Vulnerability Assessment Report

Public Website Security Review (Read-Only Scope)

Website Tested : testphp.vulnweb.com

Prepared By : Dama Karthikeya

Role : Cyber Security Intern (Beginner Level)

Date : 29-01-2026

1. Introduction

This report presents a vulnerability assessment conducted on a publicly accessible website.

The purpose of this assessment is to identify common security weaknesses that may affect the

confidentiality and integrity of the website.

The assessment was performed using non-intrusive and ethical techniques.

No exploitation or attack activities were conducted during this review.

2. Environment Setup

Operating System

- Kali Linux

Target Application

- testphp.vulnweb.com
- Intentionally vulnerable demo application by Acunetix

Tools

- OWASP ZAP (Zed Attack Proxy)
- curl (command-line HTTP client)

---

3. Scope and Ethics

Scope of Assessment:

• Public-facing pages only

• Read-only and passive analysis

• No login or authentication testing

Activities Not Performed:

• Exploitation of vulnerabilities

• Brute-force attacks

• Denial-of-Service (DoS)

• Any action that could impact website availability

4. Tools Used

The objective of this assessment is to:

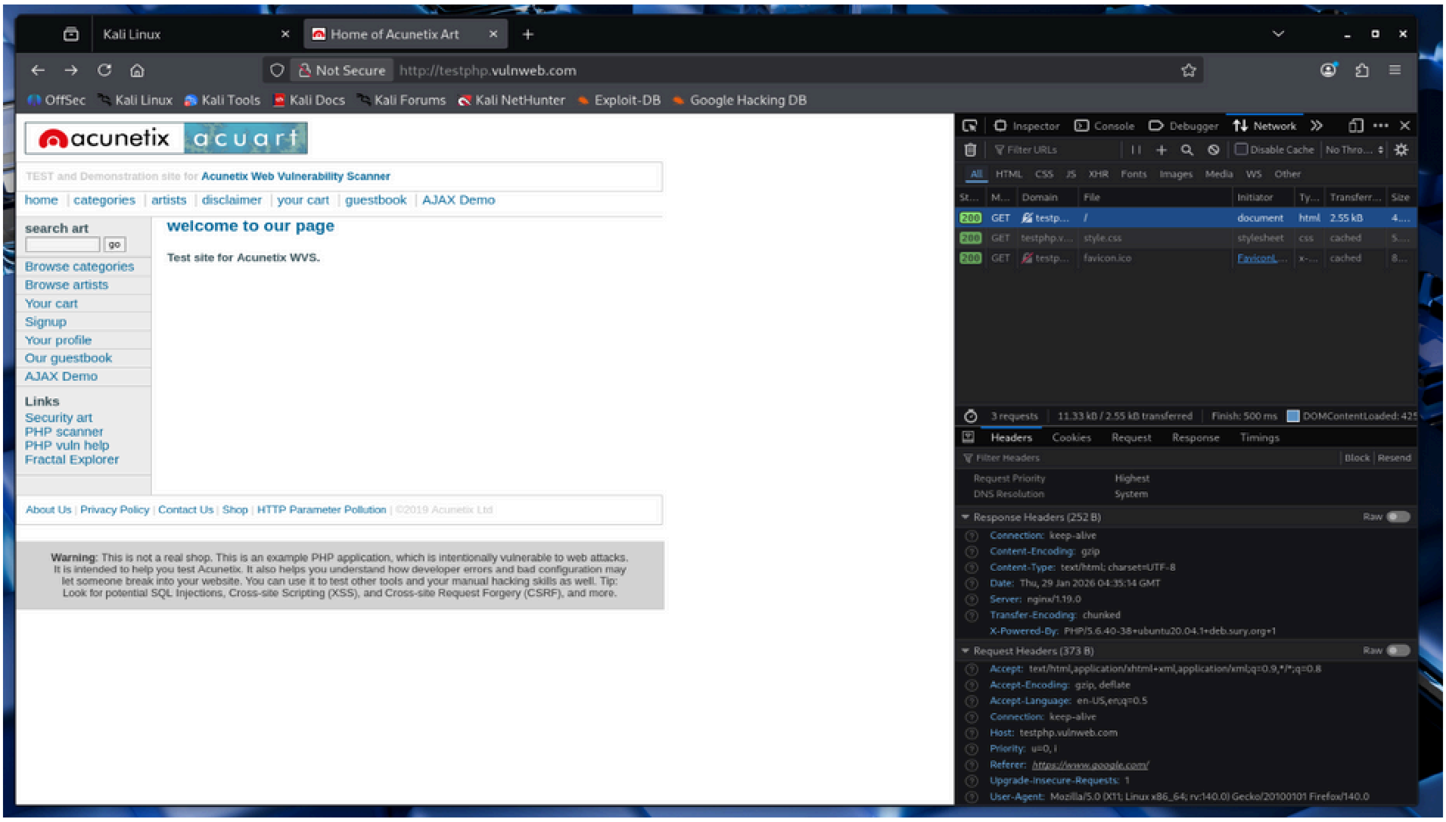
- Identify visible security weaknesses on a public website
- Analyze risks in a business-friendly manner
- Classify issues based on risk level
- Provide clear and practical remediation recommendations

The following tools were used during the assessment:

- Kali Linux – Testing environment
- Firefox Browser – Manual inspection
- OWASP ZAP – Passive vulnerability analysis
- Nmap – Basic port and exposure analysis

5. Summary of Findings

Finding	Risk Level
Missing Security Headers	Medium
Port Scan Filtering Detected	Low



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

welcome to our page

Test site for Acunetix WVS.

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

St...	M...	Domain	File	Initiator	Ty...	Transferr...	Size
200	GET	testp...	/	document	html	2.55 kB	4....
200	GET	testphp.v...	style.css	stylesheet	css	cached	5....
200	GET	testp...	favicon.ico	FaviconL...	x-...	cached	8...

```
3 requests | 11.33 kB / 2.55 kB transferred | Finish: 500 ms | DOMContentLoaded: 425

Request Priority    Highest
DNS Resolution      System

Response Headers (252 B)
Connection: keep-alive
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Thu, 29 Jan 2026 04:35:14 GMT
Server: nginx/1.19.0
Transfer-Encoding: chunked
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1

Request Headers (373 B)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Host: testphp.vulnweb.com
Priority: u=0, i
Referer: https://www.google.com/
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
```

6. Finding : Missing Security Headers

Risk Level: Medium

Description:

The website does not implement important HTTP security headers such as

Content-Security-Policy, X-Frame-Options, and Strict-Transport-Security.

Impact:

The absence of these headers may expose users to browser-based attacks

including clickjacking, cross-site scripting, and insecure communication.

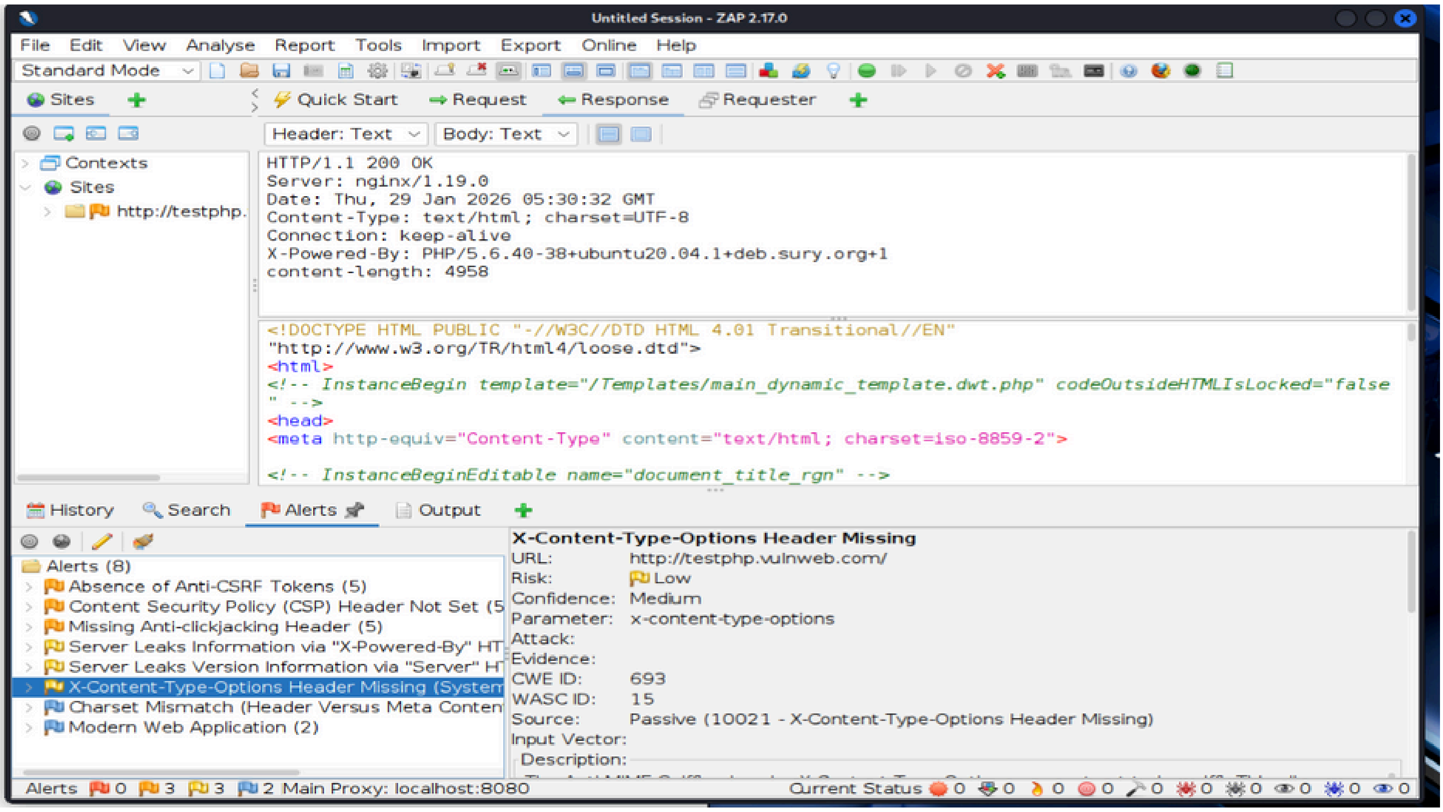
Evidence:

Browser inspection and OWASP ZAP passive scan alerts confirming missing headers.

Remediation:

Configure the web server to include recommended HTTP security headers

in all responses.



```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Thu, 29 Jan 2026 05:30:32 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
content-length: 4958
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false
" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
```

```
Alerts (8)
  Absence of Anti-CSRF Tokens (5)
  Content Security Policy (CSP) Header Not Set (5
  Missing Anti-clickjacking Header (5)
  Server Leaks Information via "X-Powered-By" HT
  Server Leaks Version Information via "Server" H
  X-Content-Type-Options Header Missing (System
  Charset Mismatch (Header Versus Meta Conten
  Modern Web Application (2)
```

```
X-Content-Type-Options Header Missing
URL:          http://testphp.vulnweb.com/
Risk:         Low
Confidence:   Medium
Parameter:    x-content-type-options
Attack:
Evidence:
CWE ID:       693
WASC ID:      15
Source:       Passive (10021 - X-Content-Type-Options Header Missing)
Input Vector:
Description:
```

```
Alerts 0 3 3 2 Main Proxy: localhost:8080          Current Status 0 0 0 0 0 0 0 0 0 0
```

---

7. Finding : Port Scanning Restricted by Firewall

Risk Level : Low (Informational)

Description:

A basic Nmap fast scan was performed to identify exposed services.

The results indicate that the target server actively filters port scan requests.

Impact:

Filtering of port scan traffic reduces the attack surface and limits

information exposure to potential attackers.

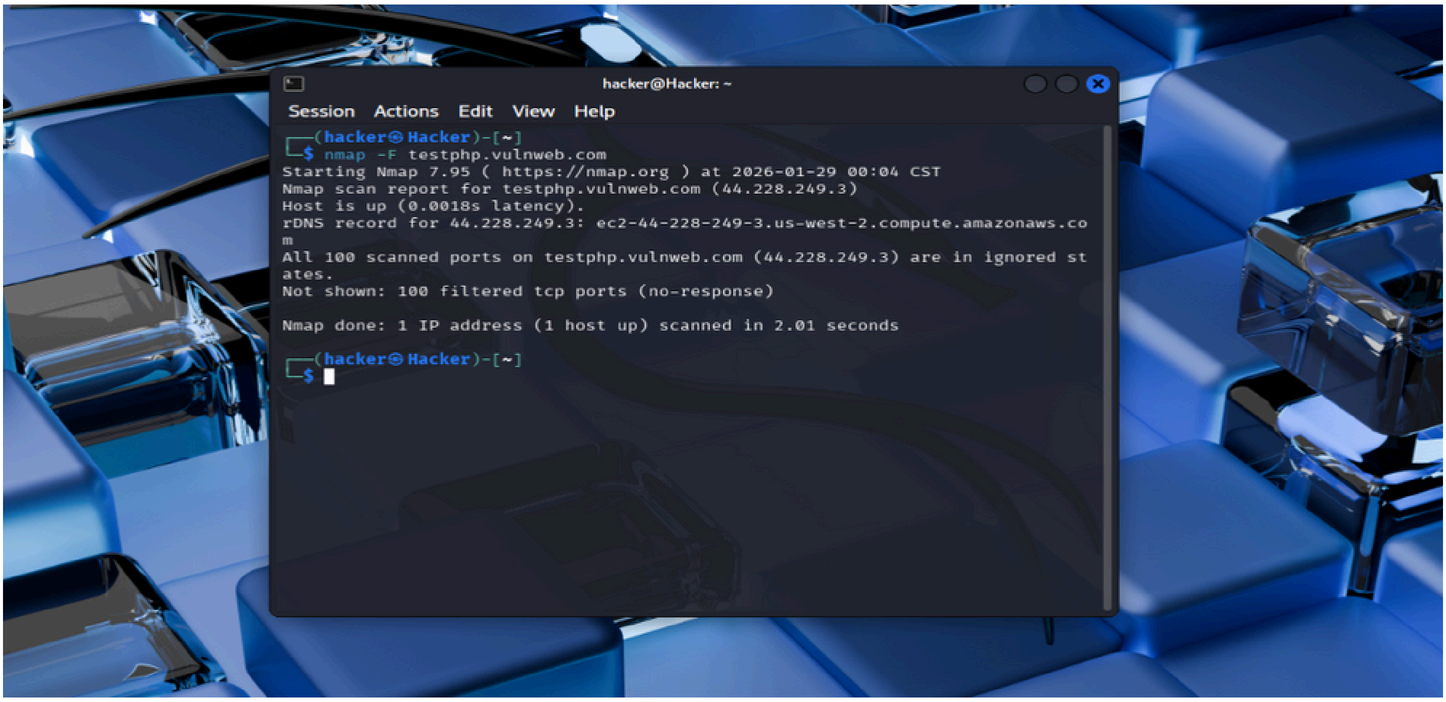
Evidence:

Screenshot of Nmap scan output showing filtered ports.

Remediation:

No immediate action required. Continue maintaining existing firewall

and cloud security configurations.



```
┌──(hacker㉿Hacker)-[~]
└─$ nmap -F testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-29 00:04 CST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.0018s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.co
m
All 100 scanned ports on testphp.vulnweb.com (44.228.249.3) are in ignored st
ates.
Not shown: 100 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 2.01 seconds

┌──(hacker㉿Hacker)-[~]
└─$ 
```

8. Conclusion

The vulnerability assessment identified a small number of security

misconfigurations that are common in many public websites.

While no critical vulnerabilities were observed, implementing recommended

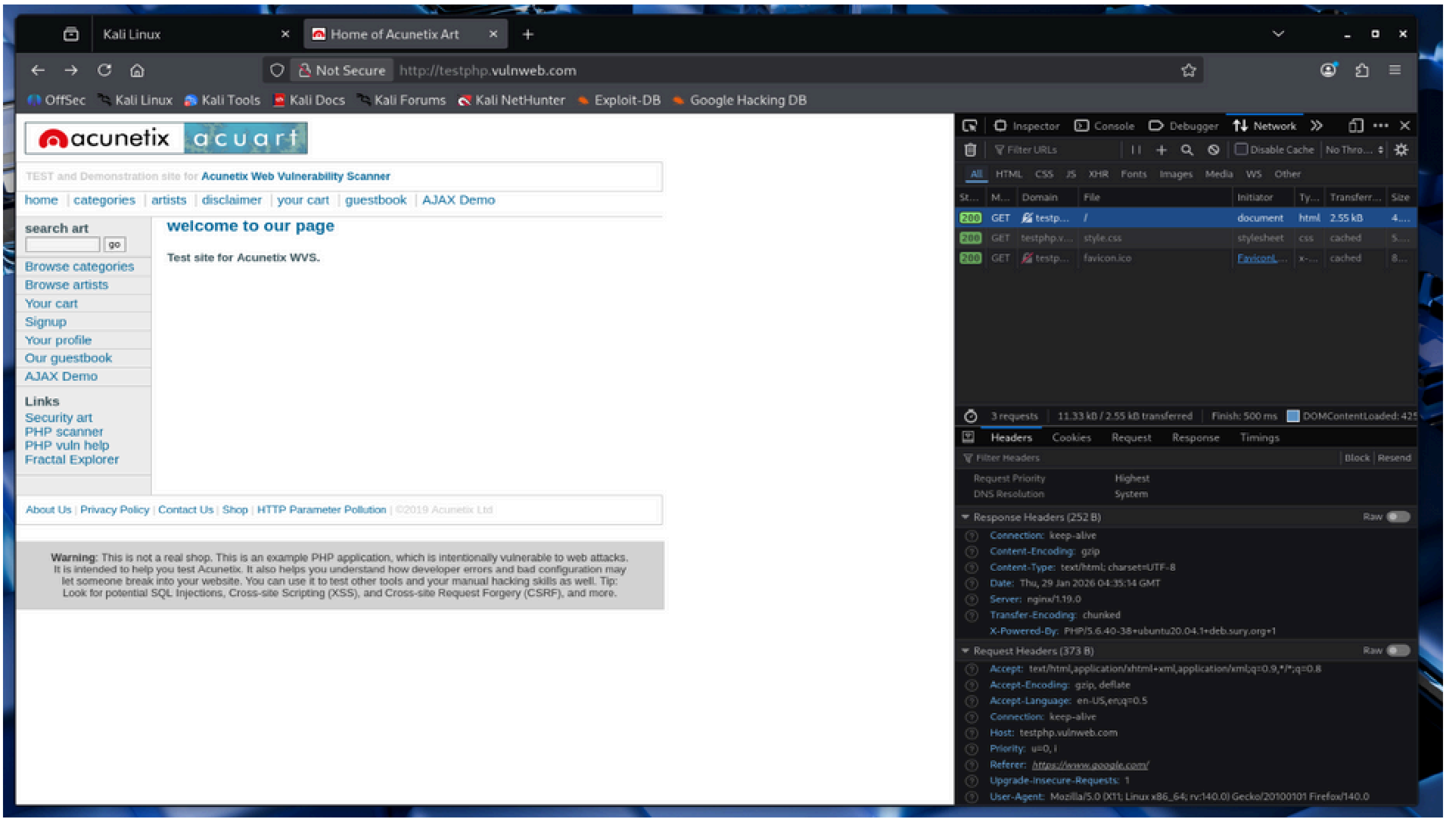
security headers would significantly improve the website's security posture.

Overall, the website demonstrates a reasonable level of protection,

with opportunities for improvement through configuration hardening.

Appendix

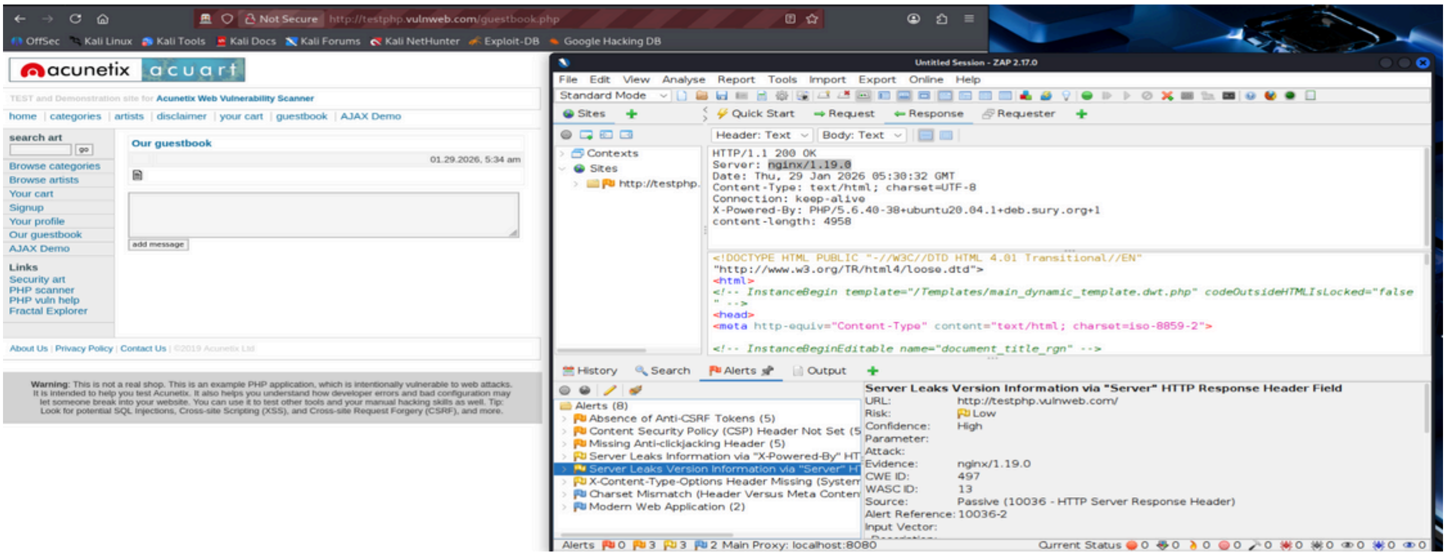
Figure 1: Browser response headers showing missing security headers



```
Response Headers (252 B)
Connection: keep-alive
Content-Encoding: gzip
Content-Type: text/html; charset=UTF-8
Date: Thu, 29 Jan 2026 04:35:14 GMT
Server: nginx/1.19.0
Transfer-Encoding: chunked
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1

Request Headers (373 B)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Host: testphp.vulnweb.com
Priority: u=0, i
Referer: https://www.google.com/
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
```

Figure 2: OWASP ZAP passive scan alert – Content Security Policy header not set

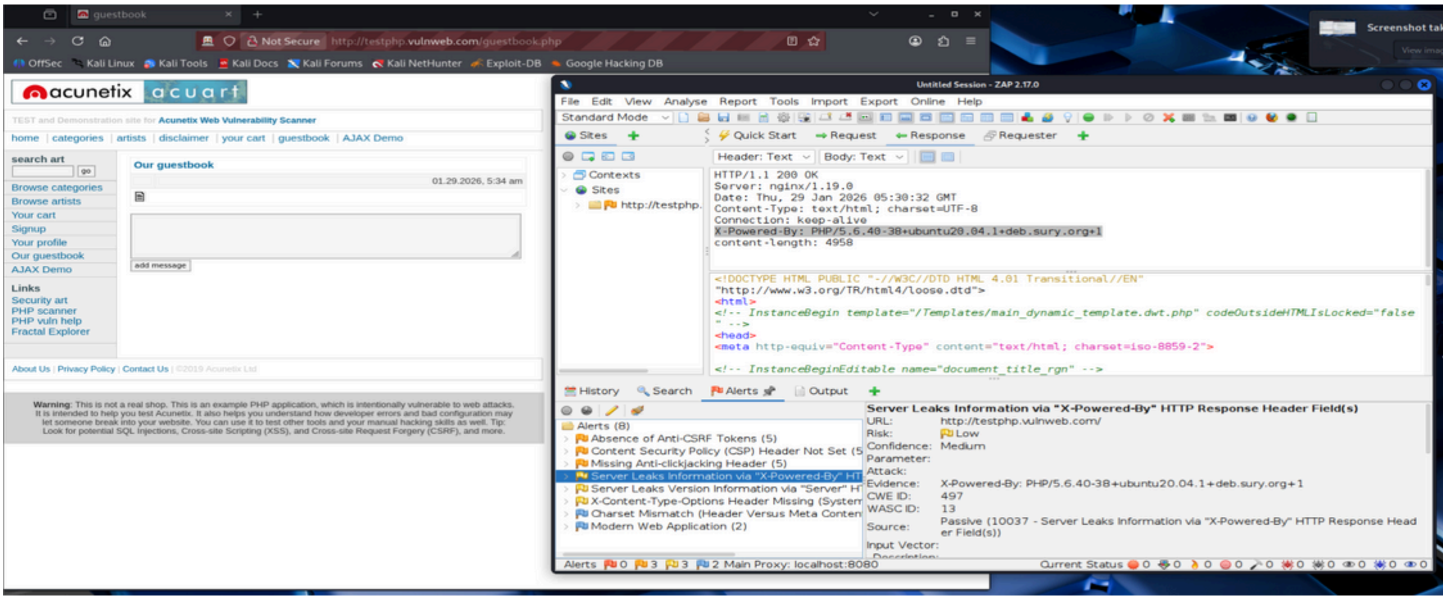


```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Thu, 29 Jan 2026 05:30:32 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
content-length: 4958
```

```
Alerts (8)
  Absence of Anti-CSRF Tokens (5)
  Content Security Policy (CSP) Header Not Set (5
  Missing Anti-clickjacking Header (5)
  Server Leaks Information via "X-Powered-By" HT
  Server Leaks Version Information via "Server" H
  X-Content-Type-Options Header Missing (System
  Charset Mismatch (Header Versus Meta Conten
  Modern Web Application (2)
```

```
Server Leaks Version Information via "Server" HTTP Response Header Field
URL:             http://testphp.vulnweb.com/
Risk:            Low
Confidence:      High
Parameter:
Attack:
Evidence:        nginx/1.19.0
CWE ID:          497
WASC ID:         13
Source:          Passive (10036 - HTTP Server Response Header)
Alert Reference: 10036-2
Input Vector:
```

Figure 3: OWASP ZAP passive scan alert – Content Security Policy header not set



TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

Our guestbook

01.29.2026, 5:34 am

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Thu, 29 Jan 2026 05:30:32 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
content-length: 4958
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false
" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
```

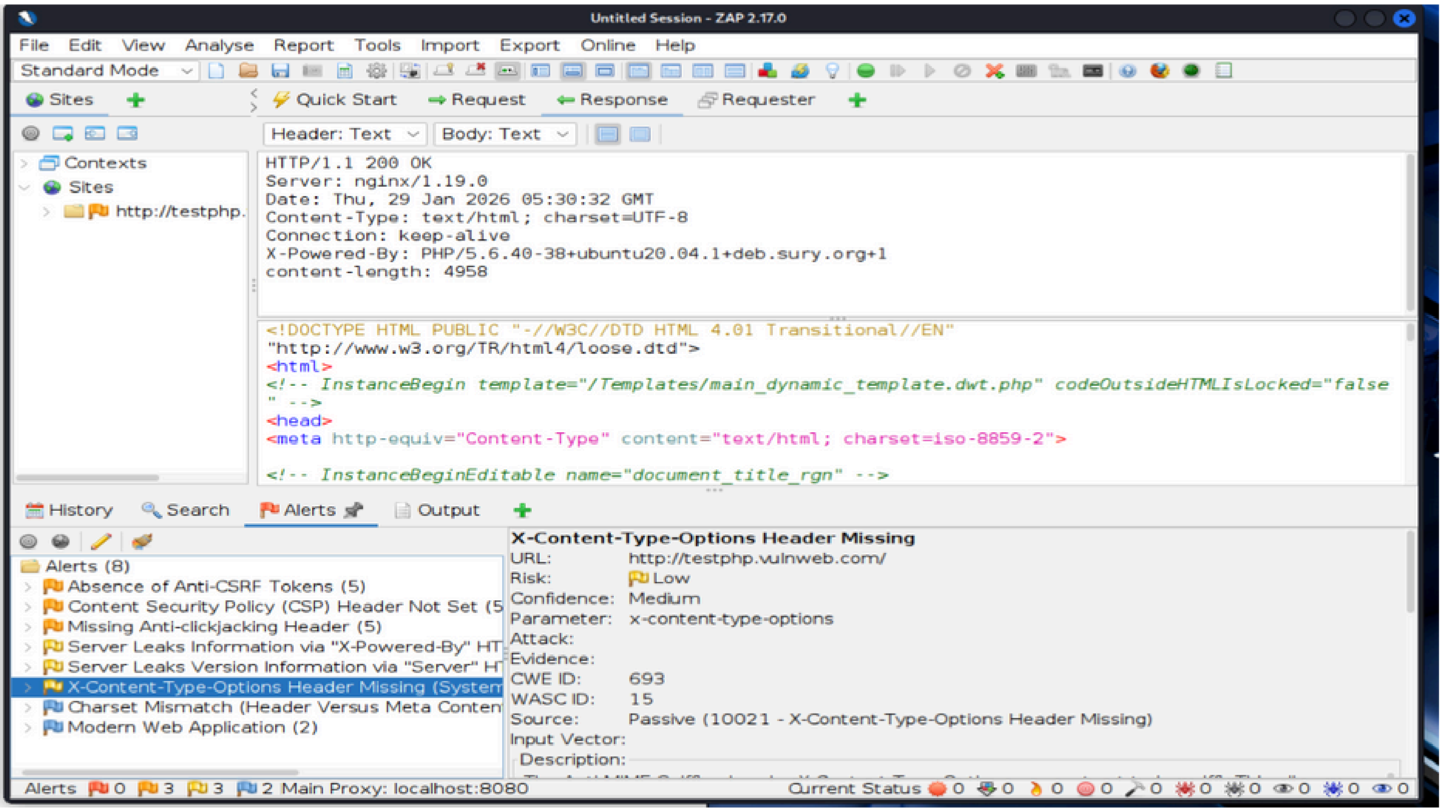
Alerts (8)
- Absence of Anti-CSRF Tokens (5)
- Content Security Policy (CSP) Header Not Set (5
- Missing Anti-clickjacking Header (5)
- Server Leaks Information via "X-Powered-By" HT
- Server Leaks Version Information via "Server" H
- X-Content-Type-Options Header Missing (System
- Charset Mismatch (Header Versus Meta Conten
- Modern Web Application (2)

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

URL: http://testphp.vulnweb.com/
Risk: Low
Confidence: Medium
Parameter:
Attack:
Evidence: X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
CWE ID: 497
WASC ID: 13
Source: Passive (10037 - Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))
Input Vector:
Description:

Alerts 0 3 3 2 Main Proxy: localhost:8080 Current Status 0 0 0 0 0 0 0 0 0 0

Figure 4: OWASP ZAP alert showing missing X-Frame-Options header



```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Thu, 29 Jan 2026 05:30:32 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
content-length: 4958
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
<!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false
" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
```

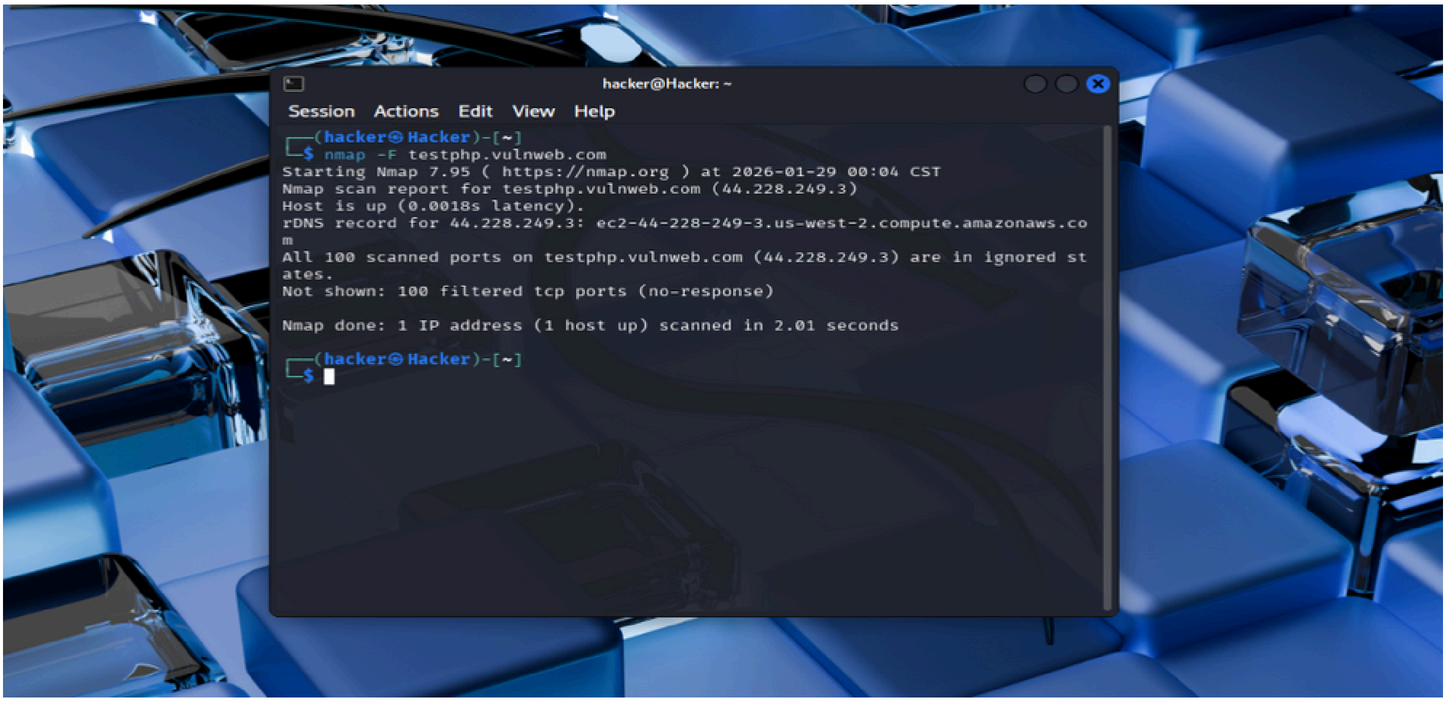
Alerts (8)
- Absence of Anti-CSRF Tokens (5)
- Content Security Policy (CSP) Header Not Set (5
- Missing Anti-clickjacking Header (5)
- Server Leaks Information via "X-Powered-By" HT
- Server Leaks Version Information via "Server" H
- X-Content-Type-Options Header Missing (System
- Charset Mismatch (Header Versus Meta Conten
- Modern Web Application (2)

X-Content-Type-Options Header Missing

URL: http://testphp.vulnweb.com/
Risk: Low
Confidence: Medium
Parameter: x-content-type-options
Attack:
Evidence:
CWE ID: 693
WASC ID: 15
Source: Passive (10021 - X-Content-Type-Options Header Missing)
Input Vector:
Description:

Alerts 0 3 3 2 Main Proxy: localhost:8080 Current Status 0 0 0 0 0 0 0 0 0 0

Figure 5: Nmap fast scan output showing filtered ports



```
┌──(hacker㉿Hacker)-[~]
└─$ nmap -F testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-29 00:04 CST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.0018s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.co
m
All 100 scanned ports on testphp.vulnweb.com (44.228.249.3) are in ignored st
ates.
Not shown: 100 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 2.01 seconds

┌──(hacker㉿Hacker)-[~]
└─$ 
```