Cyber Security Vulnerability Assessment Report :

Website Tested:

http://testphp.vulnweb.com
http://testhtml5.vulnweb.com/

Prepared by: Thejas R Shetty

CIN : FIT/FEB26/CS6248

Cyber Security Internship – Future Interns

Date: 14/02/2026

Introduction :

A **vulnerability** assessment is the process of identifying and analysing security weaknesses in a system or website.

Website security testing is important because it helps detect risks early, protect sensitive data, and prevent cyber attacks.

Type of Website :

Public intentionally vulnerable testing platform.

Target Website URL:

http://testphp.vulnweb.com

For Zmap Scanning:

http://testhtml5.vulnweb.com/

Project Objective :

The objective of this assessment is to evaluate the security posture of a public website using safe and read-only testing methods.

This assessment aims to:

- Identify common security weaknesses
- Analyse exposed services and technologies
- Classify the risk levels
- Recommend practical security improvements

Tools Used :

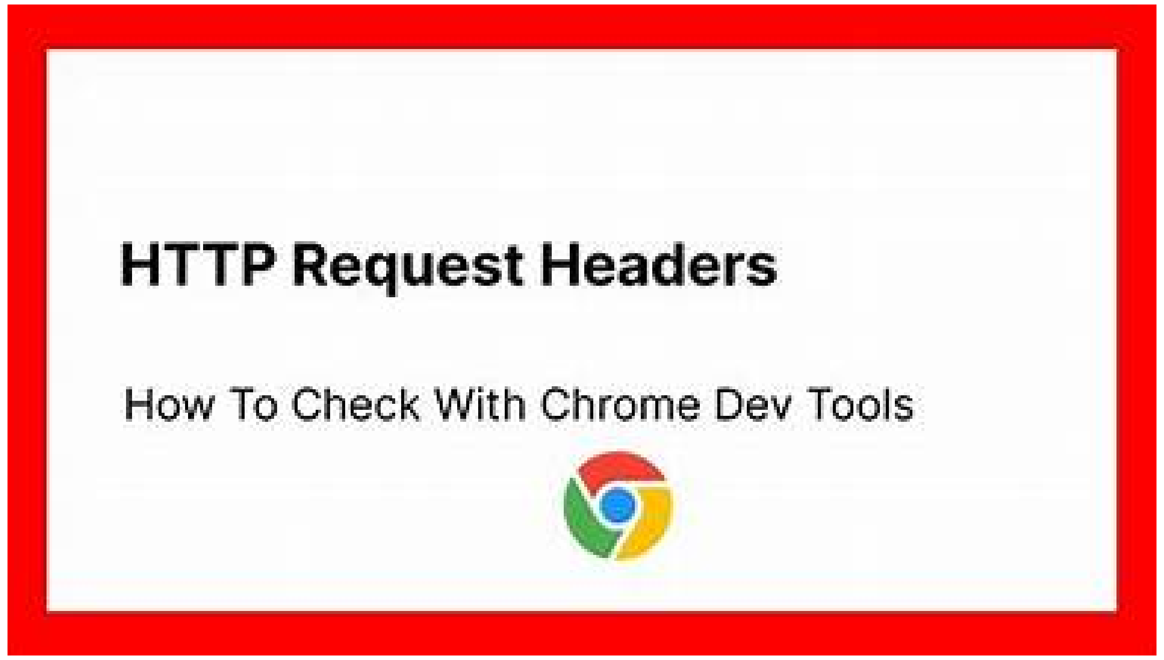
The following tools were used to perform the assessment :

- **Nmap –>** Network scanning and port detection
- **Web Browser** –> HTTP response header inspection
- **Owasp Zap** –> Vulnerability scanning
- **Web Dev Tools** –> Security Headers Analysis

ZAP->

Nmap->

WebDev Tool->



HTTP Request Headers

How To Check With Chrome Dev Tools

Testing Type :

- *Passive vulnerability assessment*
- *Read-only testing performed*
- *No exploitation attempted*
- *Only publicly accessible pages analysed*

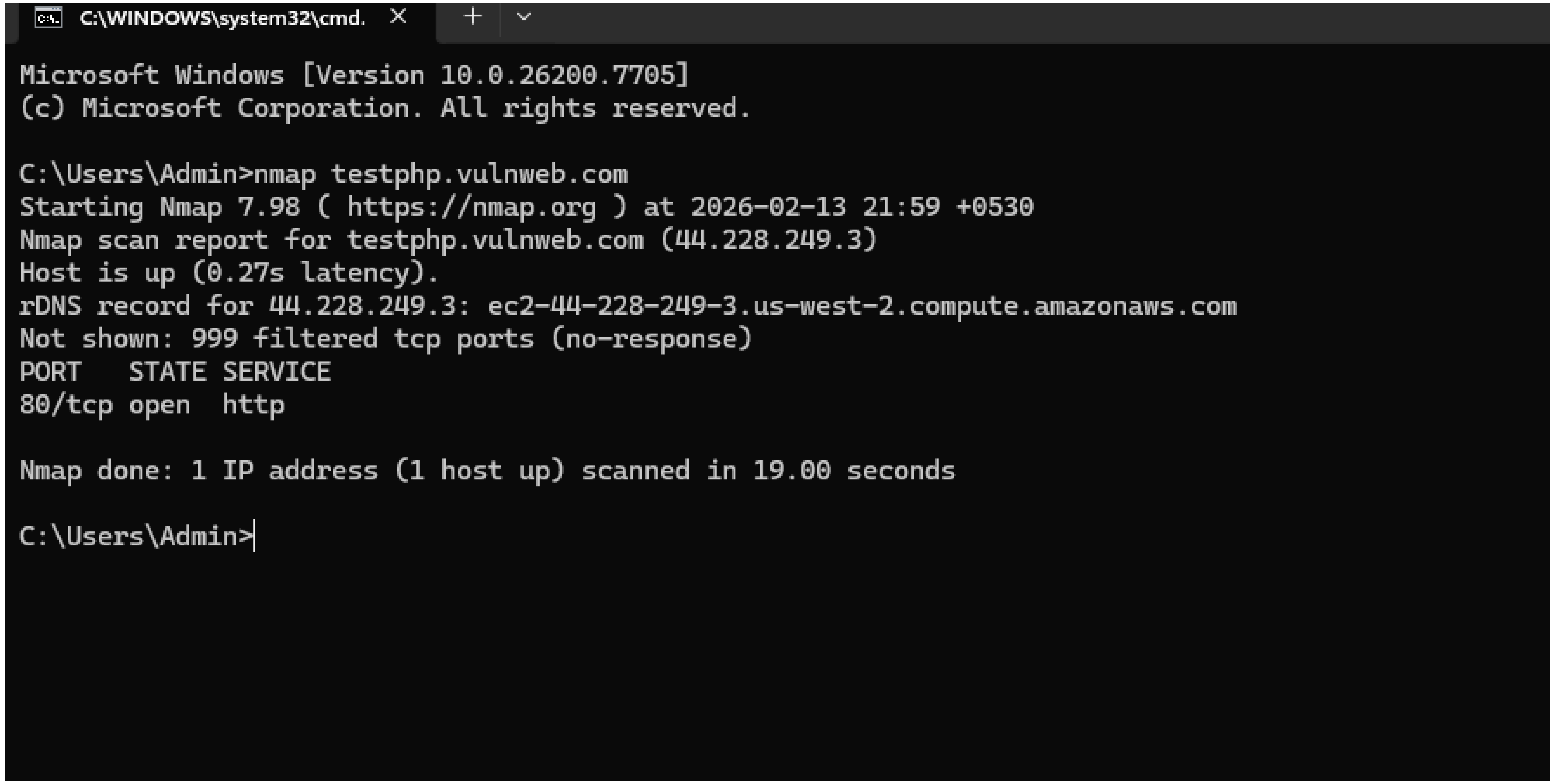
Testing Methodology :

The following steps were performed:

1. Selected a public test website
2. Conducted network scan using Nmap
3. Identified open ports and active services
4. Inspected HTTP response headers
5. Identified security weaknesses
6. Classified risks
7. Recommended mitigation steps

Nmap Scan Result :

- Open ports detected on the target system
- Running services identified
- Server information collected



```
Microsoft Windows [Version 10.0.26200.7705]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>nmap testphp.vulnweb.com
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-13 21:59 +0530
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.27s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 19.00 seconds

C:\Users\Admin>
```

Figure 1: Nmap Port Scan Result

Browser Developer Tools Result

Tool Used : Browser Developer Tools
Target Website : http://testphp.vulnweb.com
Scan Method : Manual Header Inspection

Short Result :

Server and PHP version information are visible in response ***headers. Security*** headers are missing.

Risk Level : Medium

Conclusion :

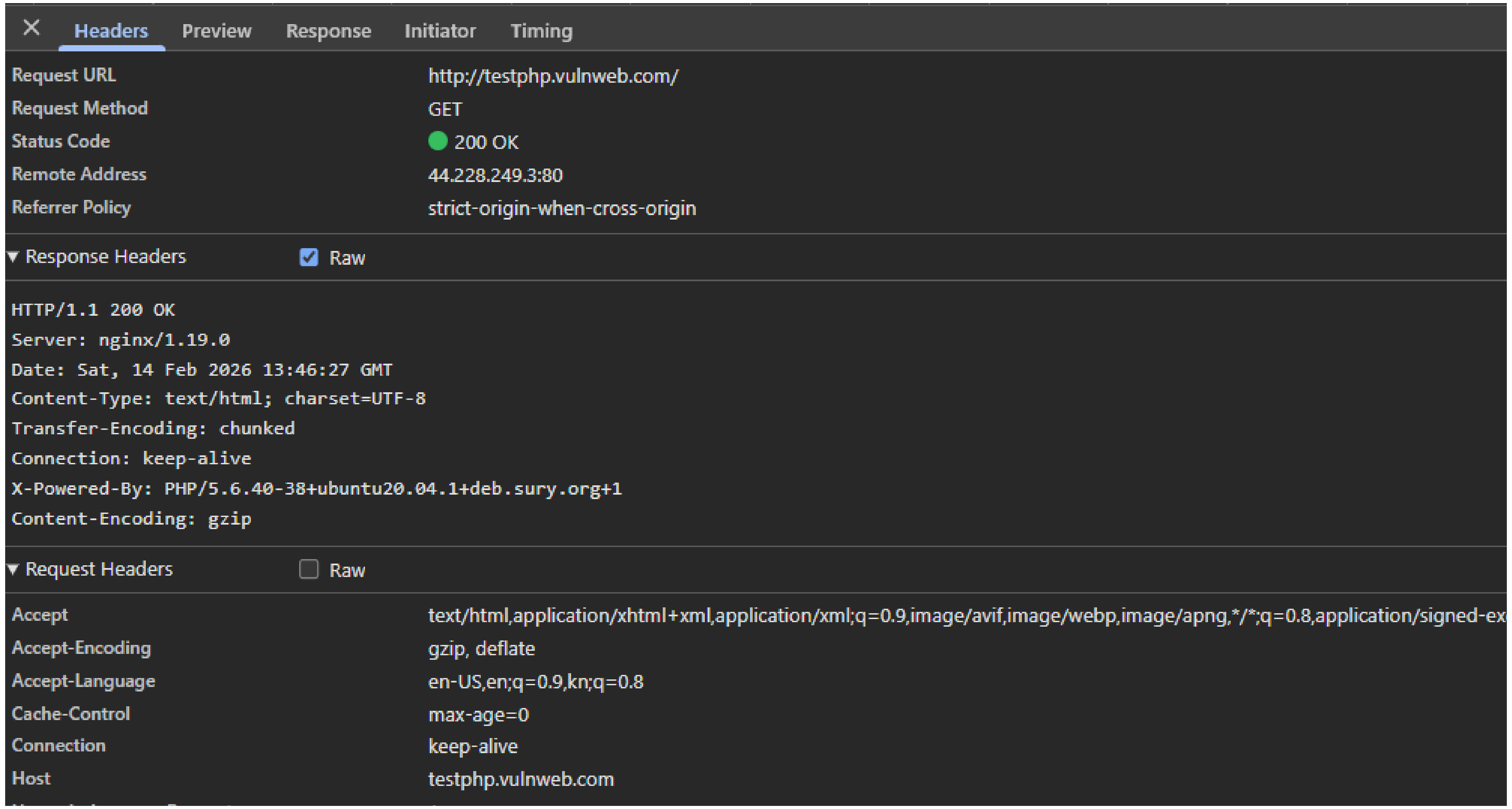
Exposed server details may help attackers identify vulnerabilities. Security headers should be added.

Security Header Analysis :

HTTP response headers reveal server details

Technology stack information visible

Server configuration information exposed



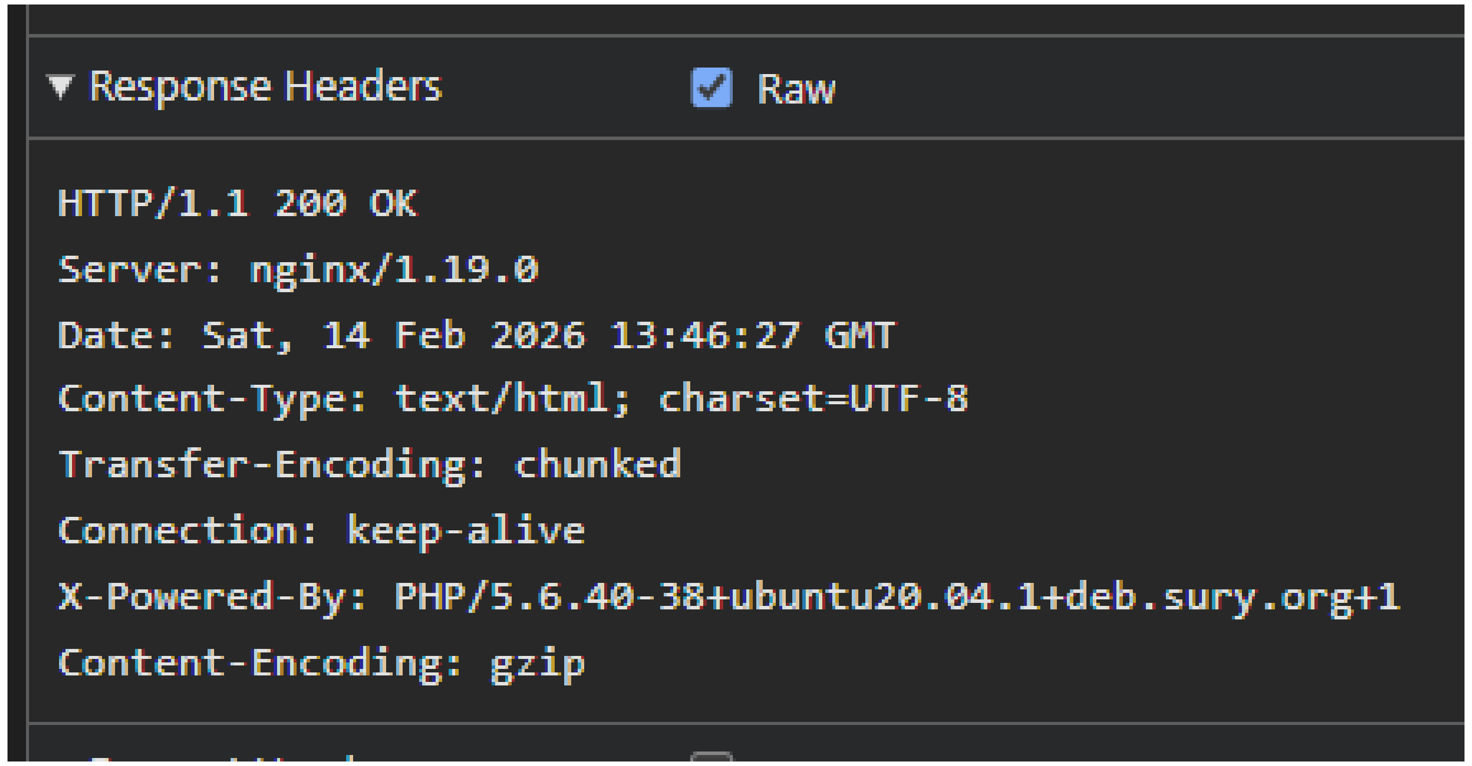
Request URL	http://testphp.vulnweb.com/
Request Method	GET
Status Code	● 200 OK
Remote Address	44.228.249.3:80
Referrer Policy	strict-origin-when-cross-origin

▾ Response Headers ☑ Raw

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Sat, 14 Feb 2026 13:46:27 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
```

▾ Request Headers ☐ Raw

Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
Accept-Encoding	gzip, deflate
Accept-Language	en-US,en;q=0.9,kn;q=0.8
Cache-Control	max-age=0
Connection	keep-alive
Host	testphp.vulnweb.com


▾ Response Headers ☑ Raw

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Sat, 14 Feb 2026 13:46:27 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
```

Figure 2: HTTP Response Header Output

Technical Description of Vulnerability :

“The web server discloses software version information through HTTP response headers. This may allow attackers to identify known vulnerabilities associated with specific software versions.”

Identified Vulnerability :

Server version exposed: nginx/1.19.0
PHP version exposed: PHP 5.6.40

Risk:

Attackers can identify outdated software and exploit known vulnerabilities.
Public vulnerability databases (CVE, NVD) may contain exploits for these versions.

Risk Level:

Medium

Recommended Fix:

Hide server and technology version information.

Risk Classification :

Vulnerability	Risk Level
Server version disclosure	Medium
PHP version disclosure	Medium
Missing security headers	Medium
HTTP usage (no encryption)	Medium
Open ports exposure	Low

OWASP ZAP Scan Result :

Tool Used : OWASP ZAP

Target Website : http://testhtml5.vulnweb.com/
Scan Method : Automated Scan

Result :
OWASP ZAP detected missing security headers and cookie security issues.

Risk Level : Medium

Conclusion :
Missing protections may allow web attacks such as session hijacking.

OWASP ZAP Alert Details

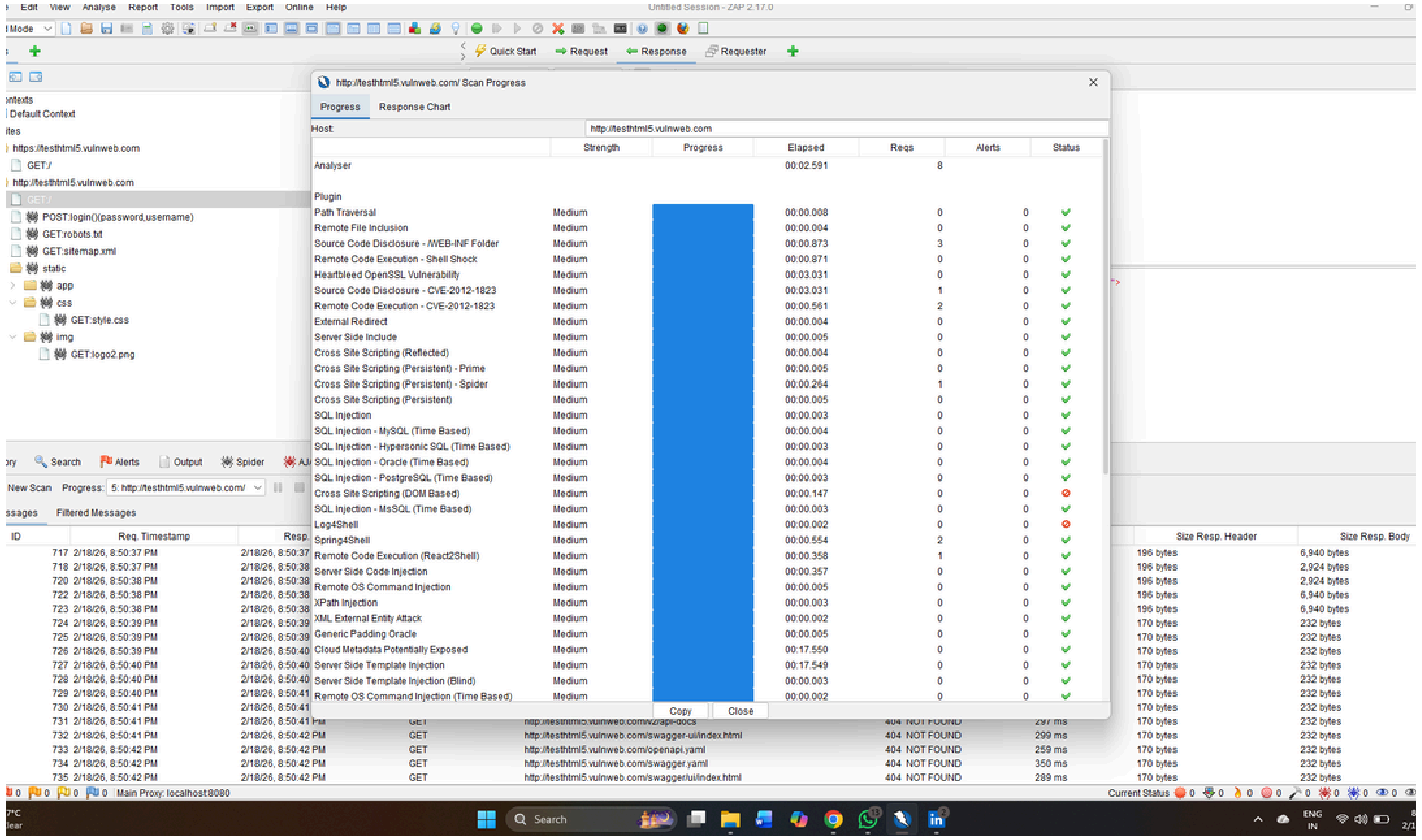
Tool Used : OWASP ZAP
Target Website : http://testhtml5.vulnweb.com/
Scan Method : Automated Scan

Result :
Multiple alerts were identified, indicating security misconfiguration.

Risk Level : Medium

Conclusion :
Security configuration improvements are required to protect the web application.

Image Description :
This screenshot shows detailed vulnerability information in OWASP ZAP. It confirms detected issues and provides evidence of security weaknesses.


Untitled Session - ZAP 2.17.0
Edit View Analyse Report Tools Import Export Online Help
Quick Start
Request
Response
Requester
Search
Alerts
Output
Spider
New Scan
Progress: 5: http://testhtml5.vulnweb.com/
Filtered Messages

http://testhtml5.vulnweb.com/ Scan Progress

Progress | Response Chart

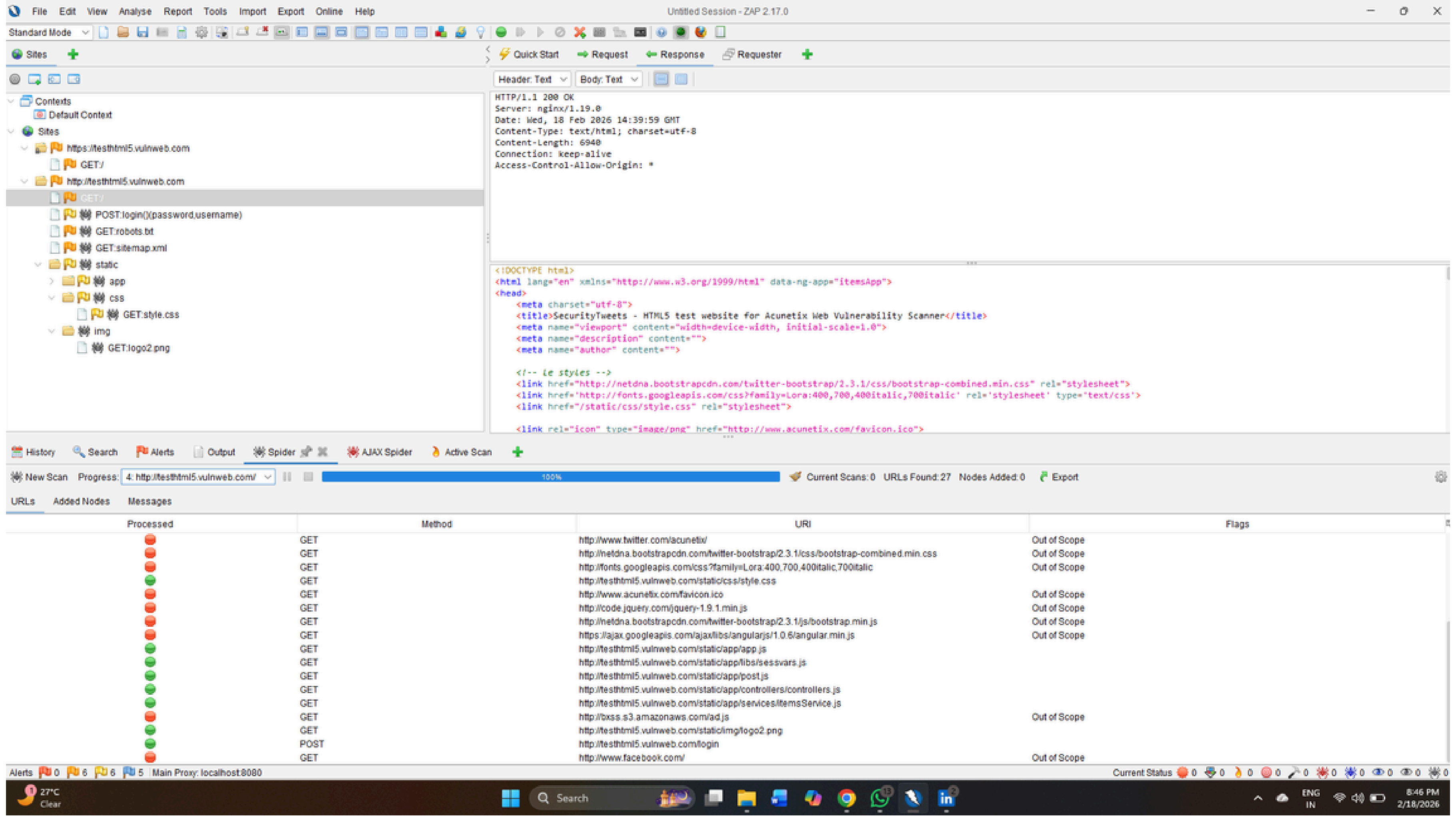
Host: http://testhtml5.vulnweb.com

	Strength	Progress	Elapsed	Reqs	Alerts	Status
Analyser			00:02.591	8		
Plugin						
Path Traversal	Medium		00:00.008	0	0	✓
Remote File Inclusion	Medium		00:00.004	0	0	✓
Source Code Disclosure - /WEB-INF Folder	Medium		00:00.873	3	0	✓
Remote Code Execution - Shell Shock	Medium		00:00.871	0	0	✓
Heartbleed OpenSSL Vulnerability	Medium		00:03.031	0	0	✓
Source Code Disclosure - CVE-2012-1823	Medium		00:03.031	1	0	✓
Remote Code Execution - CVE-2012-1823	Medium		00:00.561	2	0	✓
External Redirect	Medium		00:00.004	0	0	✓
Server Side Include	Medium		00:00.005	0	0	✓
Cross Site Scripting (Reflected)	Medium		00:00.004	0	0	✓
Cross Site Scripting (Persistent) - Prime	Medium		00:00.005	0	0	✓
Cross Site Scripting (Persistent) - Spider	Medium		00:00.264	1	0	✓
Cross Site Scripting (Persistent)	Medium		00:00.005	0	0	✓
SQL Injection	Medium		00:00.003	0	0	✓
SQL Injection - MySQL (Time Based)	Medium		00:00.004	0	0	✓
SQL Injection - Hypersonic SQL (Time Based)	Medium		00:00.003	0	0	✓
SQL Injection - Oracle (Time Based)	Medium		00:00.004	0	0	✓
SQL Injection - PostgreSQL (Time Based)	Medium		00:00.003	0	0	✓
Cross Site Scripting (DOM Based)	Medium		00:00.147	0	0	⊘
SQL Injection - MsSQL (Time Based)	Medium		00:00.003	0	0	✓
Log4Shell	Medium		00:00.002	0	0	⊘
Spring4Shell	Medium		00:00.554	2	0	✓
Remote Code Execution (React2Shell)	Medium		00:00.358	1	0	✓
Server Side Code Injection	Medium		00:00.357	0	0	✓
Remote OS Command Injection	Medium		00:00.005	0	0	✓
XPath Injection	Medium		00:00.003	0	0	✓
XML External Entity Attack	Medium		00:00.002	0	0	✓
Generic Padding Oracle	Medium		00:00.005	0	0	✓
Cloud Metadata Potentially Exposed	Medium		00:17.550	0	0	✓
Server Side Template Injection	Medium		00:17.549	0	0	✓
Server Side Template Injection (Blind)	Medium		00:00.003	0	0	✓
Remote OS Command Injection (Time Based)	Medium		00:00.002	0	0	✓

Copy | Close

ID	Req. Timestamp	Resp.					Size Resp. Header	Size Resp. Body
717	2/18/26, 8:50:37 PM	2/18/26, 8:50:37					196 bytes	6,940 bytes
718	2/18/26, 8:50:37 PM	2/18/26, 8:50:38					196 bytes	2,924 bytes
720	2/18/26, 8:50:38 PM	2/18/26, 8:50:38					196 bytes	2,924 bytes
722	2/18/26, 8:50:38 PM	2/18/26, 8:50:38					196 bytes	6,940 bytes
723	2/18/26, 8:50:38 PM	2/18/26, 8:50:38					196 bytes	6,940 bytes
724	2/18/26, 8:50:39 PM	2/18/26, 8:50:39					170 bytes	232 bytes
725	2/18/26, 8:50:39 PM	2/18/26, 8:50:39					170 bytes	232 bytes
726	2/18/26, 8:50:39 PM	2/18/26, 8:50:40					170 bytes	232 bytes
727	2/18/26, 8:50:40 PM	2/18/26, 8:50:40					170 bytes	232 bytes
728	2/18/26, 8:50:40 PM	2/18/26, 8:50:40					170 bytes	232 bytes
729	2/18/26, 8:50:40 PM	2/18/26, 8:50:41					170 bytes	232 bytes
730	2/18/26, 8:50:41 PM	2/18/26, 8:50:41					170 bytes	232 bytes
731	2/18/26, 8:50:41 PM	2/18/26, 8:50:41 PM	GET	http://testhtml5.vulnweb.com/v2/api-docs	404	NOT FOUND	297 ms	170 bytes	232 bytes
732	2/18/26, 8:50:41 PM	2/18/26, 8:50:42 PM	GET	http://testhtml5.vulnweb.com/swagger-ui/index.html	404	NOT FOUND	299 ms	170 bytes	232 bytes
733	2/18/26, 8:50:42 PM	2/18/26, 8:50:42 PM	GET	http://testhtml5.vulnweb.com/openapi.yaml	404	NOT FOUND	259 ms	170 bytes	232 bytes
734	2/18/26, 8:50:42 PM	2/18/26, 8:50:42 PM	GET	http://testhtml5.vulnweb.com/swagger.yaml	404	NOT FOUND	350 ms	170 bytes	232 bytes
735	2/18/26, 8:50:42 PM	2/18/26, 8:50:42 PM	GET	http://testhtml5.vulnweb.com/swagger/ui/index.html	404	NOT FOUND	289 ms	170 bytes	232 bytes

Main Proxy: localhost:8080



```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Wed, 18 Feb 2026 14:39:59 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 6940
Connection: keep-alive
Access-Control-Allow-Origin: *
```

```
<!DOCTYPE html>
<html lang="en" xmlns="http://www.w3.org/1999/html" data-ng-app="itemsApp">
<head>
    <meta charset="utf-8">
    <title>SecurityTweets - HTML5 test website for Acunetix Web Vulnerability Scanner</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta name="description" content="">
    <meta name="author" content="">

    <!-- Le styles -->
    <link href="http://netdna.bootstrapcdn.com/twitter-bootstrap/2.3.1/css/bootstrap-combined.min.css" rel="stylesheet">
    <link href='http://fonts.googleapis.com/css?family=Lora:400,700,400italic,700italic' rel='stylesheet' type='text/css'>
    <link href="/static/css/style.css" rel="stylesheet">

    <link rel="icon" type="image/png" href="http://www.acunetix.com/favicon.ico">
```

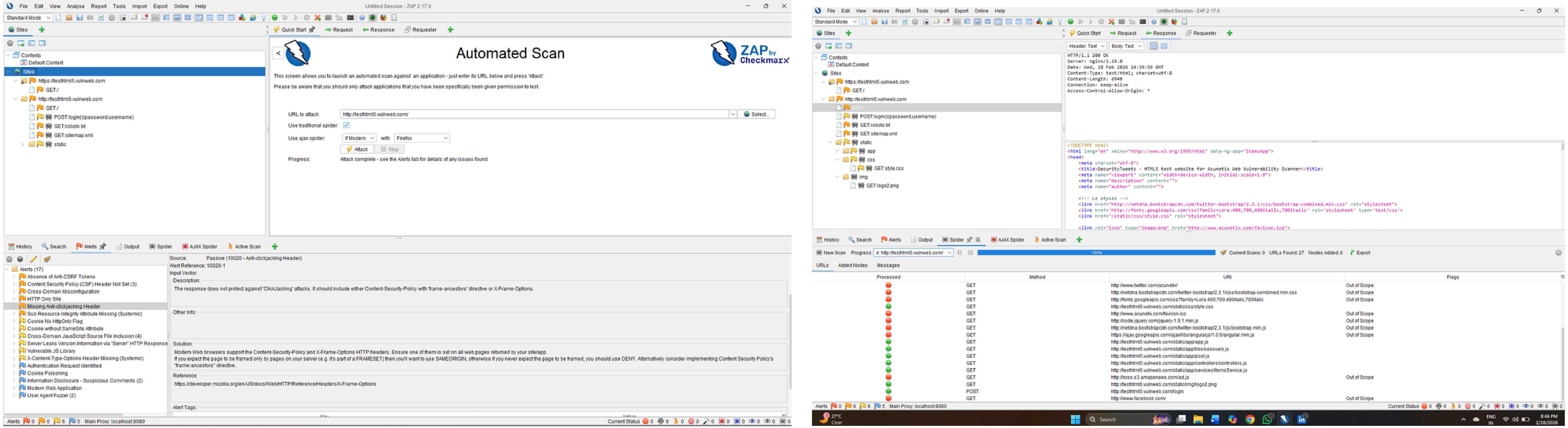
Progress: 4: http://testhtml5.vulnweb.com/ 100% Current Scans: 0 URLs Found: 27 Nodes Added: 0

Processed	Method	URI	Flags
🟥	GET	http://www.twitter.com/acunetix/	Out of Scope
🟥	GET	http://netdna.bootstrapcdn.com/twitter-bootstrap/2.3.1/css/bootstrap-combined.min.css	Out of Scope
🟥	GET	http://fonts.googleapis.com/css?family=Lora:400,700,400italic,700italic	Out of Scope
🟩	GET	http://testhtml5.vulnweb.com/static/css/style.css	
🟥	GET	http://www.acunetix.com/favicon.ico	Out of Scope
🟥	GET	http://code.jquery.com/jquery-1.9.1.min.js	Out of Scope
🟥	GET	http://netdna.bootstrapcdn.com/twitter-bootstrap/2.3.1/js/bootstrap.min.js	Out of Scope
🟥	GET	https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js	Out of Scope
🟩	GET	http://testhtml5.vulnweb.com/static/app/app.js	
🟩	GET	http://testhtml5.vulnweb.com/static/app/libs/sessvars.js	
🟩	GET	http://testhtml5.vulnweb.com/static/app/post.js	
🟩	GET	http://testhtml5.vulnweb.com/static/app/controllers/controllers.js	
🟩	GET	http://testhtml5.vulnweb.com/static/app/services/itemsService.js	
🟥	GET	http://bxss.s3.amazonaws.com/ad.js	Out of Scope
🟩	GET	http://testhtml5.vulnweb.com/static/img/logo2.png	
🟩	POST	http://testhtml5.vulnweb.com/login	
🟥	GET	http://www.facebook.com/	Out of Scope

Alerts 0 6 6 5 Main Proxy: localhost:8080

Figure 3 : ZAP Scanning

Figure 3 : ZMAP Scan Result



Contexts
Default Context
Sites
https://testhtml5.vulnweb.com
GET:/
http://testhtml5.vulnweb.com
GET:/
POST:login()(password,username)
GET:robots.txt
GET:sitemap.xml
static

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://testhtml5.vulnweb.com/ Select...

Use traditional spider: ☑

Use ajax spider: If Modern with Firefox

Attack Stop

Progress: Attack complete - see the Alerts tab for details of any issues found

Alerts (17)
- Absence of Anti-CSRF Tokens
- Content Security Policy (CSP) Header Not Set (3)
- Cross-Domain Misconfiguration
- HTTP Only Site
- Missing Anti-clickjacking Header
- Sub Resource Integrity Attribute Missing (Systemic)
- Cookie No HttpOnly Flag
- Cookie without SameSite Attribute
- Cross-Domain JavaScript Source File Inclusion (4)
- Server Leaks Version Information via "Server" HTTP Response
- Vulnerable JS Library
- X-Content-Type-Options Header Missing (Systemic)
- Authentication Request Identified
- Cookie Poisoning
- Information Disclosure - Suspicious Comments (2)
- Modern Web Application
- User Agent Fuzzer (2)

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.
If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.

Reference:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/X-Frame-Options

Alert Tags:

Alerts 0 6 6 5 Main Proxy: localhost:8080 Current Status 0 0 0 0 0 0 0 0 0 0

Contexts
Default Context
Sites
https://testhtml5.vulnweb.com
GET:/
http://testhtml5.vulnweb.com
GET:/
POST:login()(password,username)
GET:robots.txt
GET:sitemap.xml
static
app
css
GET:style.css
img
GET:logo2.png

Header: Text Body: Text

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Wed, 18 Feb 2026 14:39:59 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 6940
Connection: keep-alive
Access-Control-Allow-Origin: *
```

```
<!DOCTYPE html>
<html lang="en" xmlns="http://www.w3.org/1999/html" data-ng-app="itemsApp">
<head>
    <meta charset="utf-8">
    <title>SecurityTweets - HTML5 test website for Acunetix Web Vulnerability Scanner</title>
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta name="description" content="">
    <meta name="author" content="">

    <!-- Le styles -->
    <link href="http://netdna.bootstrapcdn.com/twitter-bootstrap/2.3.1/css/bootstrap-combined.min.css" rel="stylesheet">
    <link href='http://fonts.googleapis.com/css?family=Lora:400,700,400italic,700italic' rel='stylesheet' type='text/css'>
    <link href="/static/css/style.css" rel="stylesheet">

    <link rel="icon" type="image/png" href="http://www.acunetix.com/favicon.ico">
```

New Scan Progress: 4: http://testhtml5.vulnweb.com/ 100% Current Scans: 0 URLs Found: 27 Nodes Added: 0 Export

URLs Added Nodes Messages

Processed	Method	URI	Flags
●	GET	http://www.twitter.com/acunetix/	Out of Scope
●	GET	http://netdna.bootstrapcdn.com/twitter-bootstrap/2.3.1/css/bootstrap-combined.min.css	Out of Scope
●	GET	http://fonts.googleapis.com/css?family=Lora:400,700,400italic,700italic	Out of Scope
●	GET	http://testhtml5.vulnweb.com/static/css/style.css	
●	GET	http://www.acunetix.com/favicon.ico	Out of Scope
●	GET	http://code.jquery.com/jquery-1.9.1.min.js	Out of Scope
●	GET	http://netdna.bootstrapcdn.com/twitter-bootstrap/2.3.1/js/bootstrap.min.js	Out of Scope
●	GET	https://ajax.googleapis.com/ajax/libs/angularjs/1.0.6/angular.min.js	Out of Scope
●	GET	http://testhtml5.vulnweb.com/static/app/app.js	
●	GET	http://testhtml5.vulnweb.com/static/app/libs/sessvars.js	
●	GET	http://testhtml5.vulnweb.com/static/app/post.js	
●	GET	http://testhtml5.vulnweb.com/static/app/controllers/controllers.js	
●	GET	http://testhtml5.vulnweb.com/static/app/services/itemsService.js	
●	GET	http://bxss.s3.amazonaws.com/ad.js	Out of Scope
●	GET	http://testhtml5.vulnweb.com/static/img/logo2.png	
●	POST	http://testhtml5.vulnweb.com/login	
●	GET	http://www.facebook.com/	Out of Scope

Alerts 0 6 6 5 Main Proxy: localhost:8080 Current Status 0 0 0 0 0 0 0 0 0 0

Figure 4 : ZAP Scanning Alert

Limitations of Assessment :

- Only passive testing performed
- No authenticated testing
- No vulnerability exploitation
- Results limited to visible configurations

Conclusion

- Security testing successfully performed
- Information disclosure vulnerability identified
- Risk level classified as medium
- Security improvements recommended

“Proper configuration hardening can significantly reduce the attack surface.”