Vulnerability Assessment Report for zero.webappsecurity.com

Target Website: https://zero.webappsecurity.com
Project : 01
Assessment Type: Passive Security Scan
Date: 11-01-2026

Scope

In Scope

- Public pages
- HTTP response headers
- Passive network exposure
- Configuration analysis

Out of Scope

- Authentication bypass
- Credential testing
- Denial-of-Service testing
- Any action that could disrupt availability

Tools & Methodology

Tool	Purpose
Nmap	Identify exposed network ports and services
OWASP ZAP (Passive Mode)	Detect misconfigurations and insecure headers
Browser DevTools	Inspect cookies, headers, and client-side issues

Detailed Findings

1.Insecure Transport (HTTP only) - Port 80

Description:

The website is accesible over HTTP (80) . HTTP sends data to server as clear text which may contain sensitive information such as passwords. Attackers can intercept, read, and alter the communication between a client and a server.No lock icon on address bar

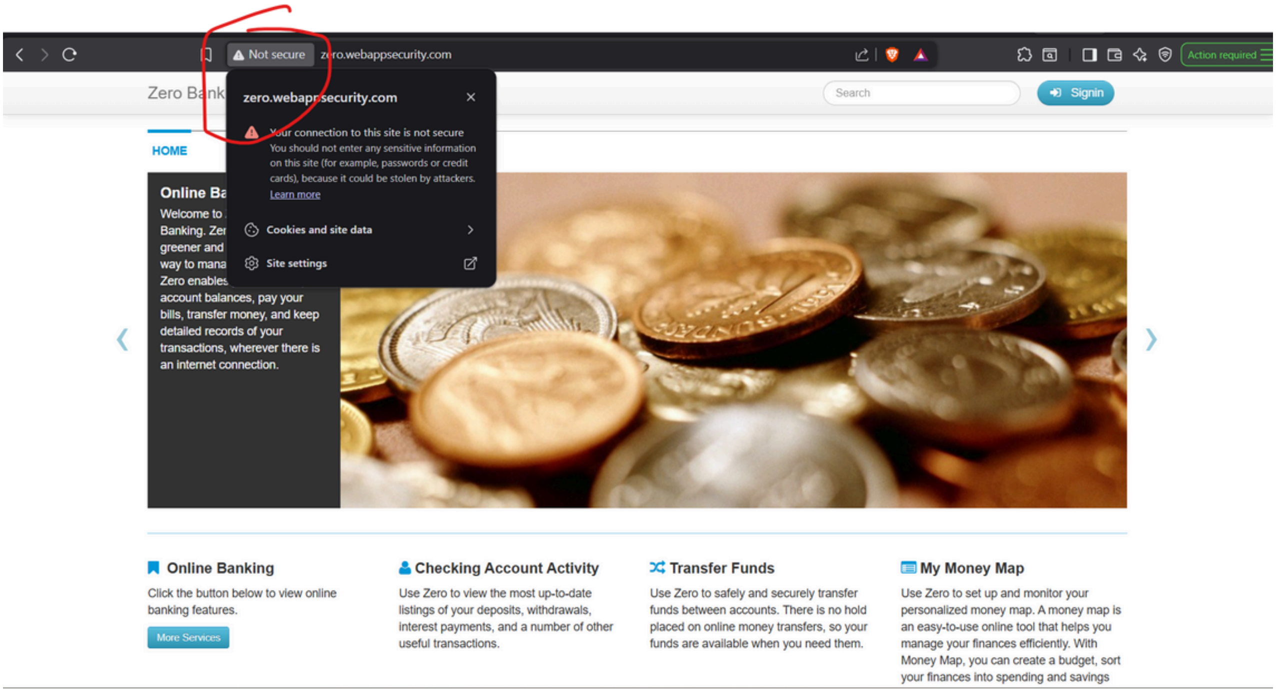
Risk Classification: HIGH

Remediation:

Enforce HTTPS (443) using TLS certifications and redirect all http traffic to https. Enable HSTS (HTTP Strict Transport Security) header to instruct browsers to only use HTTPS for future connections to your site, which helps prevent downgrade attacks and further enhances security.

Tools used : Browser (public page) and Nmap

Evidence:



Not secure zero.webappsecurity.com

zero.webappsecurity.com

Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

Cookies and site data

Site settings

Zero Bank

Search

Signin

HOME

Online Ba

Welcome to Banking. Zer greener and way to mana Zero enables account balances, pay your bills, transfer money, and keep detailed records of your transactions, wherever there is an internet connection.

Online Banking

Click the button below to view online banking features.

More Services

Checking Account Activity

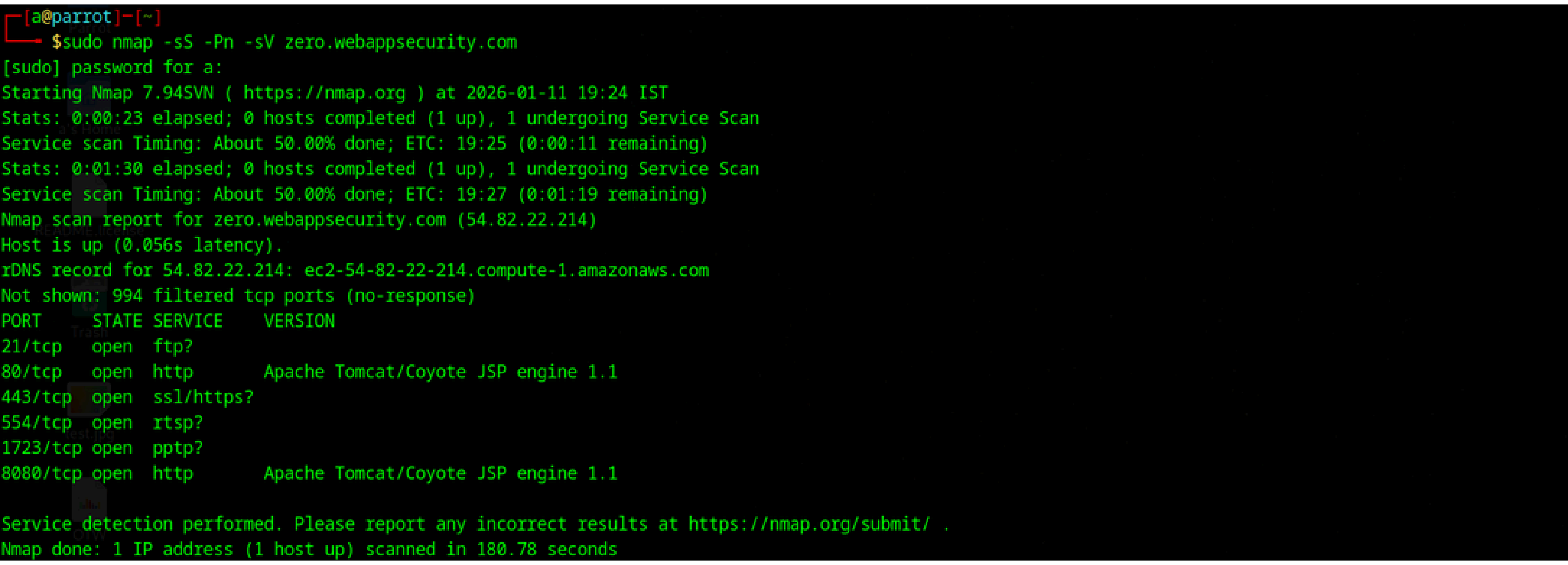
Use Zero to view the most up-to-date listings of your deposits, withdrawals, interest payments, and a number of other useful transactions.

Transfer Funds

Use Zero to safely and securely transfer funds between accounts. There is no hold placed on online money transfers, so your funds are available when you need them.

My Money Map

Use Zero to set up and monitor your personalized money map. A money map is an easy-to-use online tool that helps you manage your finances efficiently. With Money Map, you can create a budget, sort your finances into spending and savings



```
┌─[a@parrot]─[~]
└──╼ $sudo nmap -sS -Pn -sV zero.webappsecurity.com
[sudo] password for a:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-11 19:24 IST
Stats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 19:25 (0:00:11 remaining)
Stats: 0:01:30 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 19:27 (0:01:19 remaining)
Nmap scan report for zero.webappsecurity.com (54.82.22.214)
Host is up (0.056s latency).
rDNS record for 54.82.22.214: ec2-54-82-22-214.compute-1.amazonaws.com
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE   VERSION
21/tcp   open  ftp?
80/tcp   open  http      Apache Tomcat/Coyote JSP engine 1.1
443/tcp  open  ssl/https?
554/tcp  open  rtsp?
1723/tcp open  pptp?
8080/tcp open  http      Apache Tomcat/Coyote JSP engine 1.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 180.78 seconds
```

2.Broken Access Control : Unidentified Ports are open

Description:

Unidentified ports are open which can increase attack surface and allow an attacker to exploit unidentified open ports to gain unauthorized access to sensitive resources or perform actions beyond their intended permissions.

Risk Classification: MEDIUM

Remediation:

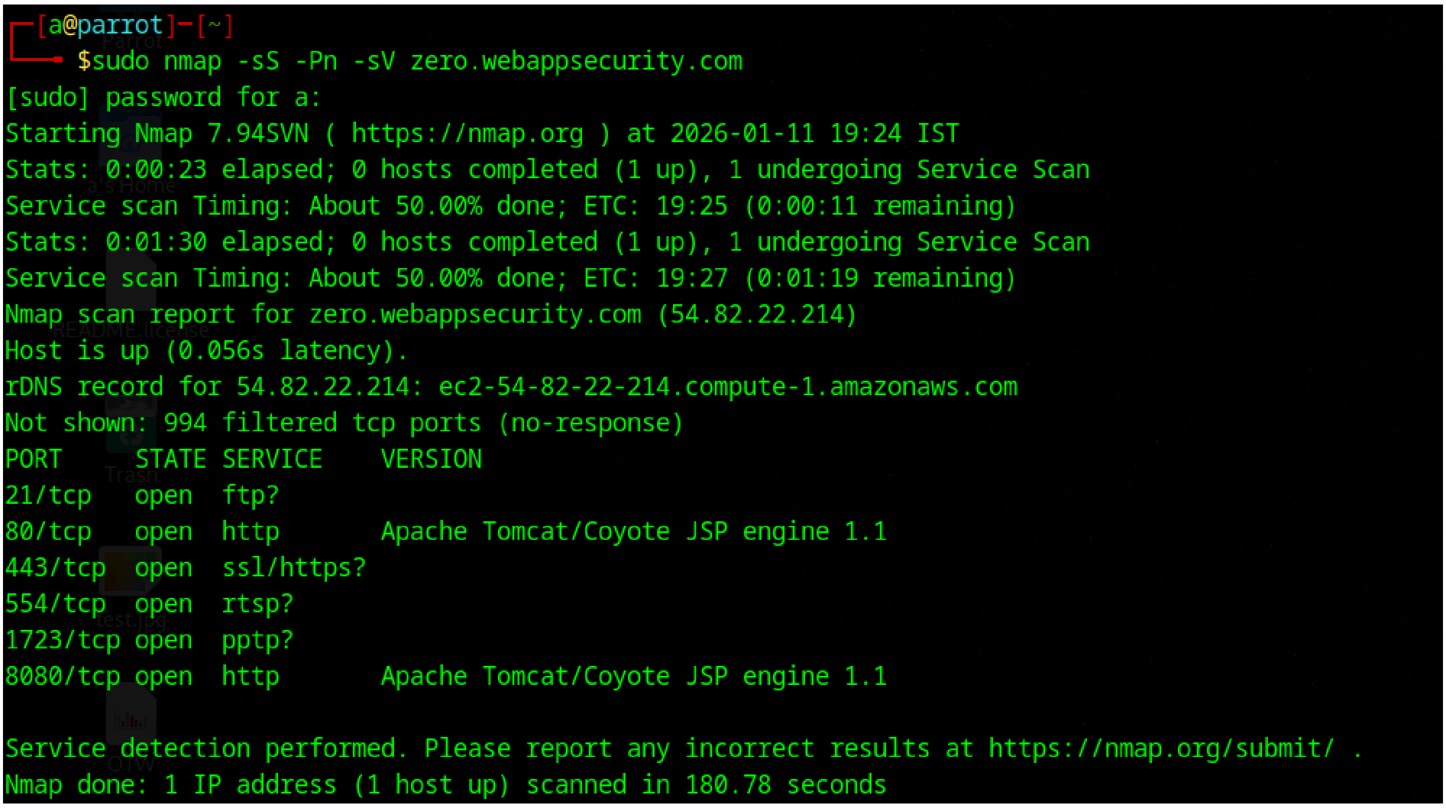
Webpages,files,directories,database components,ports should be closed while migrating application into Production Environment.

Tools used : Nmap

Steps to Reproduce : Run Nmap tool on Parrot terminal with command :

sudo nmap -sS -Pn -sV zero.webappsecurity.com (provide root password to continue)

Evidence:



```
┌─[a@parrot]─[~]
└──╼ $sudo nmap -sS -Pn -sV zero.webappsecurity.com
[sudo] password for a:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-11 19:24 IST
Stats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 19:25 (0:00:11 remaining)
Stats: 0:01:30 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 19:27 (0:01:19 remaining)
Nmap scan report for zero.webappsecurity.com (54.82.22.214)
Host is up (0.056s latency).
rDNS record for 54.82.22.214: ec2-54-82-22-214.compute-1.amazonaws.com
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp?
80/tcp   open  http       Apache Tomcat/Coyote JSP engine 1.1
443/tcp  open  ssl/https?
554/tcp  open  rtsp?
1723/tcp open  pptp?
8080/tcp open  http       Apache Tomcat/Coyote JSP engine 1.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 180.78 seconds
```

3.Missing Content Security Policy (CSP)

Description:

A missing Content Security Policy (CSP) means your website lacks a crucial security header that tells browsers which sources are trusted for content, leaving it vulnerable to attacks like Cross-Site Scripting (XSS) and data injection, allowing attackers to inject malicious scripts, steal data, or deface your site

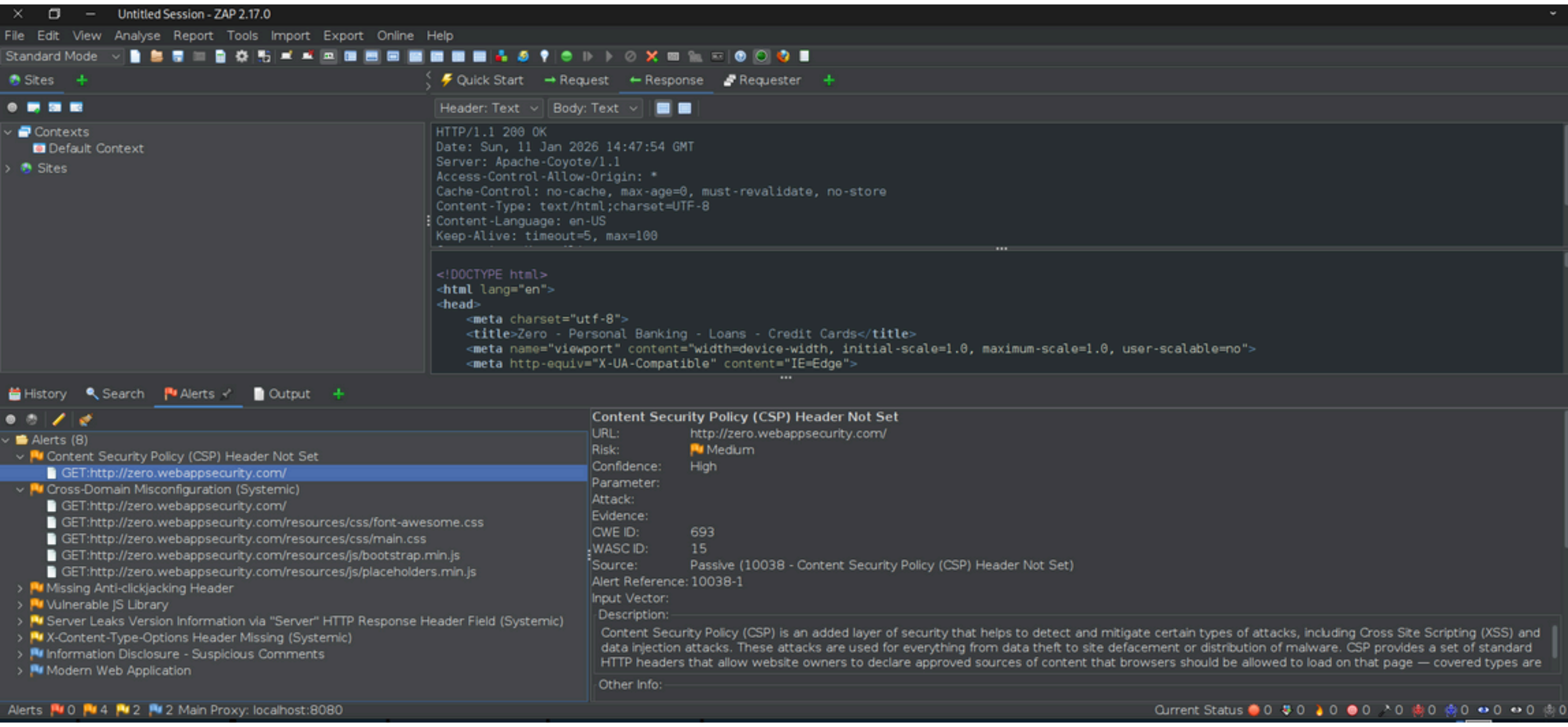
Risk Classification: MEDIUM

Remediation:

Configure your web server (Apache) or application to send the Content-Security-Policy HTTP response header. **Use Nonces/Hashes**: For dynamic content, use unique nonces (numbers used once) or hashes to allow specific inline scripts without opening up the entire page to XSS.

Tools used : Owasp-zap

Evidence:



```
HTTP/1.1 200 OK
Date: Sun, 11 Jan 2026 14:47:54 GMT
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Cache-Control: no-cache, max-age=0, must-revalidate, no-store
Content-Type: text/html;charset=UTF-8
Content-Language: en-US
Keep-Alive: timeout=5, max=100
```

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <title>Zero - Personal Banking - Loans - Credit Cards</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">
    <meta http-equiv="X-UA-Compatible" content="IE=Edge">
```

```
Alerts (8)
  Content Security Policy (CSP) Header Not Set
    GET:http://zero.webappsecurity.com/
  Cross-Domain Misconfiguration (Systemic)
    GET:http://zero.webappsecurity.com/
    GET:http://zero.webappsecurity.com/resources/css/font-awesome.css
    GET:http://zero.webappsecurity.com/resources/css/main.css
    GET:http://zero.webappsecurity.com/resources/js/bootstrap.min.js
    GET:http://zero.webappsecurity.com/resources/js/placeholders.min.js
  Missing Anti-clickjacking Header
  Vulnerable JS Library
  Server Leaks Version Information via "Server" HTTP Response Header Field (Systemic)
  X-Content-Type-Options Header Missing (Systemic)
  Information Disclosure - Suspicious Comments
  Modern Web Application
```

Content Security Policy (CSP) Header Not Set

URL:	http://zero.webappsecurity.com/
Risk:	Medium
Confidence:	High
Parameter:	
Attack:	
Evidence:	
CWE ID:	693
WASC ID:	15
Source:	Passive (10038 - Content Security Policy (CSP) Header Not Set)
Alert Reference:	10038-1
Input Vector:	

Description:

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are

Other Info:

Alerts 0 4 2 2 Main Proxy: localhost:8080

Current Status 0 0 0 0 0 0 0 0 0 0

4.Missing Security Headers

Description:

Several recommended HTTP security headers were missing or improperly configured, including:

X-frame-options Header - doesnt protect against clickjacking attacks

X-content-type-options missing - MIME type sniffing attacks.

Risk Classification: MEDIUM

Remediation:

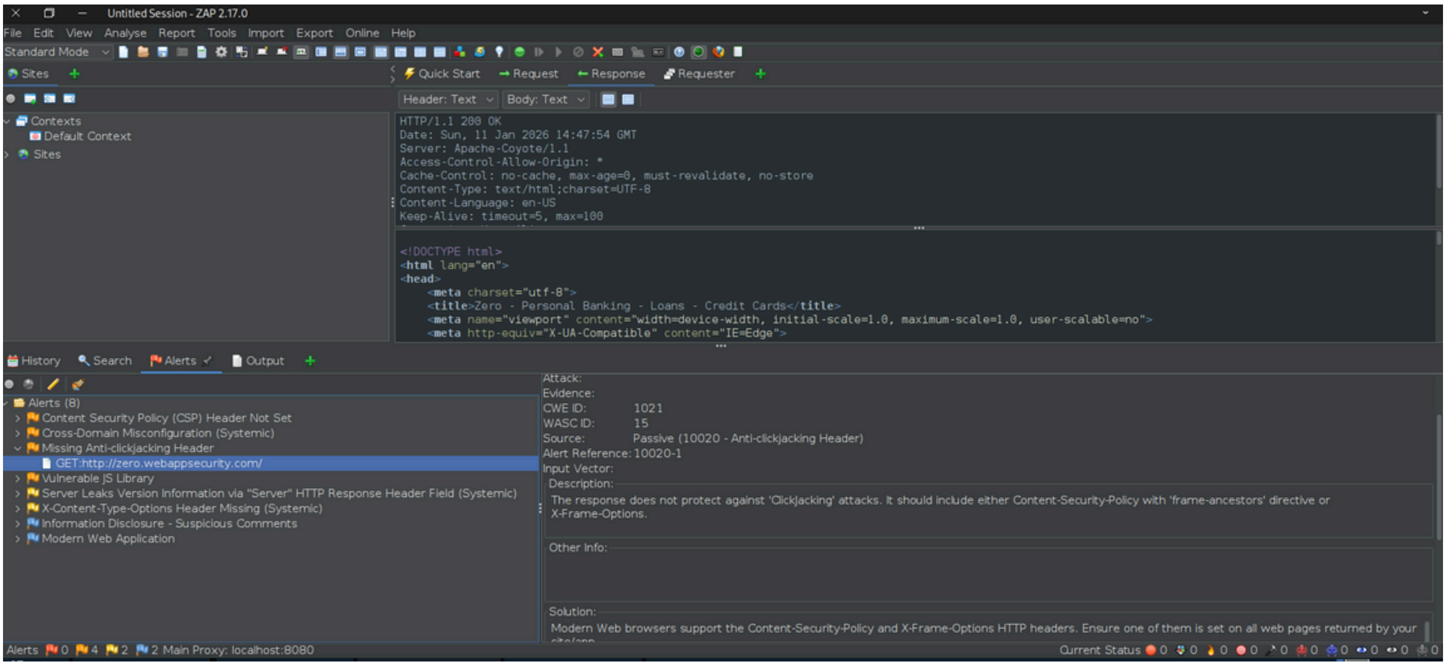
-Implement standard security headers using web server configuration .

-Follow OWASP Secure Headers guidelines.

Tools used : Owasp-zap

Evidence:

X-frame-options Header missing:


Untitled Session - ZAP 2.17.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
History
Search
Alerts
Output
Alerts 0 4 2 2 Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0

```
HTTP/1.1 200 OK
Date: Sun, 11 Jan 2026 14:47:54 GMT
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Cache-Control: no-cache, max-age=0, must-revalidate, no-store
Content-Type: text/html;charset=UTF-8
Content-Language: en-US
Keep-Alive: timeout=5, max=100
```

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <title>Zero - Personal Banking - Loans - Credit Cards</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">
    <meta http-equiv="X-UA-Compatible" content="IE=Edge">
```

- Alerts (8)
  - Content Security Policy (CSP) Header Not Set
  - Cross-Domain Misconfiguration (Systemic)
  - Missing Anti-clickjacking Header
    - GET:http://zero.webappsecurity.com/
  - Vulnerable JS Library
  - Server Leaks Version Information via "Server" HTTP Response Header Field (Systemic)
  - X-Content-Type-Options Header Missing (Systemic)
  - Information Disclosure - Suspicious Comments
  - Modern Web Application

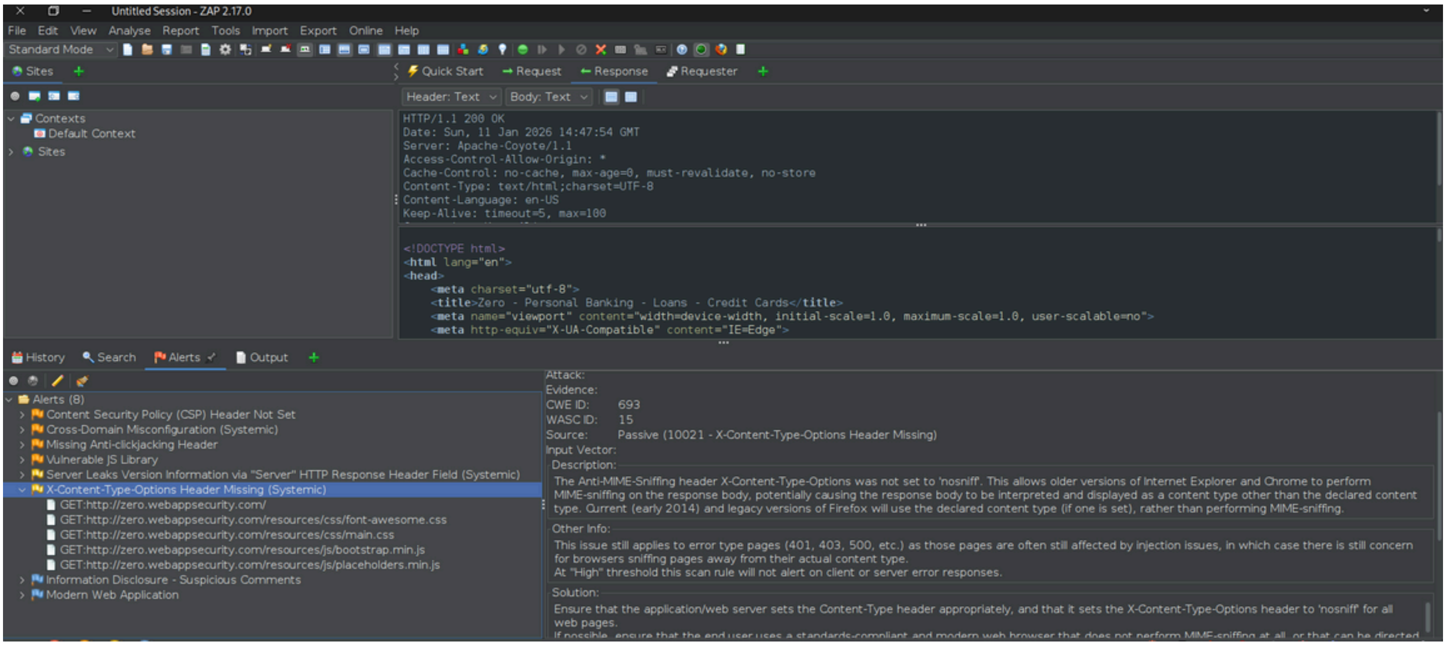
Attack:
Evidence:
CWE ID: 1021
WASC ID: 15
Source: Passive (10020 - Anti-clickjacking Header)
Alert Reference: 10020-1
Input Vector:

Description:
The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

Other Info:

Solution:
Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.

X-content-type-options missing :



```
HTTP/1.1 200 OK
Date: Sun, 11 Jan 2026 14:47:54 GMT
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Cache-Control: no-cache, max-age=0, must-revalidate, no-store
Content-Type: text/html;charset=UTF-8
Content-Language: en-US
Keep-Alive: timeout=5, max=100
```

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <title>Zero - Personal Banking - Loans - Credit Cards</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">
    <meta http-equiv="X-UA-Compatible" content="IE=Edge">
```

- Alerts (8)
  - Content Security Policy (CSP) Header Not Set
  - Cross-Domain Misconfiguration (Systemic)
  - Missing Anti-clickjacking Header
  - Vulnerable JS Library
  - Server Leaks Version Information via "Server" HTTP Response Header Field (Systemic)
  - X-Content-Type-Options Header Missing (Systemic)
    - GET:http://zero.webappsecurity.com/
    - GET:http://zero.webappsecurity.com/resources/css/font-awesome.css
    - GET:http://zero.webappsecurity.com/resources/css/main.css
    - GET:http://zero.webappsecurity.com/resources/js/bootstrap.min.js
    - GET:http://zero.webappsecurity.com/resources/js/placeholders.min.js
  - Information Disclosure - Suspicious Comments
  - Modern Web Application

Attack:
Evidence:
CWE ID: 693
WASC ID: 15
Source: Passive (10021 - X-Content-Type-Options Header Missing)
Input Vector:

Description:
The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

Other Info:
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.
At "High" threshold this scan rule will not alert on client or server error responses.

Solution:
Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.
If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed

5.Insecure Cookies

Description:

Some cookies were observed without recommended flags such as:

Secure : false (should be True for sensitive cookies such as session ID)

SameSite : “None”(should be “Strict” or “Lax”)

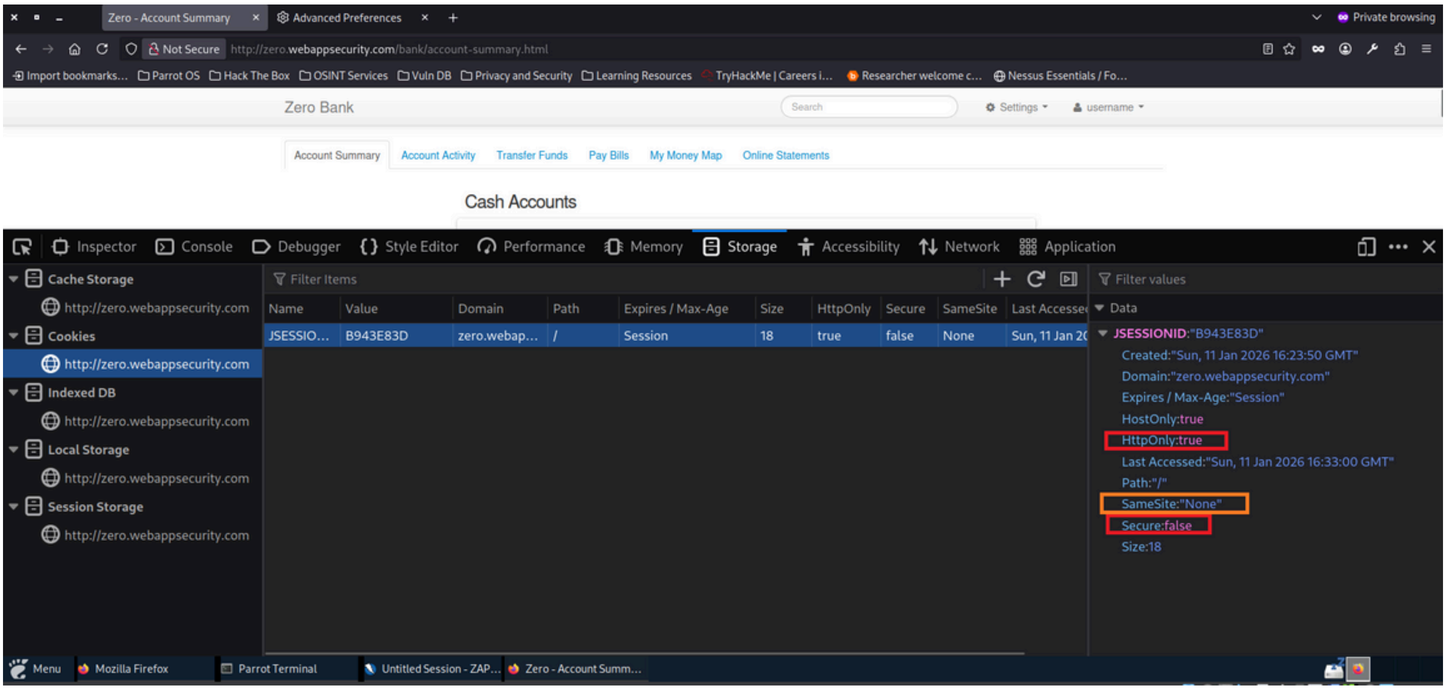
Risk Classification: MEDIUM

Remediation:

Apply Secure and HttpOnly flags to all session cookies ,Use SameSite=Strict or Lax where applicable

Tools used : Browser Devtools

Evidence:



Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accesse
JSESSIO…	B943E83D	zero.webap…	/	Session	18	true	false	None	Sun, 11 Jan 20

```
Data
JSESSIONID:"B943E83D"
  Created:"Sun, 11 Jan 2026 16:23:50 GMT"
  Domain:"zero.webappsecurity.com"
  Expires / Max-Age:"Session"
  HostOnly:true
  HttpOnly:true
  Last Accessed:"Sun, 11 Jan 2026 16:33:00 GMT"
  Path:"/"
  SameSite:"None"
  Secure:false
  Size:18
```