Vulnerability Report

Target URL: http://zero.webappsecurity.com/

Submitted by: P. K. Amudhini

Ethical Hacking Internship -- Task-2

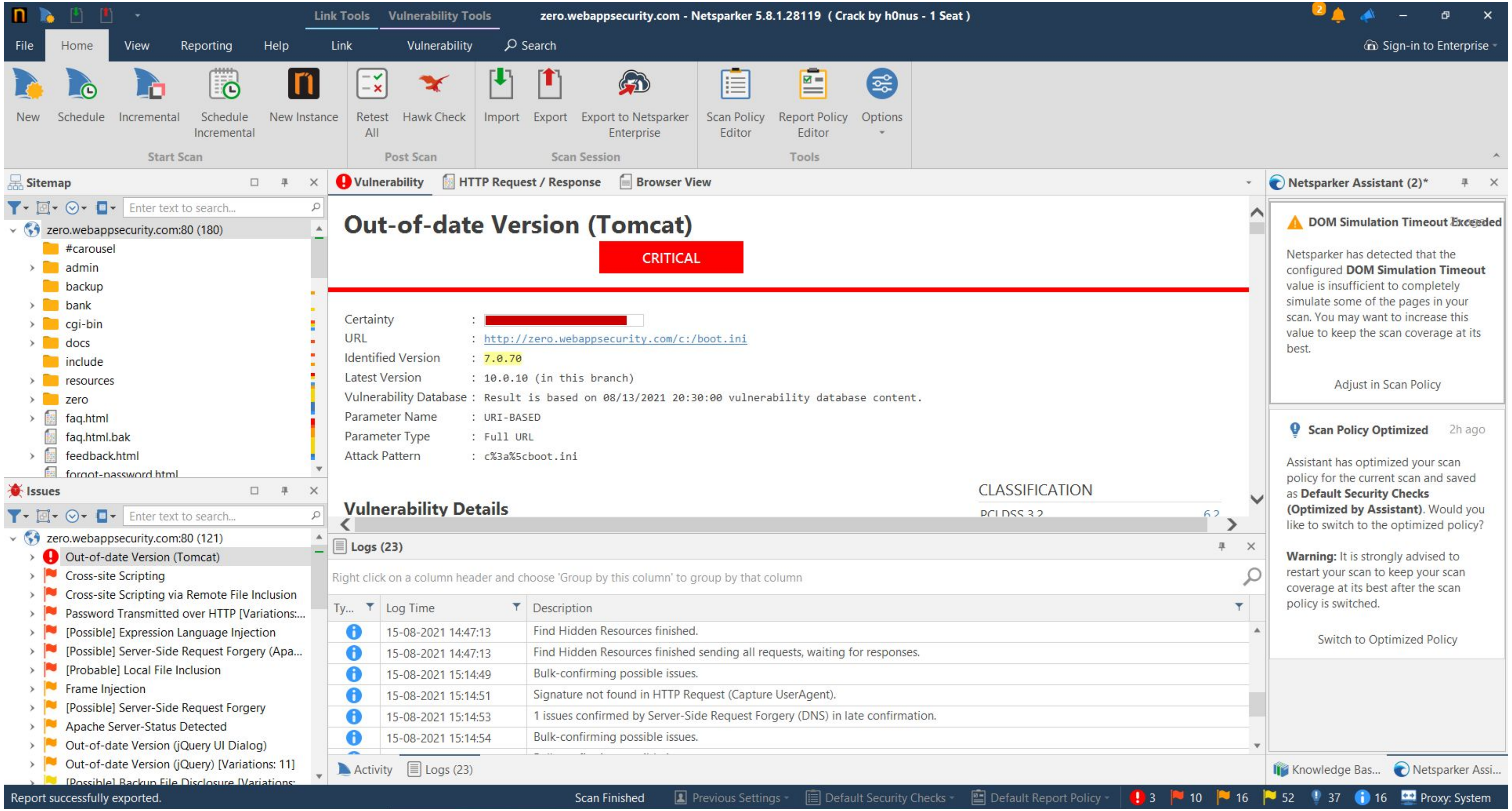
internship studio

Vulnerability Statistics

Critical	High	Medium	Low
3	10	16	52

Vulnerability Report Generated by Netsparker

Screenshot of Netsparker



Sitemap:

- zero.webappsecurity.com:80 (180)
  - #carousel
  - admin
  - backup
  - bank
  - cgi-bin
  - docs
  - include
  - resources
  - zero
  - faq.html
  - faq.html.bak
  - feedback.html
  - forgot-password.html

Issues:

- zero.webappsecurity.com:80 (121)
  - Out-of-date Version (Tomcat)
  - Cross-site Scripting
  - Cross-site Scripting via Remote File Inclusion
  - Password Transmitted over HTTP [Variations:...
  - [Possible] Expression Language Injection
  - [Possible] Server-Side Request Forgery (Apa...
  - [Probable] Local File Inclusion
  - Frame Injection
  - [Possible] Server-Side Request Forgery
  - Apache Server-Status Detected
  - Out-of-date Version (jQuery UI Dialog)
  - Out-of-date Version (jQuery) [Variations: 11]
  - [Possible] Backup File Disclosure [Variations:

Out-of-date Version (Tomcat)

CRITICAL

Certainty	:
URL	: http://zero.webappsecurity.com/c:/boot.ini
Identified Version	: 7.0.70
Latest Version	: 10.0.10 (in this branch)
Vulnerability Database	: Result is based on 08/13/2021 20:30:00 vulnerability database content.
Parameter Name	: URI-BASED
Parameter Type	: Full URL
Attack Pattern	: c%3a%5cboot.ini

Vulnerability Details

CLASSIFICATION

PCI DSS 3.2 6.2

Right click on a column header and choose 'Group by this column' to group by that column

Ty...	Log Time	Description
ℹ	15-08-2021 14:47:13	Find Hidden Resources finished.
ℹ	15-08-2021 14:47:13	Find Hidden Resources finished sending all requests, waiting for responses.
ℹ	15-08-2021 15:14:49	Bulk-confirming possible issues.
ℹ	15-08-2021 15:14:51	Signature not found in HTTP Request (Capture UserAgent).
ℹ	15-08-2021 15:14:53	1 issues confirmed by Server-Side Request Forgery (DNS) in late confirmation.
ℹ	15-08-2021 15:14:54	Bulk-confirming possible issues.

DOM Simulation Timeout Exceeded

Netsparker has detected that the configured **DOM Simulation Timeout** value is insufficient to completely simulate some of the pages in your scan. You may want to increase this value to keep the scan coverage at its best.

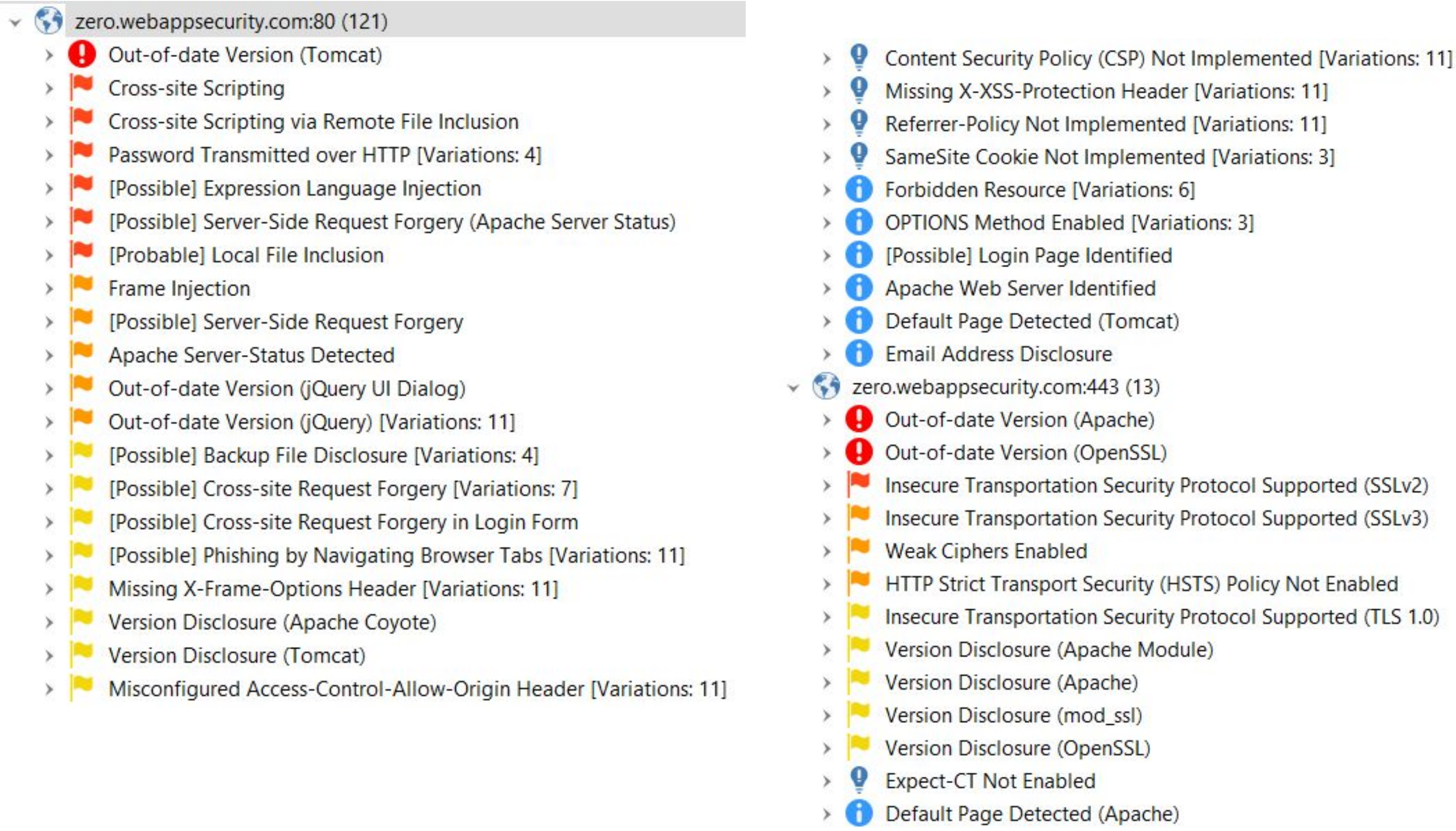
Scan Policy Optimized 2h ago

Assistant has optimized your scan policy for the current scan and saved as **Default Security Checks (Optimized by Assistant)**. Would you like to switch to the optimized policy?

Warning: It is strongly advised to restart your scan to keep your scan coverage at its best after the scan policy is switched.

Report successfully exported. Scan Finished Previous Settings Default Security Checks Default Report Policy ❗ 3 🚩 10 🚩 16 🚩 52 37 ℹ 16 Proxy: System

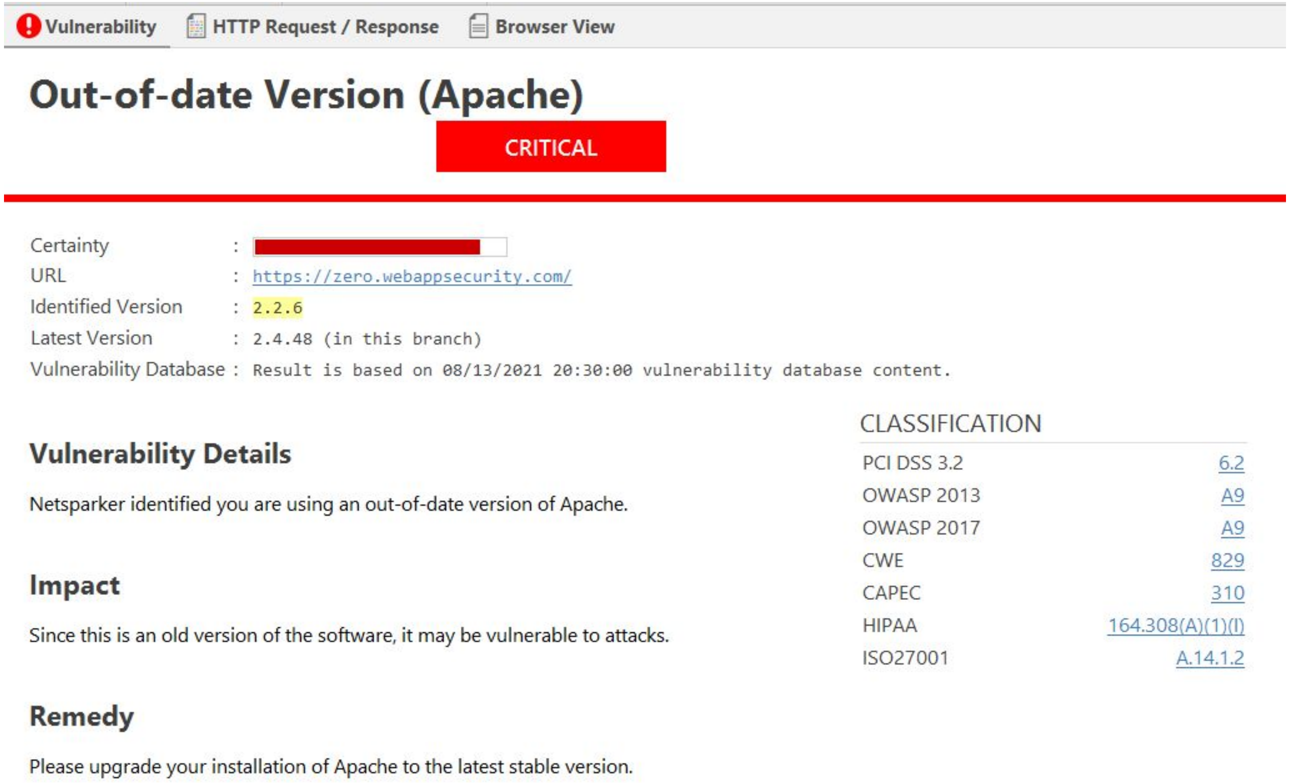
Issues Found by Netsparker



- zero.webappsecurity.com:80 (121)
  - Out-of-date Version (Tomcat)
  - Cross-site Scripting
  - Cross-site Scripting via Remote File Inclusion
  - Password Transmitted over HTTP [Variations: 4]
  - [Possible] Expression Language Injection
  - [Possible] Server-Side Request Forgery (Apache Server Status)
  - [Probable] Local File Inclusion
  - Frame Injection
  - [Possible] Server-Side Request Forgery
  - Apache Server-Status Detected
  - Out-of-date Version (jQuery UI Dialog)
  - Out-of-date Version (jQuery) [Variations: 11]
  - [Possible] Backup File Disclosure [Variations: 4]
  - [Possible] Cross-site Request Forgery [Variations: 7]
  - [Possible] Cross-site Request Forgery in Login Form
  - [Possible] Phishing by Navigating Browser Tabs [Variations: 11]
  - Missing X-Frame-Options Header [Variations: 11]
  - Version Disclosure (Apache Coyote)
  - Version Disclosure (Tomcat)
  - Misconfigured Access-Control-Allow-Origin Header [Variations: 11]
  - Content Security Policy (CSP) Not Implemented [Variations: 11]
  - Missing X-XSS-Protection Header [Variations: 11]
  - Referrer-Policy Not Implemented [Variations: 11]
  - SameSite Cookie Not Implemented [Variations: 3]
  - Forbidden Resource [Variations: 6]
  - OPTIONS Method Enabled [Variations: 3]
  - [Possible] Login Page Identified
  - Apache Web Server Identified
  - Default Page Detected (Tomcat)
  - Email Address Disclosure
- zero.webappsecurity.com:443 (13)
  - Out-of-date Version (Apache)
  - Out-of-date Version (OpenSSL)
  - Insecure Transportation Security Protocol Supported (SSLv2)
  - Insecure Transportation Security Protocol Supported (SSLv3)
  - Weak Ciphers Enabled
  - HTTP Strict Transport Security (HSTS) Policy Not Enabled
  - Insecure Transportation Security Protocol Supported (TLS 1.0)
  - Version Disclosure (Apache Module)
  - Version Disclosure (Apache)
  - Version Disclosure (mod_ssl)
  - Version Disclosure (OpenSSL)
  - Expect-CT Not Enabled
  - Default Page Detected (Apache)

Critical Vulnerabilities Found

Out-of-date Version (Apache)



Out-of-date Version (Apache)

CRITICAL

Certainty :

URL : https://zero.webappsecurity.com/

Identified Version : 2.2.6

Latest Version : 2.4.48 (in this branch)

Vulnerability Database : Result is based on 08/13/2021 20:30:00 vulnerability database content.

Vulnerability Details

Netsparker identified you are using an out-of-date version of Apache.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Remedy

Please upgrade your installation of Apache to the latest stable version.

CLASSIFICATION

PCI DSS 3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
CWE	829
CAPEC	310
HIPAA	164.308(A)(1)(I)
ISO27001	A.14.1.2

Out-of-date Version (Apache)

Vulnerability Type: Critical

Identified Version: 2.2.6
Latest Version: 2.4.48

Impact:
The website will be more vulnerable to ransomware attacks, malware and data breaches which can have catastrophic consequences.

Remedy:
Update Apache to latest version

Remedy Reference:
https://httpd.apache.org/download.cgi

Out-of-date Version (Apache)

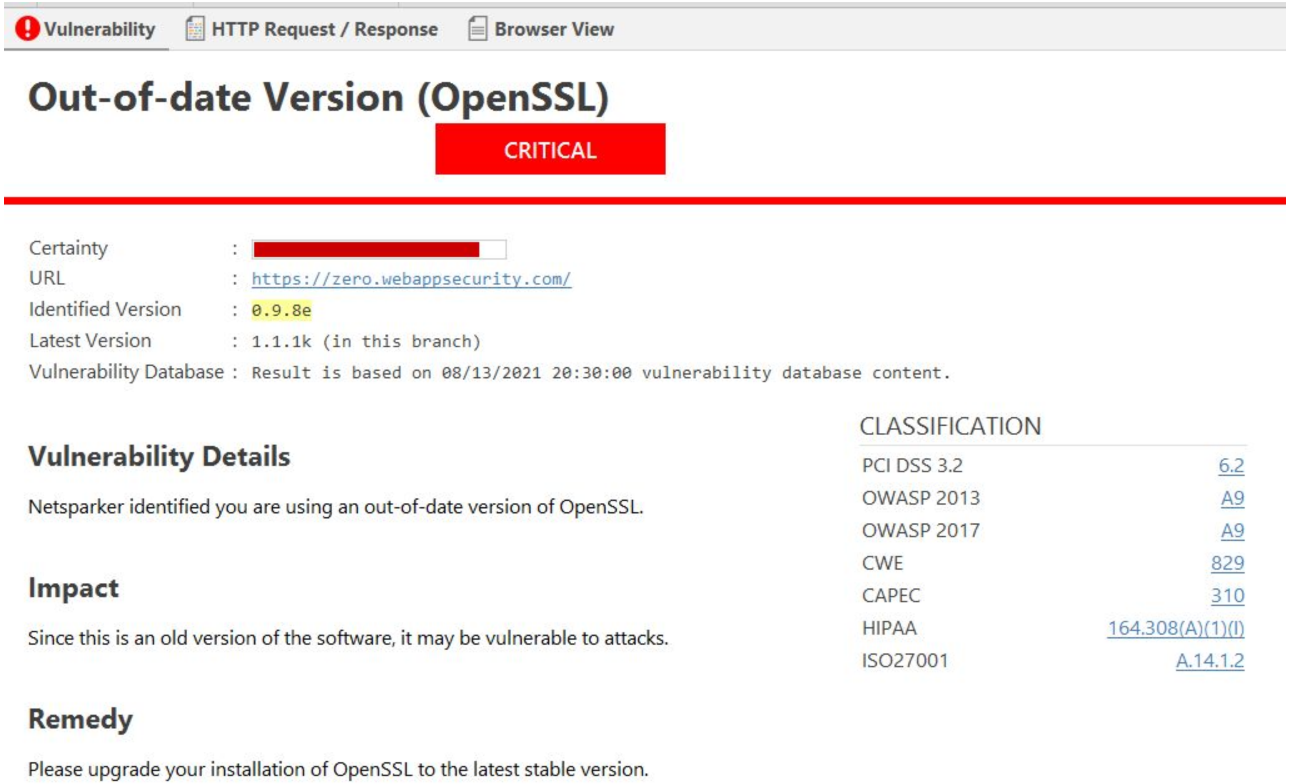
Few Vulnerabilities found in this version:

- **Improper Input Validation Vulnerability (Critical):**
  Incorrect input validation can lead to injection attacks, memory leakage, and compromised systems.

- **Improper Authentication Vulnerability (Critical):**
  When access control checks are incorrectly applied, users are able to access data or perform actions that they should not be allowed to perform. This can lead to a wide range of problems, including information exposures, denial of service, and arbitrary code execution.

- **Numeric Errors Vulnerability (High):**
  The peculiarities of fixed-size integer arithmetic and conversions are subtle and can easily lead to serious security vulnerabilities.

Out-of-date Version (OpenSSL)



Out-of-date Version (OpenSSL)

CRITICAL

Certainty	:	
URL	:	https://zero.webappsecurity.com/
Identified Version	:	0.9.8e
Latest Version	:	1.1.1k (in this branch)
Vulnerability Database	:	Result is based on 08/13/2021 20:30:00 vulnerability database content.

Vulnerability Details

Netsparker identified you are using an out-of-date version of OpenSSL.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Remedy

Please upgrade your installation of OpenSSL to the latest stable version.

CLASSIFICATION

PCI DSS 3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
CWE	829
CAPEC	310
HIPAA	164.308(A)(1)(I)
ISO27001	A.14.1.2

Out-of-date Version (OpenSSL)

Vulnerability Type: Critical

Identified Version: 0.9.8e
Latest Version: 1.1.1k

Impact:
The website will be more vulnerable to ransomware attacks, malware and data breaches which can have catastrophic consequences.

Remedy:
Update OpenSSL to latest version

Remedy Reference:
https://www.openssl.org/

Out-of-date Version (OpenSSL)

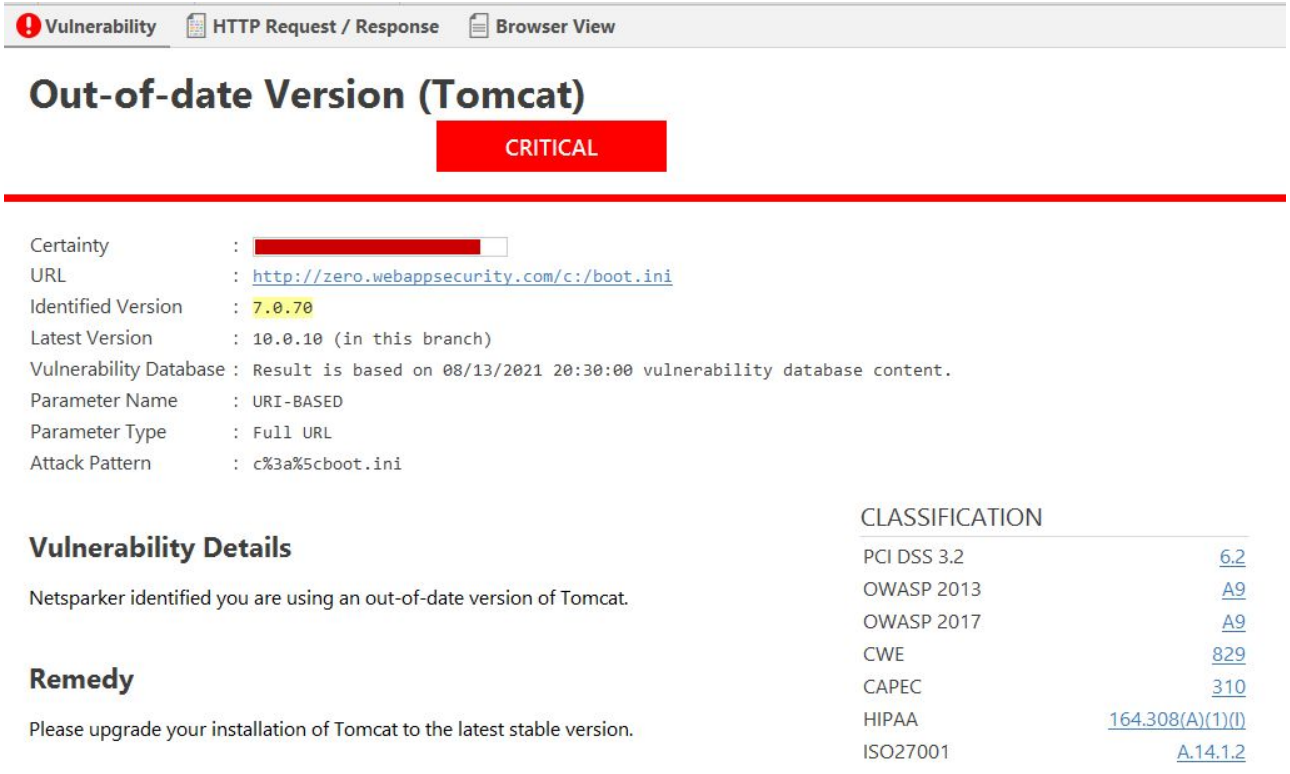
<u>Few Vulnerabilities found in this version:</u>

- **Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability (Critical):**
  Allows attackers to obtain sensitive information from process stack memory or cause a denial of service.

- **Exposure of Sensitive Information to an Unauthorized Actor Vulnerability (High):**
  There is a change of information leak affecting the confidentiality of the user.

- **Numeric Errors Vulnerability (High):**
  The peculiarities of fixed-size integer arithmetic and conversions are subtle and can easily lead to serious security vulnerabilities.

Out-of-date Version (Tomcat)



Out-of-date Version (Tomcat)

CRITICAL

Certainty	:
URL	: http://zero.webappsecurity.com/c:/boot.ini
Identified Version	: 7.0.70
Latest Version	: 10.0.10 (in this branch)
Vulnerability Database	: Result is based on 08/13/2021 20:30:00 vulnerability database content.
Parameter Name	: URI-BASED
Parameter Type	: Full URL
Attack Pattern	: c%3a%5cboot.ini

Vulnerability Details

Netsparker identified you are using an out-of-date version of Tomcat.

Remedy

Please upgrade your installation of Tomcat to the latest stable version.

CLASSIFICATION

PCI DSS 3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
CWE	829
CAPEC	310
HIPAA	164.308(A)(1)(I)
ISO27001	A.14.1.2

Out-of-date Version (Tomcat)

Vulnerability Type: Critical

Identified Version: 7.0.70
Latest Version: 10.0.10

Impact:
The website will be more vulnerable to ransomware attacks, malware and data breaches which can have catastrophic consequences.

Remedy:
Update Tomcat to latest version

Remedy Reference:
https://tomcat.apache.org/whichversion.html

Out-of-date Version (Tomcat)

Few Vulnerabilities found in this version:

- **Exposure of Resource to Wrong Sphere Vulnerability (Critical):**
  Resources such as files and directories may be inadvertently exposed through mechanisms such as insecure permissions, or when a program accidentally operates on the wrong object.

- **Unreachable Exit Condition ('Infinite Loop') Vulnerability (High):**
  An improper handling of overflow in the UTF-8 decoder with supplementary characters can lead to an infinite loop in the decoder causing a Denial of Service.

- **Unrestricted Upload of File with Dangerous Type Vulnerability (High):**
  May grant access or host other illegal software objects that will increase the chance of further security risks. The hacker may gain control of the webserver and modify the website to remove useful pieces of data.

Thank You

Detailed scan report generated by Netsparker is provided in Github

https://github.com/jill-amudhini/InternshipStudio-EthicalHacking