16-09-22

Dear Interviewer, Greetings!!

Thank you for the opportunity to perform the technical assessment. It was really a great refreshment and able to learn few open source tool and techniques. Am indeed thankful for that and looking forward to hear from you soon..

Please find the below findings..

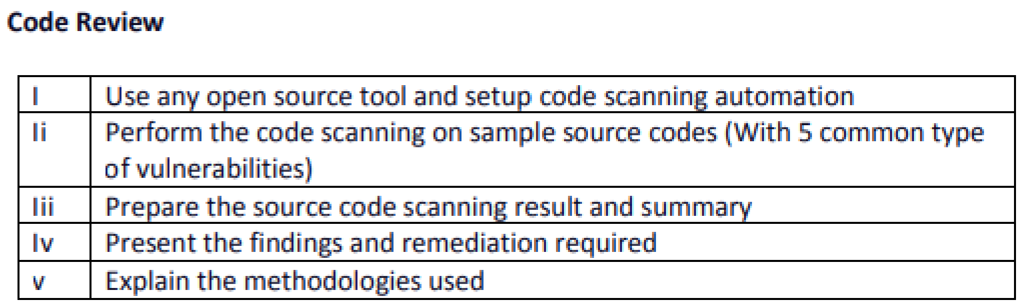
Sincerely,

[Rangarajan]

Assignment Details: 1

Technical Assignment Prepare the testing environment and choose 2 of the following assignments below that best match to your past experiences for one of the following Github repositories

- https://github.com/scalessec/Toast-Swift
- https://github.com/jogetworkflow/jw-community



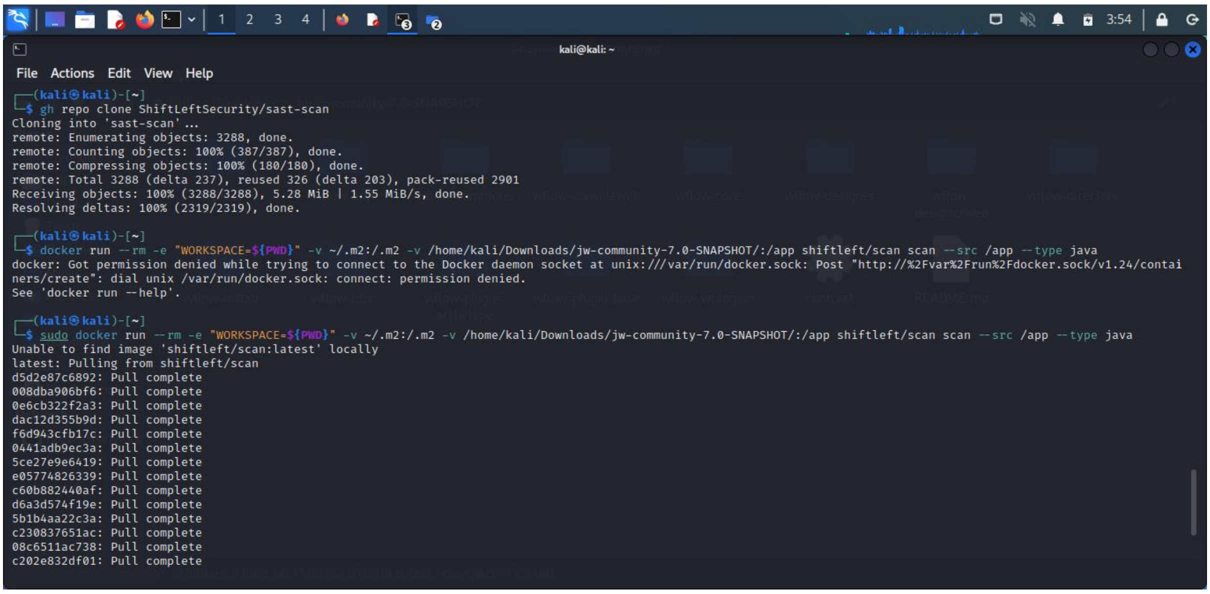
Code Review

I	Use any open source tool and setup code scanning automation
Ii	Perform the code scanning on sample source codes (With 5 common type of vulnerabilities)
Iii	Prepare the source code scanning result and summary
Iv	Present the findings and remediation required
v	Explain the methodologies used

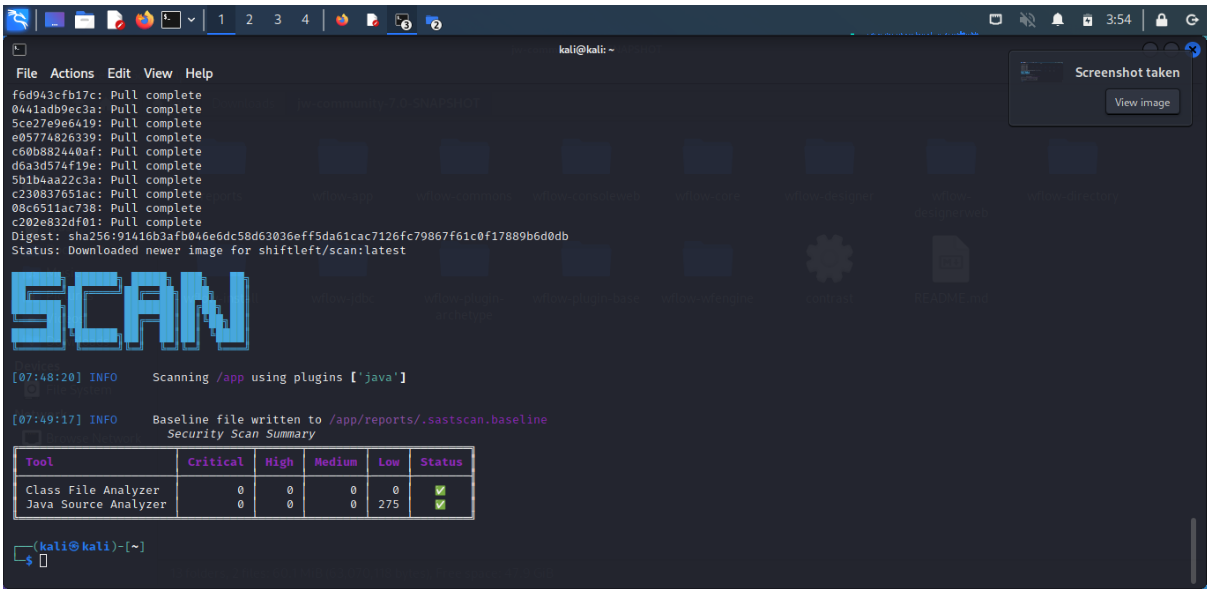
1. **Tool Name : ShiftLeftSecurity Scan**

ShiftLeft Scan lets you protect custom code with static analysis (SAST), secure open-source libraries (SCA), and employ hard-coded secrets detection and OSS license violation checks.

Platform: Kali VM.



```
┌──(kali㉿kali)-[~]
└─$ gh repo clone ShiftLeftSecurity/sast-scan
Cloning into 'sast-scan'...
remote: Enumerating objects: 3288, done.
remote: Counting objects: 100% (387/387), done.
remote: Compressing objects: 100% (180/180), done.
remote: Total 3288 (delta 237), reused 326 (delta 203), pack-reused 2901
Receiving objects: 100% (3288/3288), 5.28 MiB | 1.55 MiB/s, done.
Resolving deltas: 100% (2319/2319), done.

┌──(kali㉿kali)-[~]
└─$ docker run --rm -e "WORKSPACE=${PWD}" -v ~/.m2:/.m2 -v /home/kali/Downloads/jw-community-7.0-SNAPSHOT/:/app shiftleft/scan scan --src /app --type java
docker: Got permission denied while trying to connect to the Docker daemon socket at unix:///var/run/docker.sock: Post "http://%2Fvar%2Frun%2Fdocker.sock/v1.24/contai
ners/create": dial unix /var/run/docker.sock: connect: permission denied.
See 'docker run --help'.

┌──(kali㉿kali)-[~]
└─$ sudo docker run --rm -e "WORKSPACE=${PWD}" -v ~/.m2:/.m2 -v /home/kali/Downloads/jw-community-7.0-SNAPSHOT/:/app shiftleft/scan scan --src /app --type java
Unable to find image 'shiftleft/scan:latest' locally
latest: Pulling from shiftleft/scan
d5d2e87c6892: Pull complete
008dba906bf6: Pull complete
0e6cb322f2a3: Pull complete
dac12d355b9d: Pull complete
f6d943cfb17c: Pull complete
0441adb9ec3a: Pull complete
5ce27e9e6419: Pull complete
e05774826339: Pull complete
c60b882440af: Pull complete
d6a3d574f19e: Pull complete
5b1b4aa22c3a: Pull complete
c230837651ac: Pull complete
08c6511ac738: Pull complete
c202e832df01: Pull complete
```



```
f6d943cfb17c: Pull complete
0441adb9ec3a: Pull complete
5ce27e9e6419: Pull complete
e05774826339: Pull complete
c60b882440af: Pull complete
d6a3d574f19e: Pull complete
5b1b4aa22c3a: Pull complete
c230837651ac: Pull complete
08c6511ac738: Pull complete
c202e832df01: Pull complete
Digest: sha256:91416b3afb046e6dc58d63036eff5da61cac7126fc79867f61c0f17889b6d0db
Status: Downloaded newer image for shiftleft/scan:latest

SCAN

[07:48:20] INFO     Scanning /app using plugins ['java']

[07:49:17] INFO     Baseline file written to /app/reports/.sastscan.baseline
                      Security Scan Summary
╔══════════════════════╤══════════╤══════╤════════╤═════╤════════╗
║ Tool                 │ Critical │ High │ Medium │ Low │ Status ║
╟──────────────────────┼──────────┼──────┼────────┼─────┼────────╢
║ Class File Analyzer  │        0 │    0 │      0 │   0 │   ✅   ║
║ Java Source Analyzer │        0 │    0 │      0 │ 275 │   ✅   ║
╚══════════════════════╧══════════╧══════╧════════╧═════╧════════╝

┌──(kali㉿kali)-[~]
└─$ ▯
```

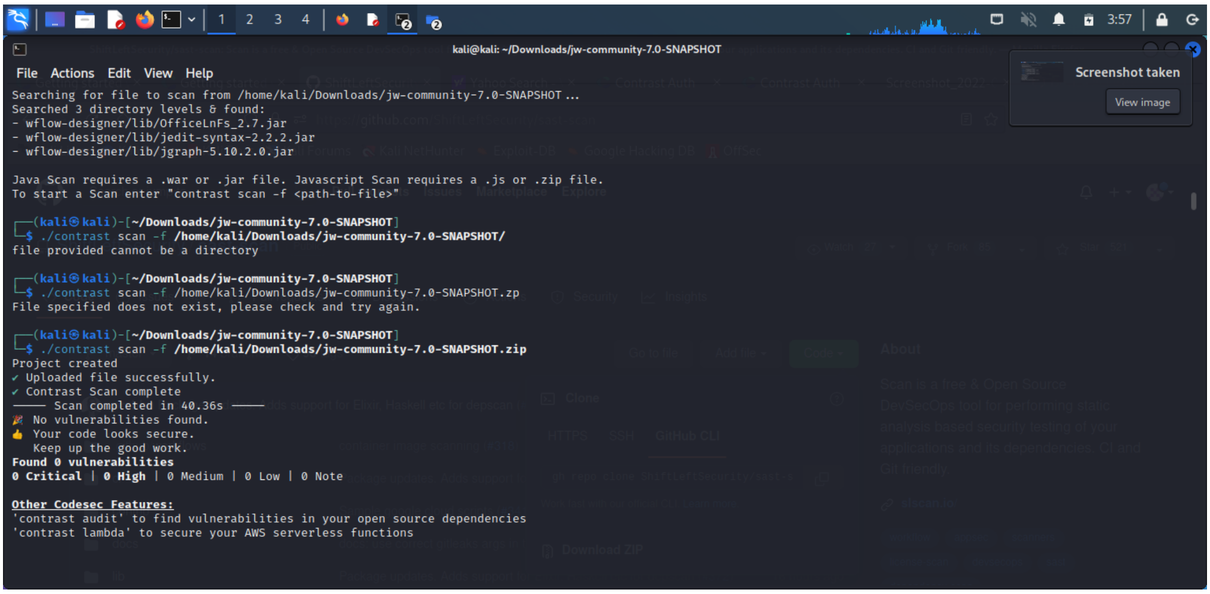
Summary of the finding s:

Tool	Critical	High	Medium	Low
Class File Analyzer	0	0	0	0
Java Source Analyzer	0	0	0	275

2. Tool Name: Contrast OSS

Contrast OSS works by installing an intelligent agent that equips the application with smart sensors to analyze code in real time from within the application

Plafform: Kali VM


kali@kali: ~/Downloads/jw-community-7.0-SNAPSHOT
File Actions Edit View Help
Screenshot taken
View image
3:57

```
Searching for file to scan from /home/kali/Downloads/jw-community-7.0-SNAPSHOT ...
Searched 3 directory levels & found:
- wflow-designer/lib/OfficeLnFs_2.7.jar
- wflow-designer/lib/jedit-syntax-2.2.2.jar
- wflow-designer/lib/jgraph-5.10.2.0.jar

Java Scan requires a .war or .jar file. Javascript Scan requires a .js or .zip file.
To start a Scan enter "contrast scan -f <path-to-file>"

┌──(kali㉿kali)-[~/Downloads/jw-community-7.0-SNAPSHOT]
└─$ ./contrast scan -f /home/kali/Downloads/jw-community-7.0-SNAPSHOT/
file provided cannot be a directory

┌──(kali㉿kali)-[~/Downloads/jw-community-7.0-SNAPSHOT]
└─$ ./contrast scan -f /home/kali/Downloads/jw-community-7.0-SNAPSHOT.zp
File specified does not exist, please check and try again.

┌──(kali㉿kali)-[~/Downloads/jw-community-7.0-SNAPSHOT]
└─$ ./contrast scan -f /home/kali/Downloads/jw-community-7.0-SNAPSHOT.zip
Project created
✔ Uploaded file successfully.
✔ Contrast Scan complete
───── Scan completed in 40.36s ─────
🎉 No vulnerabilities found.
👍 Your code looks secure.
   Keep up the good work.
Found 0 vulnerabilities
0 Critical | 0 High | 0 Medium | 0 Low | 0 Note

Other Codesec Features:
'contrast audit' to find vulnerabilities in your open source dependencies
'contrast lambda' to secure your AWS serverless functions
```

Summary of the finding s:

Critical	High	Medium	Low
0	0	0	0

Assignment Details: 2

Technical Assignment Prepare the testing environment and choose 2 of the following assignments below that best match to your past experiences for one of the following Github repositories

- https://github.com/scalessec/Toast-Swift
- https://github.com/jogetworkflow/jw-community

Security Scanning

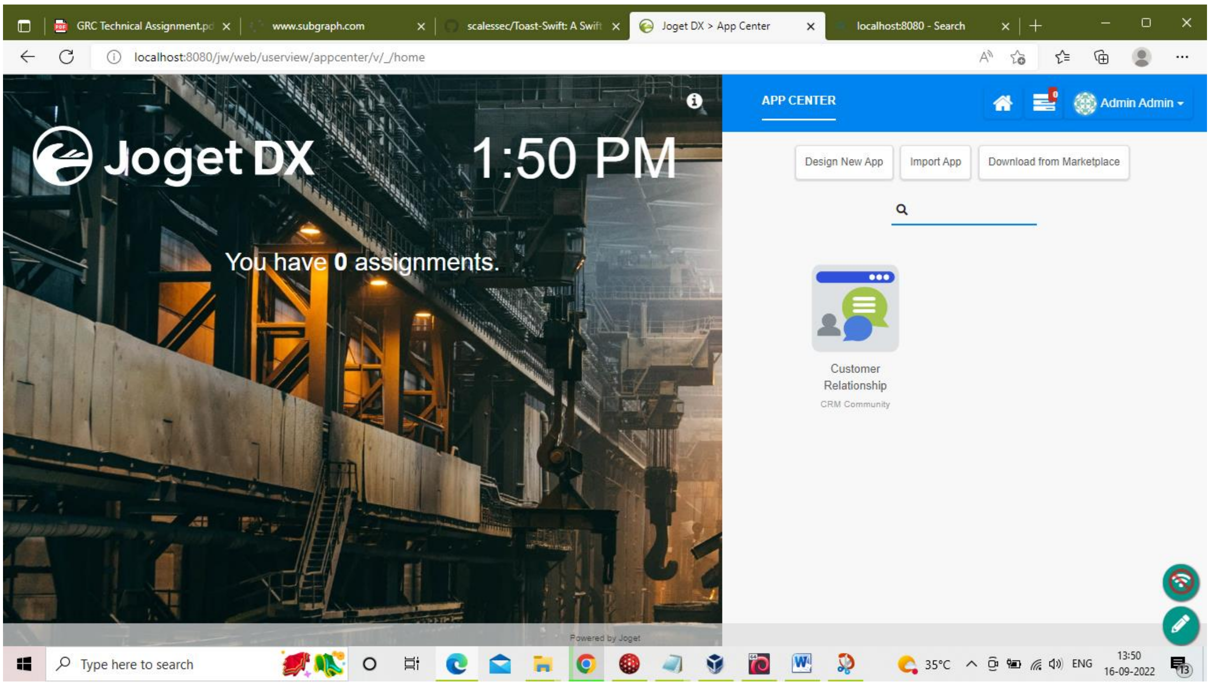
I	Use any open source tool and setup scanning
Ii	Perform the security scanning on a test machine (with 5 security loopholes)
Iii	Prepare the scanning result and summary
Iv	Present the findings and remediation required
v	Explain the methodologies used

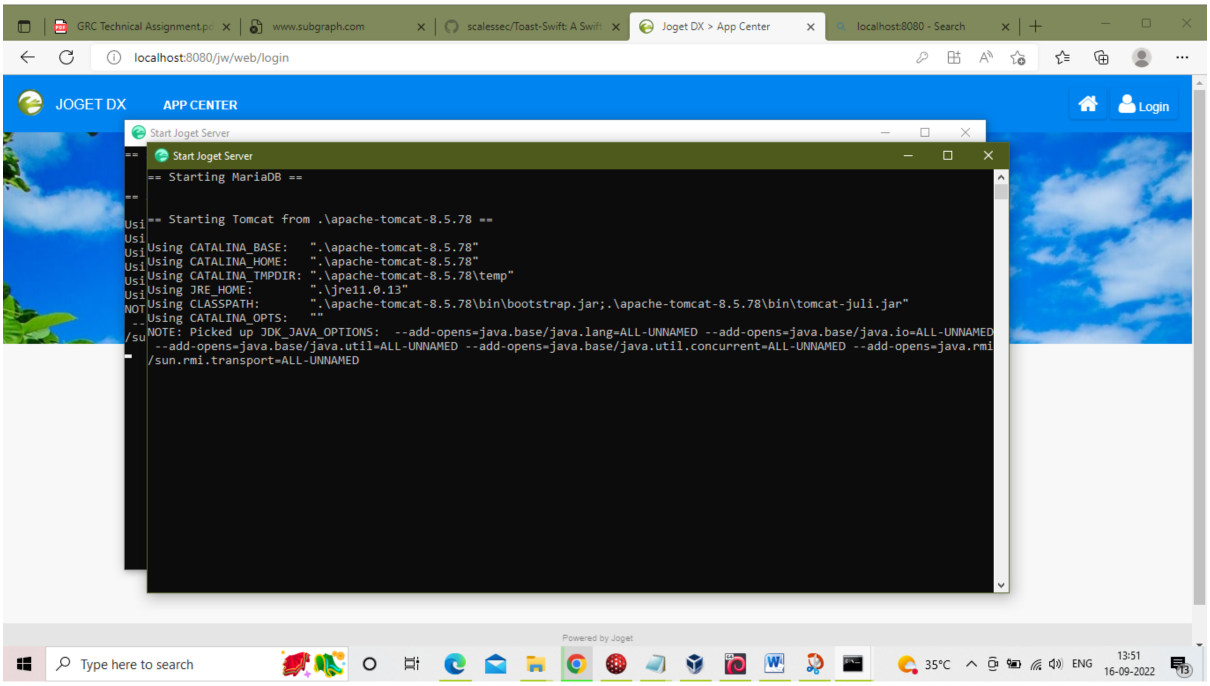
Tool Name : Vega

Vega, the Open Source Web Application Security Platform.

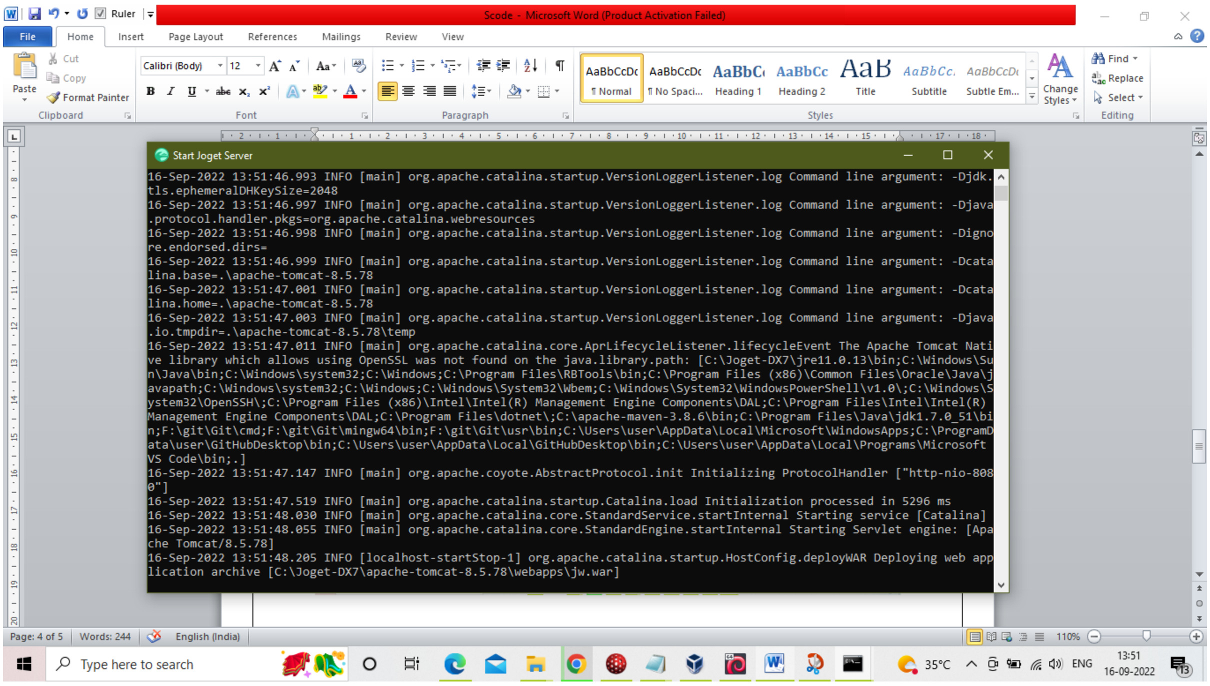
Platform : Windows 10 OS & Joget setup 7.0.32

Web Application:



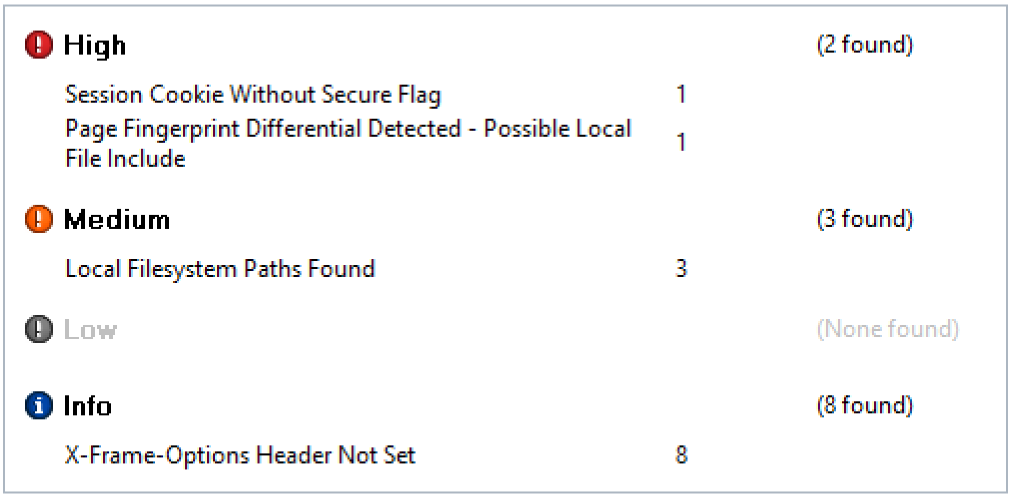


```
== Starting MariaDB ==


== Starting Tomcat from .\apache-tomcat-8.5.78 ==

Using CATALINA_BASE:   ".\apache-tomcat-8.5.78"
Using CATALINA_HOME:   ".\apache-tomcat-8.5.78"
Using CATALINA_TMPDIR: ".\apache-tomcat-8.5.78\temp"
Using JRE_HOME:        ".\jre11.0.13"
Using CLASSPATH:       ".\apache-tomcat-8.5.78\bin\bootstrap.jar;.\apache-tomcat-8.5.78\bin\tomcat-juli.jar"
Using CATALINA_OPTS:   ""
NOTE: Picked up JDK_JAVA_OPTIONS:  --add-opens=java.base/java.lang=ALL-UNNAMED --add-opens=java.base/java.io=ALL-UNNAMED
 --add-opens=java.base/java.util=ALL-UNNAMED --add-opens=java.base/java.util.concurrent=ALL-UNNAMED --add-opens=java.rmi
/sun.rmi.transport=ALL-UNNAMED
```



```
16-Sep-2022 13:51:46.993 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djdk.
tls.ephemeralDHKeySize=2048
16-Sep-2022 13:51:46.997 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djava
.protocol.handler.pkgs=org.apache.catalina.webresources
16-Sep-2022 13:51:46.998 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Digno
re.endorsed.dirs=
16-Sep-2022 13:51:46.999 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Dcata
lina.base=.\apache-tomcat-8.5.78
16-Sep-2022 13:51:47.001 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Dcata
lina.home=.\apache-tomcat-8.5.78
16-Sep-2022 13:51:47.003 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djava
.io.tmpdir=.\apache-tomcat-8.5.78\temp
16-Sep-2022 13:51:47.011 INFO [main] org.apache.catalina.core.AprLifecycleListener.lifecycleEvent The Apache Tomcat Nati
ve library which allows using OpenSSL was not found on the java.library.path: [C:\Joget-DX7\jre11.0.13\bin;C:\Windows\Su
n\Java\bin;C:\Windows\system32;C:\Windows;C:\Program Files\RBTools\bin;C:\Program Files (x86)\Common Files\Oracle\Java\j
avapath;C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;C:\Windows\System32\WindowsPowerShell\v1.0\;C:\Windows\S
ystem32\OpenSSH\;C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\DAL;C:\Program Files\Intel\Intel(R)
Management Engine Components\DAL;C:\Program Files\dotnet\;C:\apache-maven-3.8.6\bin;C:\Program Files\Java\jdk1.7.0_51\bi
n;F:\git\Git\cmd;F:\git\Git\mingw64\bin;F:\git\Git\usr\bin;C:\Users\user\AppData\Local\Microsoft\WindowsApps;C:\ProgramD
ata\user\GitHubDesktop\bin;C:\Users\user\AppData\Local\GitHubDesktop\bin;C:\Users\user\AppData\Local\Programs\Microsoft
VS Code\bin;.]
16-Sep-2022 13:51:47.147 INFO [main] org.apache.coyote.AbstractProtocol.init Initializing ProtocolHandler ["http-nio-808
0"]
16-Sep-2022 13:51:47.519 INFO [main] org.apache.catalina.startup.Catalina.load Initialization processed in 5296 ms
16-Sep-2022 13:51:48.030 INFO [main] org.apache.catalina.core.StandardService.startInternal Starting service [Catalina]
16-Sep-2022 13:51:48.055 INFO [main] org.apache.catalina.core.StandardEngine.startInternal Starting Servlet engine: [Apa
che Tomcat/8.5.78]
16-Sep-2022 13:51:48.205 INFO [localhost-startStop-1] org.apache.catalina.startup.HostConfig.deployWAR Deploying web app
lication archive [C:\Joget-DX7\apache-tomcat-8.5.78\webapps\jw.war]
```

Scan Alert Summary



High		(2 found)
Session Cookie Without Secure Flag	1	
Page Fingerprint Differential Detected - Possible Local File Include	1	
Medium		(3 found)
Local Filesystem Paths Found	3	
Low		(None found)
Info		(8 found)
X-Frame-Options Header Not Set	8	

Summary of the findings:

Critical	High	Medium	Low
0	2	3	0

DETAILS OF FINDINGS:

HIGH : 1

Classification	Error Message
Resource	**/jw/web/userview/appcenter/v/_/home**
Parameter	**_action**
Method	**GET**
Risk	**High**

REQUEST

GET /jw/web/userview/appcenter/v/_/home?_action=/./

RESOURCE CONTENT

```
   <!DOCTYPE html>
<html  lang="en">
```

```
    <head>
        <meta http-equiv="X-UA-Compatible" content="IE=edge"/>
<meta charset="utf-8" />
<meta  name="viewport"  content="width=device-width,  initial-
scale=1">
<meta name="msapplication-tap-highlight" content="no"/>
<meta name="theme-color" content="#0084F0"/>
<link rel="apple-touch-icon" hr...
```

IMPACT

- It has detected a different response fingerprint in relation to a local file include injection attempt.
- This may indicate a local file include vulnerability, though this is not confirmed.
- If this is due to a local file include vulnerability, exploitation of local file include vulnerabilities can allow attackers to gain unauthorized access to files, which may also aid in other attacks.
- Differing responses may also indicate the presence of a file enumeration vulnerability, which instead of allowing the attacker to gain access to file contents, may allow them to determine if files exist on the system.

REMEDIATION

- To prevent this type of vulnerability, the developer should canonicalize the path of any filesystem resource that has a path composed of externally-supplied input and then perform an authorization check prior to access.
- The realpath() library call will return the canonical path of the resource. It is implemented in PHP, Perl, and Python.
- For Ruby frameworks, File.expand_path can be used.
- GetFullPath() can be used on ASP.NET applications.
- getCanonicalPath() can be used in Java code.
- Additional protection against unauthorized access to filesystem resources can be obtained by using chroot() or similar mechanisms to limit filesystem access to the web application and http server process, although this can be difficult to manage.

REFERENCES

Some additional links with relevant information published by third-parties:

- Directory Traversal (Wikipedia)
- Path Traversal (OWASP)
- Avoiding Path Traversal (OWASP)

HIGH : 2

Classification	Information
Resource	**/jw/**
Risk	**High**

REQUEST

GET /jw/

RESOURCE CONTENT

```
JSESSIONID=E6DE9713FE07767DE2F649E3C4156332; Path=/jw; HttpOnly
```

IMPACT

- Cookies can be exposed to network eavesdroppers.
- Session cookies are authentication credentials; attackers who obtain them can get unauthorized access to affected web applications.

REMEDIATION

- When creating the cookie in the code, set the secure flag to true.

REFERENCES

Some additional links with relevant information published by third-parties:

- Secure Flag
- HttpOnly OWASP Reference

MEDIUM : 1

Classification	Information
Resource	**/jw/web/userview/appcenter/v/_/home**
Risk	Medium

REQUEST

GET /jw/web/userview/appcenter/v/_/home

RESOURCE CONTENT

```
/lib/material-design-iconic-font/fonts/Material-Design-Iconic-
Font.woff
```

IMPACT

- It has detected what may be absolute filesystem paths in scanned content.
- Disclosure of these paths reveals information about the filesystem layout.
- This information can be sensitive, its disclosure can increase the chances of success for other attacks.

REMEDIATION

- Absolute paths are often found in error output.
- Both the system administrators and developers should be made aware, as the problem may be due to an application error or server misconfiguration.
- Error output containing sensitive information such as absolute system paths should not be sent to remote clients on production servers.
- This output should be sent to another output stream, such as an error log.

REFERENCES

Some additional links with relevant information published by third-parties:

- Information Leakage (OWASP)

MEDIUM: 2

Classification	Information
Resource	**/jw/nosuchpage123**
Risk	Medium

REQUEST

GET /jw/nosuchpage123

RESOURCE CONTENT

```
/home/style.css
```

IMPACT

- It has detected what may be absolute filesystem paths in scanned content.
- Disclosure of these paths reveals information about the filesystem layout.
- This information can be sensitive, its disclosure can increase the chances of success for other attacks.

REMEDIATION

- Absolute paths are often found in error output.
- Both the system administrators and developers should be made aware, as the problem may be due to an application error or server misconfiguration.
- Error output containing sensitive information such as absolute system paths should not be sent to remote clients on production servers.
- This output should be sent to another output stream, such as an error log.

REFERENCES

Some additional links with relevant information published by third-parties:

- Information Leakage (OWASP)

MEDIUM: 3

Classification	Information
Resource	**/**
Risk	Medium

REQUEST

GET /

RESOURCE CONTENT

```
/apache/tomcat/tree/
```

IMPACT

- It has detected what may be absolute filesystem paths in scanned content.

- Disclosure of these paths reveals information about the filesystem layout.
- This information can be sensitive, its disclosure can increase the chances of success for other attacks.

REMEDIATION

- Absolute paths are often found in error output.
- Both the system administrators and developers should be made aware, as the problem may be due to an application error or server misconfiguration.
- Error output containing sensitive information such as absolute system paths should not be sent to remote clients on production servers.
- This output should be sent to another output stream, such as an error log.

REFERENCES

Some additional links with relevant information published by third-parties:

- Information Leakage (OWASP

******************************End of Document************************************