Reporting Vulnerability

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

Netsparker Vulnerability Report

Overview:

- The Netsparker vulnerability scan was conducted on http://zero.webappsecurity.com.
- The detailed scan report PDF is attached in the folder for reference.
- Additionally, a Base Knowledge report is also provided.

Highlights:

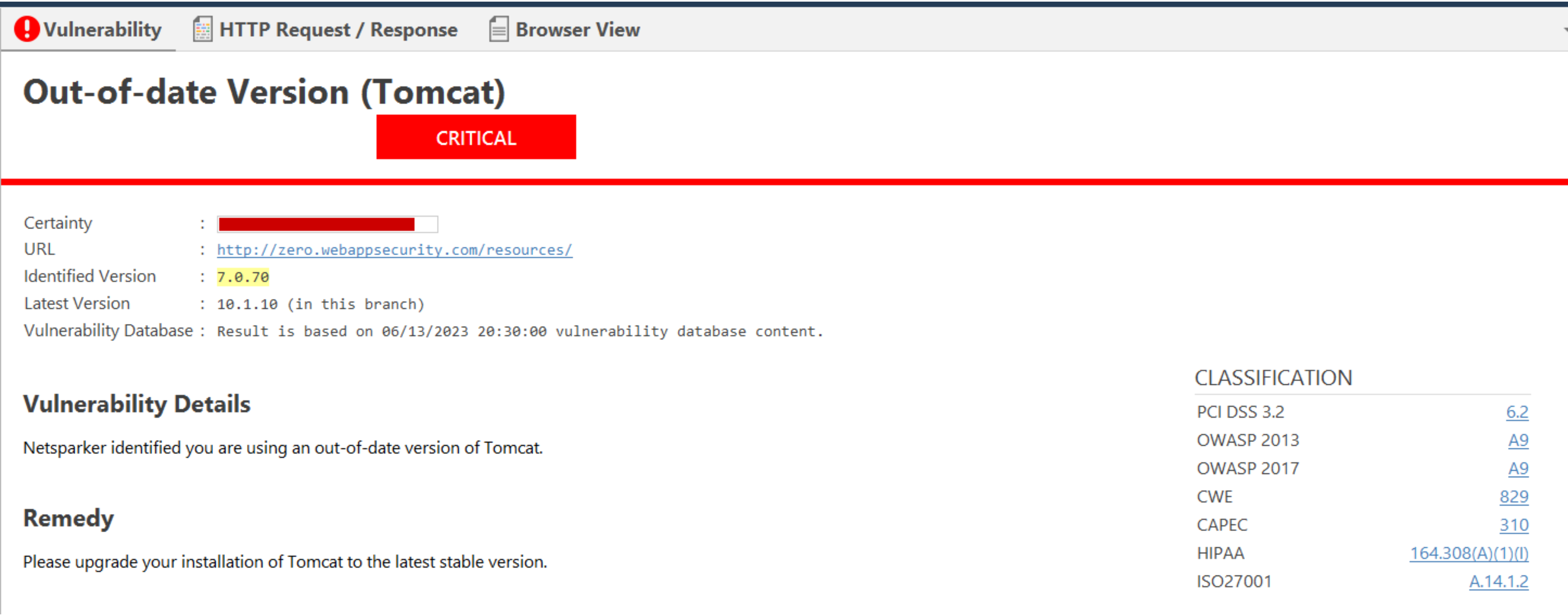
- Critical vulnerabilities identified: 3
- High vulnerabilities identified: 5
- Medium vulnerabilities identified: 7
- Low vulnerabilities identified: 13
- Best Practice recommendations: 5
- Informational findings: 7

Testing Environment:

- Netsparker version: 5.8.2.28358.
- Settings: Default
- Scan Policy: Extensive Security Checks
- OS: Windows machine.
- Initiated on: 15th June 2023 at 15:07:45 (UTC+05:30).

3 Critical Vulnerabilities are:

1. Out-of-date Version (Tomcat)



Out-of-date Version (Tomcat)

CRITICAL

Certainty :

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

Identified Version : 7.0.70

Latest Version : 10.1.10 (in this branch)

Vulnerability Database : Result is based on 06/13/2023 20:30:00 vulnerability database content.

Vulnerability Details

Netsparker identified you are using an out-of-date version of Tomcat.

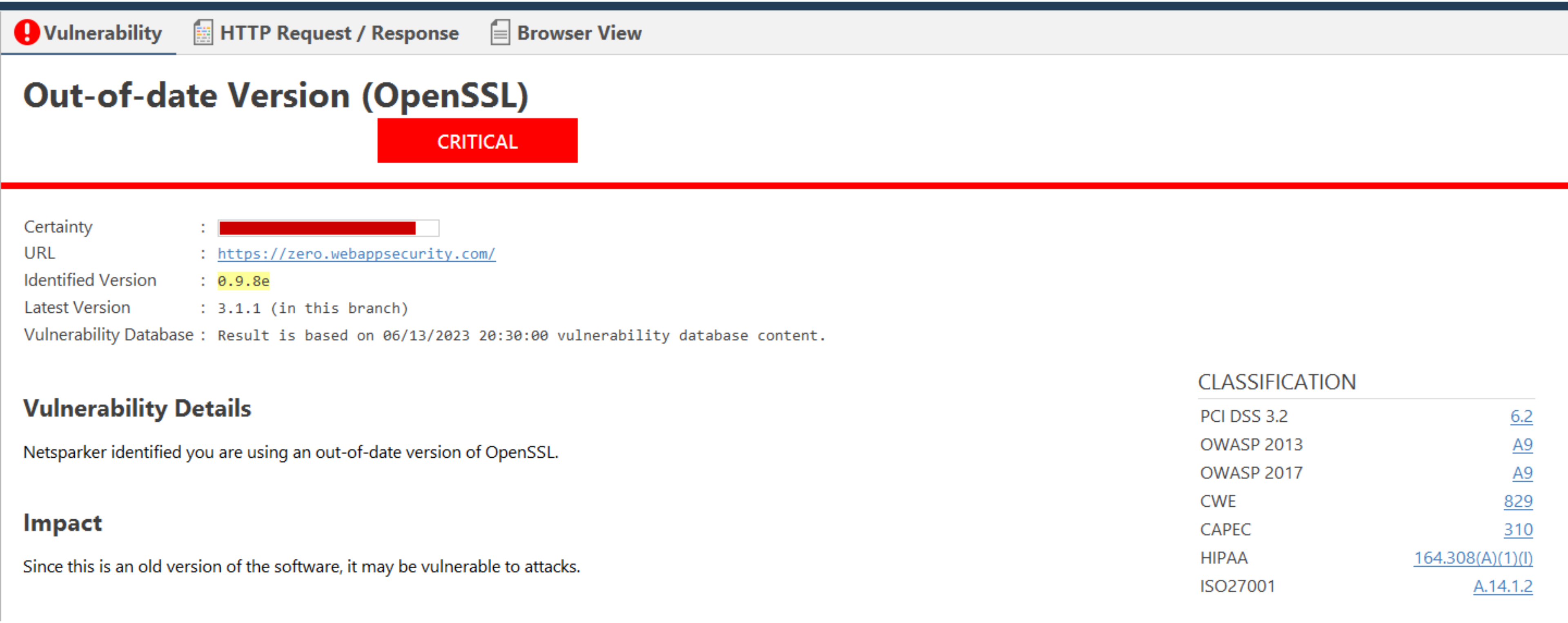
Remedy

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

2. Out-of-date Version (OpenSSL)



Out-of-date Version (OpenSSL)

CRITICAL

Certainty :

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

Identified Version : 0.9.8e

Latest Version : 3.1.1 (in this branch)

Vulnerability Database : Result is based on 06/13/2023 20:30:00 vulnerability database content.

Vulnerability Details

Netsparker identified you are using an out-of-date version of OpenSSL.

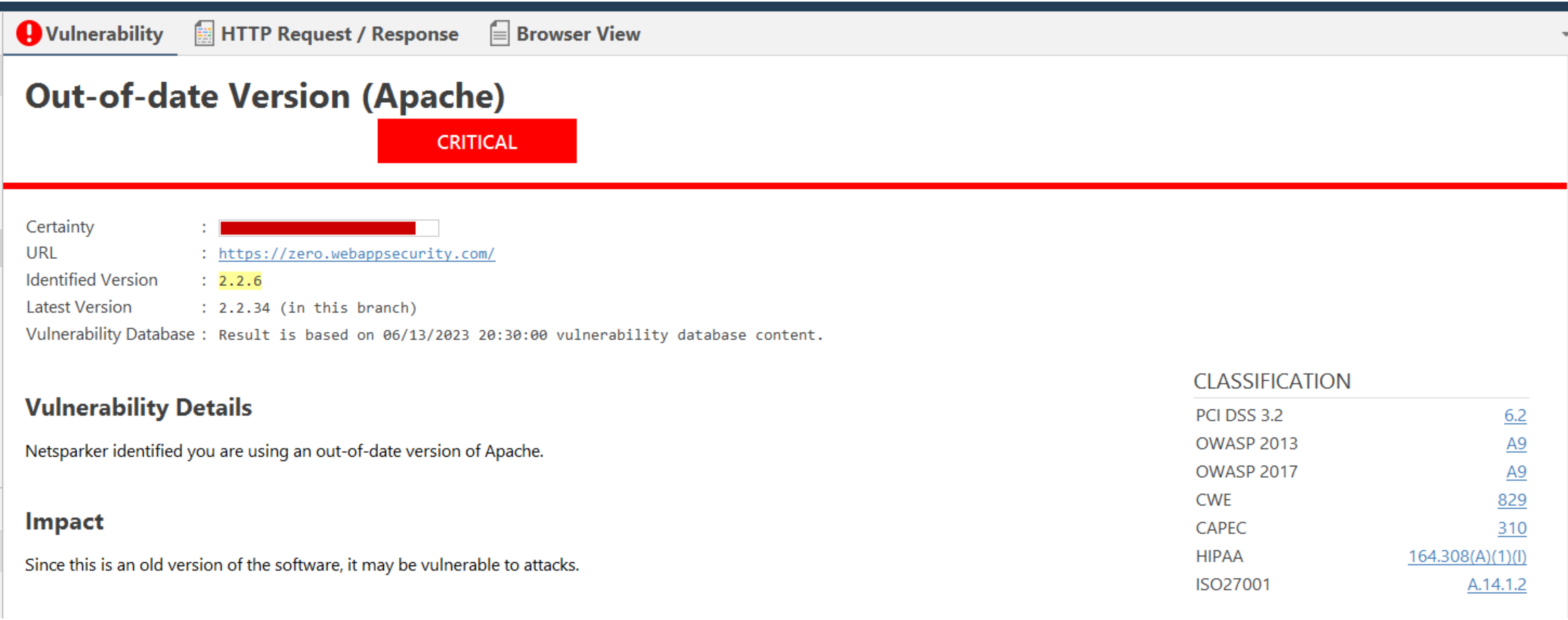
Impact

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

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

3. Out-of-date Version (Apache)



Out-of-date Version (Apache)

CRITICAL

Certainty :

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

Identified Version : 2.2.6

Latest Version : 2.2.34 (in this branch)

Vulnerability Database : Result is based on 06/13/2023 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.

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 Report in own language

Summary:

The vulnerability report focuses on an out-of-date version of the Apache HTTP Server (version 2.2.6) identified in the web application. The report highlights the potential security risks associated with this outdated version and recommends upgrading to the latest stable version (2.2.34).

Description:

Netsparker, the scanning tool used, has classified this vulnerability based on various standards such as PCI DSS 3.2, OWASP 2013/2017, CWE 829, CAPEC 310, HIPAA 164.308(A)(1)(I), and ISO27001 A.14.1.2. It signifies the importance of addressing the vulnerability promptly to maintain compliance with these standards and mitigate potential risks.

Environment:

The scanning process was conducted using Netsparker version 5.8.2.28358 on a Windows machine. The scan was initiated on 15th June 2023 at 15:07:45 (UTC+05:30). The scan was performed using the default settings and employed the Extensive Security Checks scan policy.

Impact:

- Using an outdated version of Apache HTTP Server may expose the web application to security threats.
- Several known vulnerabilities have been identified in the old version, which may be exploited by attackers.
- The vulnerabilities can lead to various risks, including request smuggling, response splitting, cache pollution, denial of service, and the execution of arbitrary commands.

Recommendations:

Upgrade your installation of Apache to the latest stable version.

Proof of Concept (PoC):

Some specific vulnerabilities found in the outdated Apache HTTP Server version 2.2.6. These include:

- CVE-2016-8743: Whitespace acceptance vulnerability leading to request smuggling and cache pollution.
- CVE-2016-5387: Presence of untrusted client data in the HTTP_PROXY environment variable, allowing HTTP traffic redirection.
- CVE-2012-0031: Scoreboard manipulation leading to denial of service or other impacts.
- CVE-2012-0053: Improper restriction of header information resulting in cookie exposure.
- CVE-2012-0883: Placing a zero-length directory name in LD_LIBRARY_PATH, potentially allowing privilege escalation.
- CVE-2013-1862: Data logging vulnerability permitting remote command execution.
- CVE-2013-1896: Failure to properly determine whether DAV is enabled, leading to a denial of service.
- CVE-2013-6438: Improper handling of whitespace characters causing a denial of service.

Furthermore, it should be noted that an additional Cross-Site Scripting (XSS) vulnerability has been identified, which was not detected by my Netsparker during the scan. This particular vulnerability may carries the potential for critical impact.

Attaching a report regarding this

Summary:

This report highlights a discovered vulnerability in your company's web application related to Cross-site Scripting (XSS). The vulnerability allows an attacker to execute dynamic scripts, such as JavaScript or VBScript, within the context of the application.

Description:

This report outlines a critical vulnerability identified in your website, known as Cross-site Scripting (XSS), which demands immediate attention. XSS occurs when the website fails to adequately sanitize and validate user input, allowing malicious code to be injected and executed within the application's context.

By exploiting this vulnerability, threat actors can engage in various malicious activities, compromising the integrity and security of your website and its users. These activities include the hijacking of active user sessions, perpetrating phishing attacks, and intercepting sensitive data for nefarious purposes.

Environment:

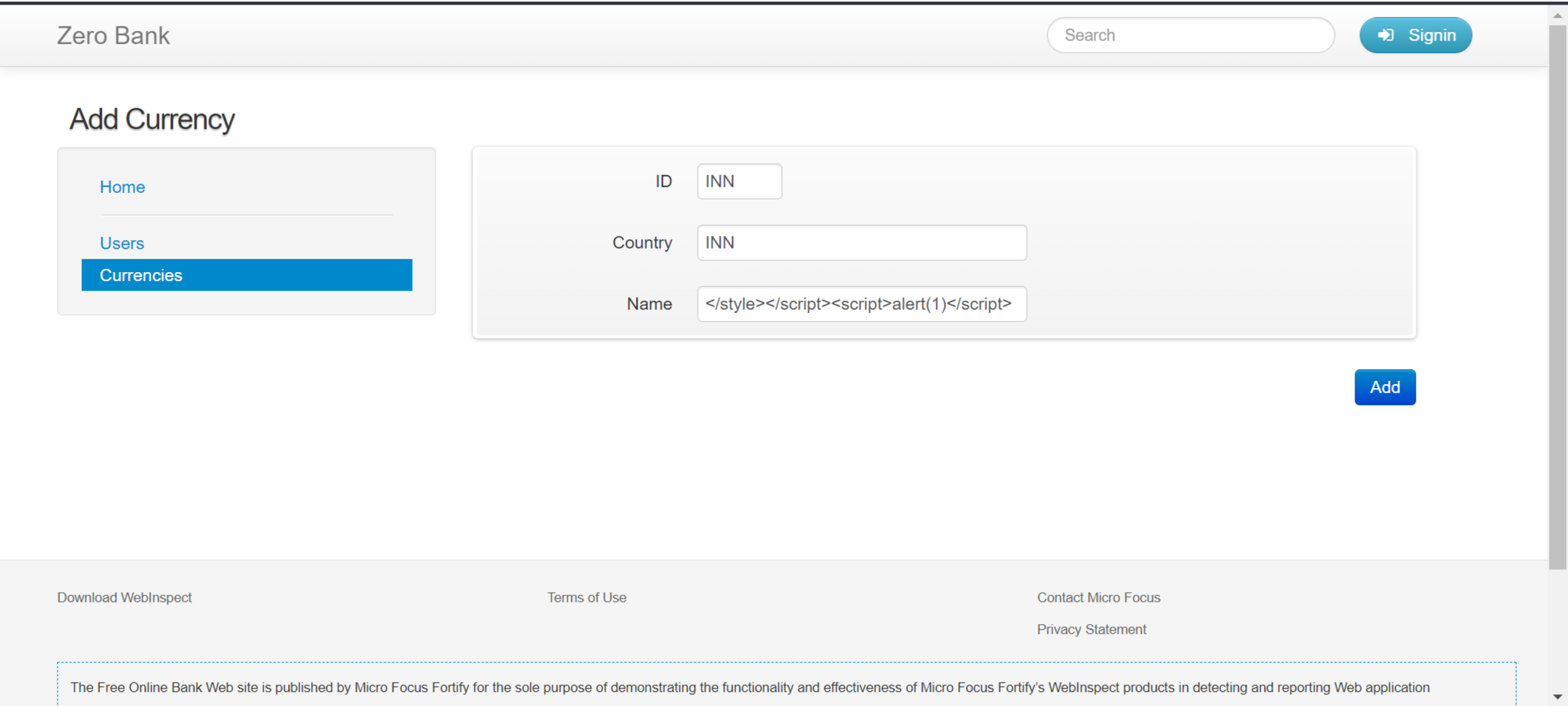
Scope: Web Application
Product name: Zero Bank
OS name and version (incl SP): Windows 11 22H2
Attack type: Universal XSS
Maximum user privileges needed to reproduce your issue: no privileges

Steps To Reproduce:

1. Access the web page using the provided URL: http://zero.webappsecurity.com/admin/currencies-add.html.
2. On the loaded page, locate the "Name" field.
3. Inject the following payload into the "Name" field: *</style></script><script>alert(1)</script>*.
4. Proceed to visit the http://zero.webappsecurity.com/admin/currencies-add.html web page.
5. Once on the "currency.html" page, the injected JavaScript payload will trigger, resulting in an alert displaying the value "1".

These steps demonstrate the presence of a Cross-site Scripting (XSS) vulnerability within the web application.
To support this report, I have attached a video and screenshots that clearly demonstrate the vulnerability. Kindly refer to the "Proof of Concept (POC)" section for further details and visual evidence.

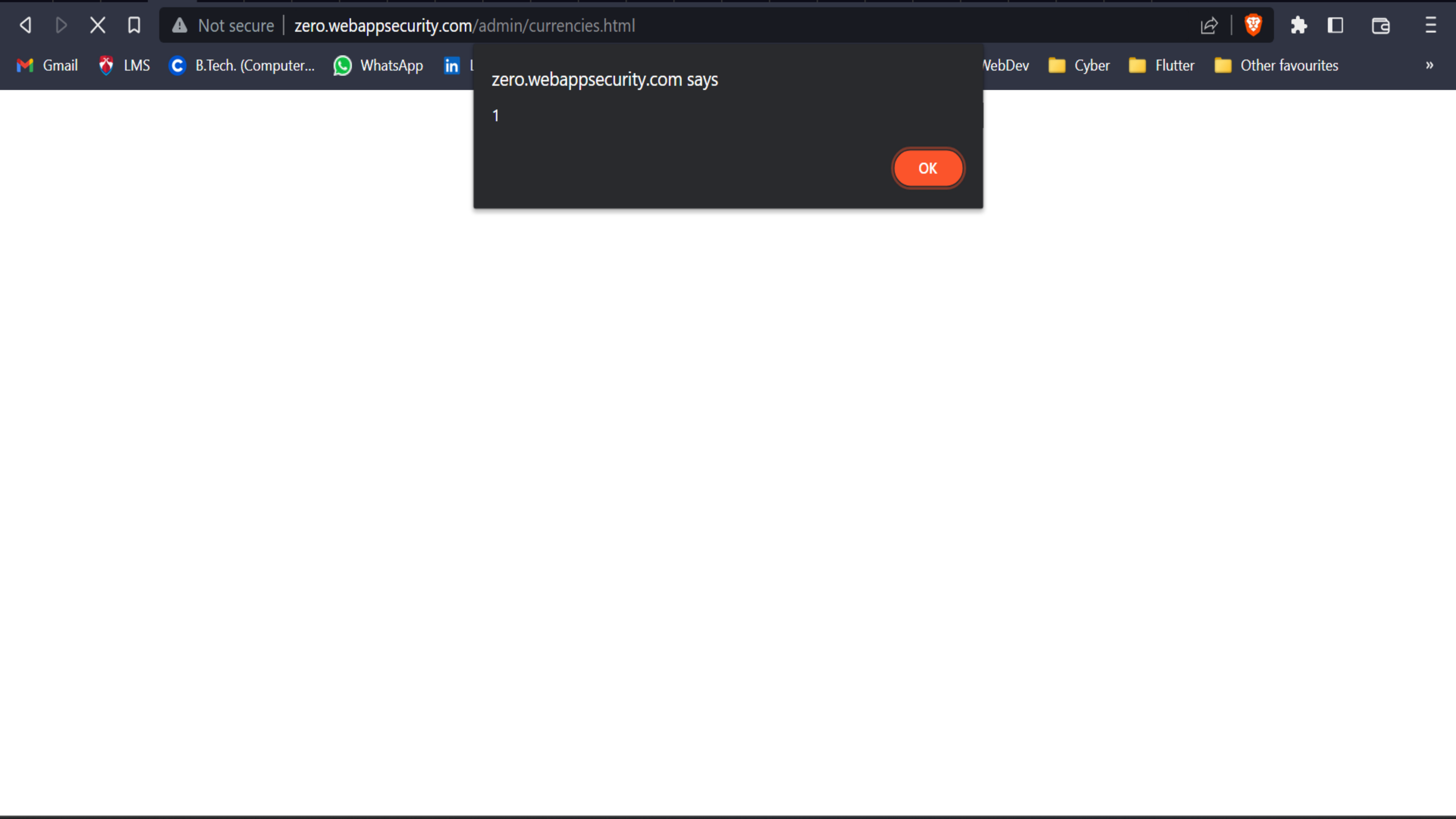
Proof of Concept (PoC):



Add Currency

ID	INN
Country	INN
Name	</style></script><script>alert(1)</script>

The Free Online Bank Web site is published by Micro Focus Fortify for the sole purpose of demonstrating the functionality and effectiveness of Micro Focus Fortify's WebInspect products in detecting and reporting Web application



zero.webappsecurity.com says

1

Video Demonstration:

Impact:

The identified Cross-site Scripting (XSS) vulnerability poses significant risks to the security and integrity of the web application. If exploited, the following impacts can be expected:

- Session Hijacking
- Phishing Attacks
- Data Interception and Man-in-the-Middle Attacks
- Reputation and Trust Damage

Recommendations:

- Implement thorough input validation and output encoding techniques.
- Deploy and configure a robust Content Security Policy (CSP).
- Integrate secure coding practices into the development process.
- Develop an effective incident response plan for XSS attacks.

Thank You

Submitted by: Vishal Balani