions.yml=YAML
com.fortify.sca.jsp.UseNativeParser=true
com.fortify.sca.parser.python.ignore.module.1=test.badsyntax_future3
com.fortify.sca.parser.python.ignore.module.2=test.badsyntax_future4
com.fortify.sca.parser.python.ignore.module.3=test.badsyntax_future5
com.fortify.sca.parser.python.ignore.module.4=test.badsyntax_future6
com.fortify.sca.parser.python.ignore.module.5=test.badsyntax_future7
com.fortify.sca.parser.python.ignore.module.6=test.badsyntax_future8

com.fortify.sca.parser.python.ignore.module.7=test.badsyntax_future9
com.fortify.sca.parser.python.ignore.module.8=test.badsyntax_nocaret
com.fortify.sca.skip.libraries.AngularJS=angular.js,angular.min.js,angular-animate.js,angular-aria.js,angular_1_router.js,angular-cookies.js,angular-message-format.js,angular-messages.js,angular-mocks.js,angular-parse-ext.js,angular-resource.js,angular-route.js,angular-sanitize.js,angular-touch.js
com.fortify.sca.skip.libraries.ES6=es6-shim.min.js,system-polyfills.js,shims_for_IE.js
com.fortify.sca.skip.libraries.jQuery=jquery.js,jquery.min.js,jquery-migrate.js,jquery-migrate.min.js,jquery-ui.js,jquery-ui.min.js,jquery.mobile.js,jquery.mobile.min.js,jquery.color.js,jquery.color.min.js,jquery.color.svg-names.js,jquery.color.svg-names.min.js,jquery.color.plus-names.js,jquery.color.plus-names.min.js,jquery.tools.min.js
com.fortify.sca.skip.libraries.javascript=bootstrap.js,bootstrap.min.js,typescript.js,typescriptServices.js
com.fortify.sca.skip.libraries.typescript=typescript.d.ts,typescriptServices.d.ts
com.fortify.search.defaultSyntaxVer=2
com.sun.management.jmxremote=true
dotnet.install.dir=C:\Windows\Microsoft.NET\Framework64\
dotnet.sdk.v11.install.dir=
dotnet.sdk.v20.install.dir=
dotnet.sdk.v3x.install.dir=
dotnet.v30.referenceAssemblies=
dotnet.v35.referenceAssemblies=
file.encoding=Cp1252
file.encoding.pkg=sun.io
file.separator=\
java.awt.graphicsenv=sun.awt.Win32GraphicsEnvironment
java.awt.headless=true
java.awt.printerjob=sun.awt.windows.WPrinterJob
java.class.path=C:\Fortify\Fortify_SCA_and_Apps_20.2.2\Core\lib\exe\sca-exe.jar
java.class.version=52.0
java.endorsed.dirs=C:\Fortify\Fortify_SCA_and_Apps_20.2.2\jre\lib\endorsed
java.ext.dirs=C:\Fortify\Fortify_SCA_and_Apps_20.2.2\jre\lib\ext;C:\WINDOWS\Sun\Java\lib\ext
java.home=C:\Fortify\Fortify_SCA_and_Apps_20.2.2\jre
java.io.tmpdir=C:\Users\sanjukta\AppData\Local\Temp\
java.library.path=C:\Fortify\Fortify_SCA_and_Apps_20.2.2\bin;C:\WINDOWS\Sun\Java\bin;C:\WINDOWS\system32;C:\WINDOWS;C:\Program Files\Microsoft\jdk-11.0.12.7-hotspot\bin;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\WINDOWS\System32\WindowsPowerShell\v1.0\;C:\WINDOWS\System32\OpenSSH\;C:\Program Files\Microsoft SQL Server\150\Tools\Binn\;C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\170\Tools\Binn\;C:\Program Files\dotnet\;C:\Fortify\Fortify_SCA_and_Apps_20.2.2\bin;C:\Users\sanjukta\AppData\Local\Microsoft\WindowsApps;;C:\Fortify\Fortify_SCA_and_Apps_20.2.2\bin\..\Core\lib;.
java.rmi.server.randomIDs=true
java.runtime.name=OpenJDK Runtime Environment
java.runtime.version=1.8.0_181-b02
java.specification.name=Java Platform API Specification
java.specification.vendor=Oracle Corporation
java.specification.version=1.8
java.vendor=Azul Systems, Inc.
java.vendor.url=http://www.azulsystems.com/
java.vendor.url.bug=http://www.azulsystems.com/support/
java.version=1.8.0_181
java.vm.info=mixed mode
java.vm.name=OpenJDK 64-Bit Server VM
java.vm.specification.name=Java Virtual Machine Specification

java.vm.specification.vendor=Oracle Corporation
java.vm.specification.version=1.8
java.vm.vendor=Azul Systems, Inc.
java.vm.version=25.181-b02
line.separator=

log4j.configurationFile=C:\Fortify\Fortify_SCA_and_Apps_20.2.2\Core\config\log4j2.xml
log4j.isThreadContextMapInheritable=true
max.file.path.length=255
os.arch=amd64
os.name=Windows 10
os.version=10.0
path.separator=;
stderr.isatty=false
stdout.isatty=false
sun.arch.data.model=64
sun.boot.class.path=C:\Fortify\Fortify_SCA_and_Apps_20.2.2\jre\lib\resources.jar;C:\Fortify\Fortify_SCA_and_Apps_20.2.2\jre\lib\rt.jar;C:\Fortify\Fortify_SCA_and_Apps_20.2.2\jre\lib\sunrsasign.jar;C:\Fortify\Fortify_SCA_and_Apps_20.2.2\jre\lib\jsse.jar;C:\Fortify\Fortify_SCA_and_Apps_20.2.2\jre\lib\jce.jar;C:\Fortify\Fortify_SCA_and_Apps_20.2.2\jre\lib\charsets.jar;C:\Fortify\Fortify_SCA_and_Apps_20.2.2\jre\lib\jfr.jar;C:\Fortify\Fortify_SCA_and_Apps_20.2.2\jre\classes
sun.boot.library.path=C:\Fortify\Fortify_SCA_and_Apps_20.2.2\jre\bin
sun.cpu.endian=little
sun.cpu.isalist=amd64
sun.desktop=windows
sun.io.unicode.encoding=UnicodeLittle
sun.java.command=sourceanalyzer -Djava.awt.headless=true -Dcom.sun.management.jmxremote=true -XX:SoftRefLRUPolicyMSPerMB=3000 -Dwin32.LocalAppdata=C:\Users\sanjukta\AppData\Local -Ddotnet.install.dir=C:\Windows\Microsoft.NET\Framework64\ -Ddotnet.sdk.v11.install.dir= -Ddotnet.sdk.v20.install.dir= -Ddotnet.sdk.v3x.install.dir= -Ddotnet.v30.referenceAssemblies= -Ddotnet.v35.referenceAssemblies= -Dcom.fortify.sca.env.exesearchpath=C:\Fortify\Fortify_SCA_and_Apps_20.2.2\bin;C:\Program Files\Microsoft\jdk-11.0.12.7-hotspot\bin;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;C:\WINDOWS\System32\WindowsPowerShell\v1.0\;C:\WINDOWS\System32\OpenSSH\;C:\Program Files\Microsoft SQL Server\150\Tools\Binn\;C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\170\Tools\Binn\;C:\Program Files\dotnet\;C:\Fortify\Fortify_SCA_and_Apps_20.2.2\bin;C:\Users\sanjukta\AppData\Local\Microsoft\WindowsApps;;C:\Fortify\Fortify_SCA_and_Apps_20.2.2\bin\..\Core\lib -Dcom.fortify.sca.ProjectRoot=C:\Users\sanjukta\AppData\Local/Fortify -Dstdout.isatty=false -Dstderr.isatty=false -Dcom.fortify.sca.PID=24144 -Xmx14736498688 -Dcom.fortify.TotalPhysicalMemory=16883982336 -Xss16M -Dcom.fortify.sca.JVMArgs=-XX:SoftRefLRUPolicyMSPerMB=3000 -Xmx14736498688 -Xss16M -Djava.class.path=C:\Fortify\Fortify_SCA_and_Apps_20.2.2\Core\lib\exe\sca-exe.jar -scan -pid-file C:\Users\sanjukta\AppData\Local\Temp\PID643306302670714532.tmp @C:\Users\sanjukta\AppData\Local\Fortify\AWB-20.2.2\ndcbbsrweb\ndcbbsrwebScan.txt
sun.jnu.encoding=Cp1252
sun.management.compiler=HotSpot 64-Bit Tiered Compilers
sun.os.patch.level=
user.country=US
user.dir=C:\Fortify\Fortify_SCA_and_Apps_20.2.2\bin
user.home=C:\Users\sanjukta
user.language=en
user.name=sanjukta
user.script=
user.timezone=Asia/Calcutta

user.variant=
win32.LocalAppdata=C:\Users\sanjukta\AppData\Local

Commandline Arguments

-scan
-pid-file
C:\Users\sanjukta\AppData\Local\Temp\PID643306302670714532.tmp
-b
ndcbbsrweb
-machine-output
-format
fpr
-f
C:\Users\sanjukta\AppData\Local/Fortify\AWB-20.2.2\ndcbbsrweb\ndcbbsrweb.fpr

Warnings

[12022] The class "javax.servlet.ServletContext" could not be found on the classpath, but it was found in the JAR file provided by Fortify in "C:\Fortify\Fortify_SCA_and_Apps_20.2.2\Core\default_jars\javax.servlet-api-3.0.1.jar" as a convenience. To ensure consistent translation behavior add the JAR file that contains "javax.servlet.ServletContext" to the classpath given to the translation step. Refer to the documentation about "default JARs" in the SCA User Guide for more information.
[13509]
[rulescript] [script: Spring_EL_resolution, version: 6.40] Spring_EL_resolution line 415: TypeError: Cannot call method "indexOf" of undefined
[rulescript] var pathindex = viewname.indexOf('{');
[rulescript] at Spring_EL_resolution:415

[1395]
File:D:/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/index.html, Message:Misplaced closing tag " " (line: 109, col: 8).
[1395]
File:D:/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/includes/header.html, Message:Misplaced closing tag "
" (line: 113, col: 10).
[1395] File:D:/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/includes/footer.html, Message:Misplaced closing tag "
" (line: 102, col: 11).
[1395] File:D:/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/includes/footer.html, Message:Misplaced closing tag "</aside>" (line: 104, col: 13).
[1395]
File:D:/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/aboutus.html, Message:Misplaced closing tag " " (line: 120, col: 7).
[1395]
File:D:/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/includes/footer.html, Message:Misplaced closing tag "
" (line: 102, col: 11).
[1395]
File:D:/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/includes/footer.html, Message:Misplaced closing tag "</aside>" (line: 104, col: 13).
[1395]
File:D:/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/aboutus.html, Message:Misplaced closing tag " " (line: 120, col: 7).
[1395] File:D:/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-

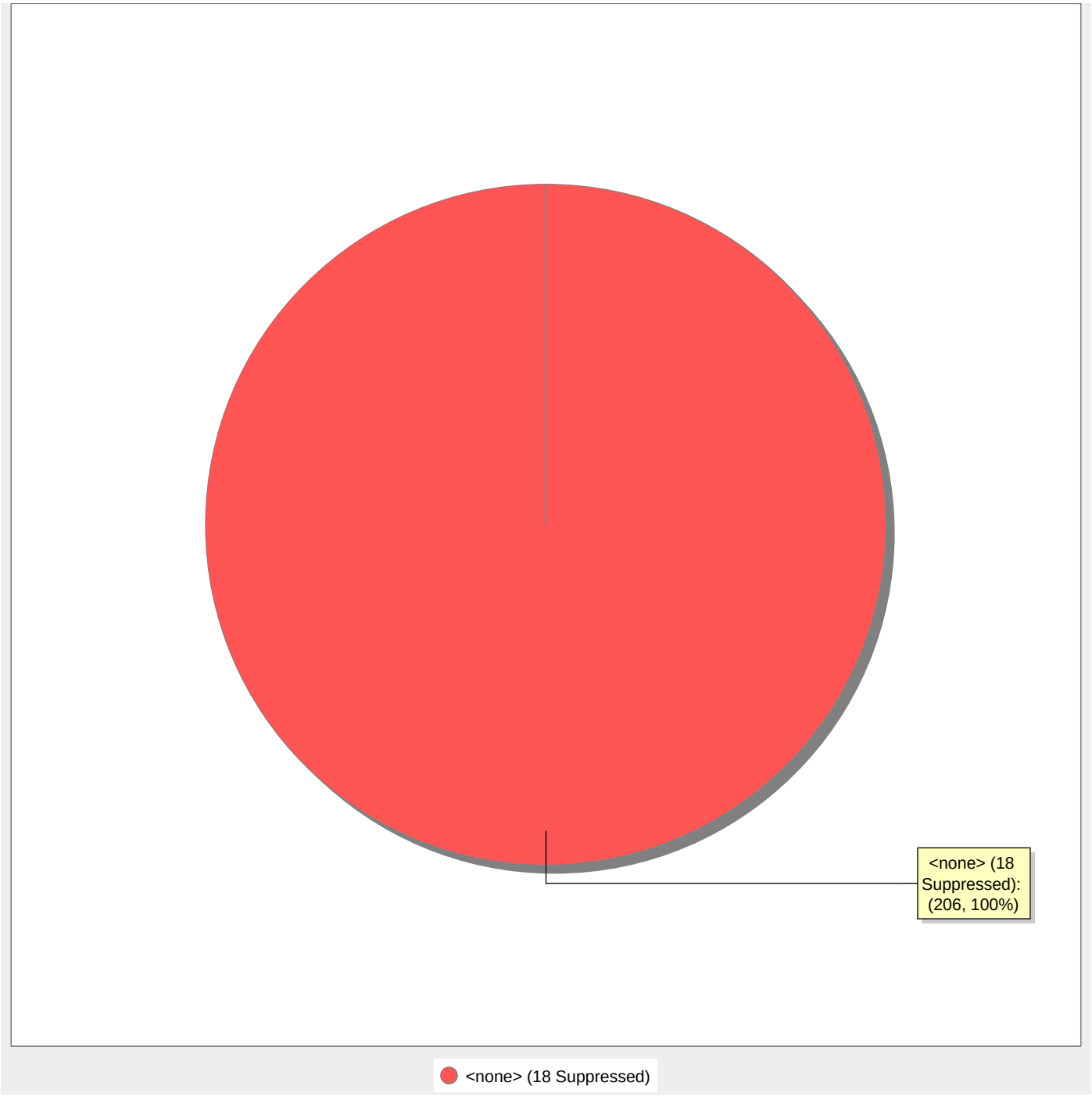
INF/classes/templates/aboutus.html, Message:Misplaced closing tag " " (line: 120, col: 7).
[1395] File:D:/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/index.html, Message:Misplaced closing tag " " (line: 109, col: 8).
[1395]
File:D:/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/includes/header.html, Message:Misplaced closing tag "
" (line: 113, col: 10).
[1395]
File:D:/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/classes/templates/index.html, Message:Misplaced closing tag " " (line: 109, col: 8).
[1395]
File:D:/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/includes/footer.html, Message:Misplaced closing tag "
" (line: 102, col: 11).
[1395]
File:D:/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/src/main/resources/templates/includes/footer.html, Message:Misplaced closing tag "</aside>" (line: 104, col: 13).
[1395] File:D:/SCA/Year_2023/NDCBBSR/NDCBBSR_4th_Lvl_gupta/ndcbbsrweb/ndcbbsrweb/target/Ndcbbsrweb/WEB-INF/classes/templates/includes/header.html, Message:Misplaced closing tag "
" (line: 113, col: 10).

Issue Count by Category

Issues by Category	
Trust Boundary Violation	52
Poor Error Handling: Overly Broad Catch	17
Access Control: Database (13 Suppressed)	16
System Information Leak	14
Path Manipulation	12
Mass Assignment: Insecure Binder Configuration	9
Poor Error Handling: Overly Broad Throws	9
Cookie Security: Cookie not Sent Over SSL	7
Often Misused: File Upload	6
Resource Injection	6
Dead Code: Unused Method	5
Cookie Security: HTTPOnly not Set	4
Cookie Security: Overly Broad Domain	4
Cookie Security: Overly Broad Path	4
Open Redirect	4
Cookie Security: Overly Broad Session Cookie Domain	3
Cookie Security: Overly Broad Session Cookie Path	3
Cross-Site Request Forgery (3 Suppressed)	3
Password Management: Password in Configuration File	3
Poor Error Handling: Empty Catch Block	3
Poor Style: Value Never Read	3
J2EE Bad Practices: Leftover Debug Code	2
Null Dereference	2
Password Management	2
Build Misconfiguration: External Maven Dependency Repository (1 Suppressed)	1
Code Correctness: Byte Array to String Conversion	1
Code Correctness: Erroneous String Compare	1
Header Manipulation (1 Suppressed)	1
Header Manipulation: SMTP	1
HTML5: Missing Content Security Policy	1
Key Management: Empty Encryption Key	1
Key Management: Hardcoded Encryption Key	1
Password Management: Password in Comment	1
Privacy Violation	1
Spring Security Misconfiguration: Lack of Fallback Check	1
Unchecked Return Value	1
Unreleased Resource: Streams	1

Issue Breakdown by Analysis

Issues by Analysis



New Issues

Issues by New Issue

The following issues have been discovered since the last scan.