Vulnerability Assessment Report

Cyber Security Internship – Task 1

1.1 Introduction

This report presents the findings of a vulnerability assessment performed on the web application testphp.vulnweb.com. The objective of this assessment was to identify potential security weaknesses, misconfigurations, and outdated software that could be exploited by malicious actors.

1.2 Executive Summary

During the assessment, several critical and medium-severity vulnerabilities were discovered. The application is running on an outdated tech stack (PHP 5.6.40), which is no longer supported and contains numerous known security flaws. Additionally, the lack of modern security headers and CSRF protections exposes users to data theft and session hijacking.

2.1 Scope of Statement

The scope of this assessment was limited to the following:

- **Target URL:** http://testphp.vulnweb.com
- **Infrastructure:** Web server fingerprinting and port scanning.
- **Application Security:** Passive scanning of web headers and basic input validation.

2.2 Tools Used

To ensure a comprehensive analysis, the following industry-standard tools were utilized:

- **Nmap (Zenmap):** Used for network discovery and service version detection.
- **OWASP ZAP (Passive):** Utilized for identifying common web vulnerabilities like missing headers and CSRF issues.
- **Browser DevTools:** Used for manual inspection of HTTP Response Headers and network traffic.

Technical Analysis

Finding 01: Outdated Software Version

- **Severity: High**
- **Description:** The server is running Nginx 1.19.0 and PHP 5.6.40. PHP 5.6 has reached its End-of-Life (EOL) and no longer receives security patches.
- **Evidence:** Nmap output shows Port 80 open with version nginx 1.19.0 and PHP/5.6.40.

Finding 02: Missing Security Headers

- **Severity: Medium**
- **Description:** Critical security headers such as Content-Security-Policy (CSP) and X-Frame-Options are missing.
- **Impact:** This makes the site vulnerable to Clickjacking and Cross-Site Scripting (XSS) attacks.

Finding 03: Lack of Anti-CSRF Tokens

- **Severity: Medium**
- **Description:** The application forms do not utilize unique tokens to prevent Cross-Site Request Forgery.
- **Evidence:** OWASP ZAP Alert: "Absence of Anti-CSRF Tokens" detected on search.php.

Finding 04: Information Disclosure via Headers

- **Severity: Low**
- **Description:** The X-Powered-By header reveals the exact version of PHP being used.
- **Impact:** This helps attackers tailor their exploits to specific known vulnerabilities.

5.1 Remediation Steps

To secure the application, the following actions are highly recommended:

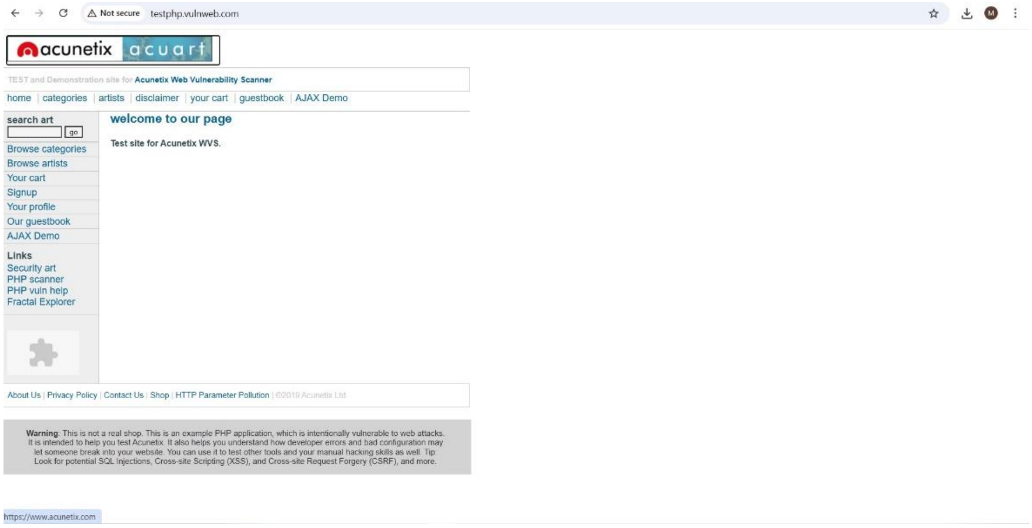
1. **Upgrade PHP:** Immediately move from PHP 5.6.40 to a supported version (e.g., PHP 8.2 or higher).
2. **Implement Security Headers:** Configure the Nginx server to send X-Frame-Options: DENY and a strict Content-Security-Policy.
3. **Enable CSRF Protection:** Integrate unique per-session tokens for all sensitive forms and state-changing requests.

4. **Disable Information Disclosure:** Modify the php.ini file to set expose_php = Off to hide version numbers from headers.

5.2 Conclusion

The assessment confirms that testphp.vulnweb.com currently operates with significant security gaps. Implementing the above remediation steps will drastically reduce the attack surface and protect user data.

Proof of concept



⚠ Not secure testphp.vulnweb.com

acunetix acuart

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

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art [go]

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

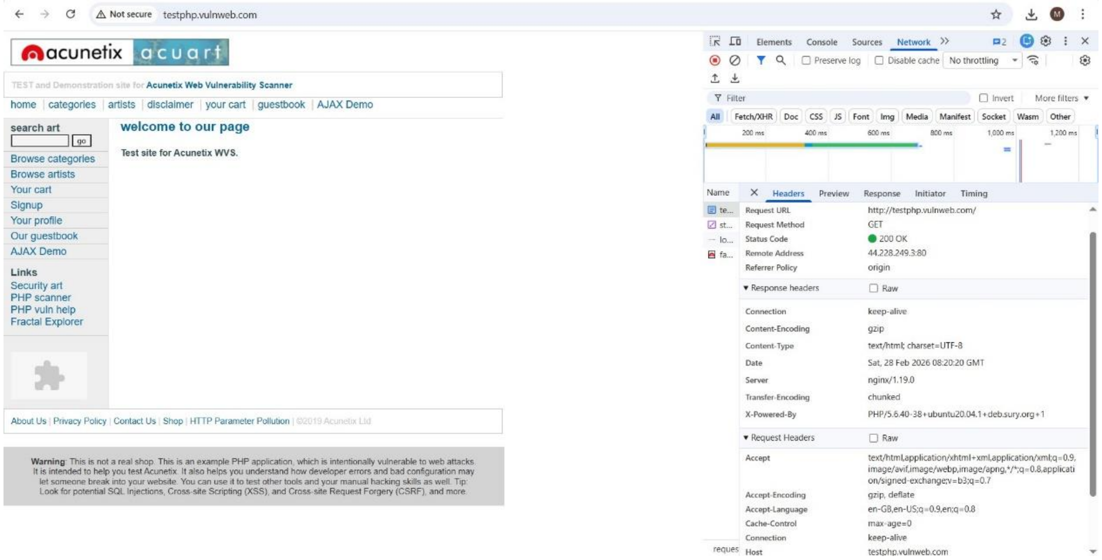
welcome to our page

Test site for Acunetix WVS.

About Us | Privacy Policy | Contact Us | Shop | HTTP Parameter Pollution | ©2019 Acunetix Ltd

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.

https://www.acunetix.com



⚠ Not secure testphp.vulnweb.com

acunetix acuart

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

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art [go]

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

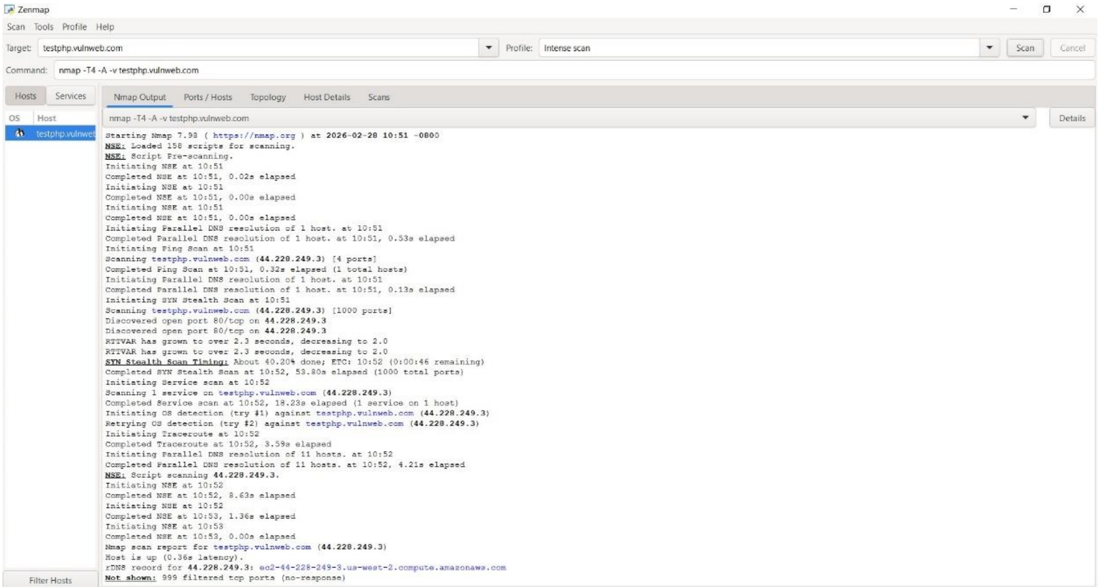
welcome to our page

Test site for Acunetix WVS.

About Us | Privacy Policy | Contact Us | Shop | HTTP Parameter Pollution | ©2019 Acunetix Ltd

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.

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

▾ Response headers   □ Raw

Connection           keep-alive
Content-Encoding     gzip
Content-Type         text/html; charset=UTF-8
Date                 Sat, 28 Feb 2026 08:20:20 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    □ Raw

Accept               text/html,application/xhtml+xml,application/xml;q=0.9,
                     image/avif,image/webp,image/apng,*/*;q=0.8,applicati
                     on/signed-exchange;v=b3;q=0.7
Accept-Encoding      gzip, deflate
Accept-Language      en-GB,en-US;q=0.9,en;q=0.8
Cache-Control        max-age=0
Connection           keep-alive
Host                 testphp.vulnweb.com
```

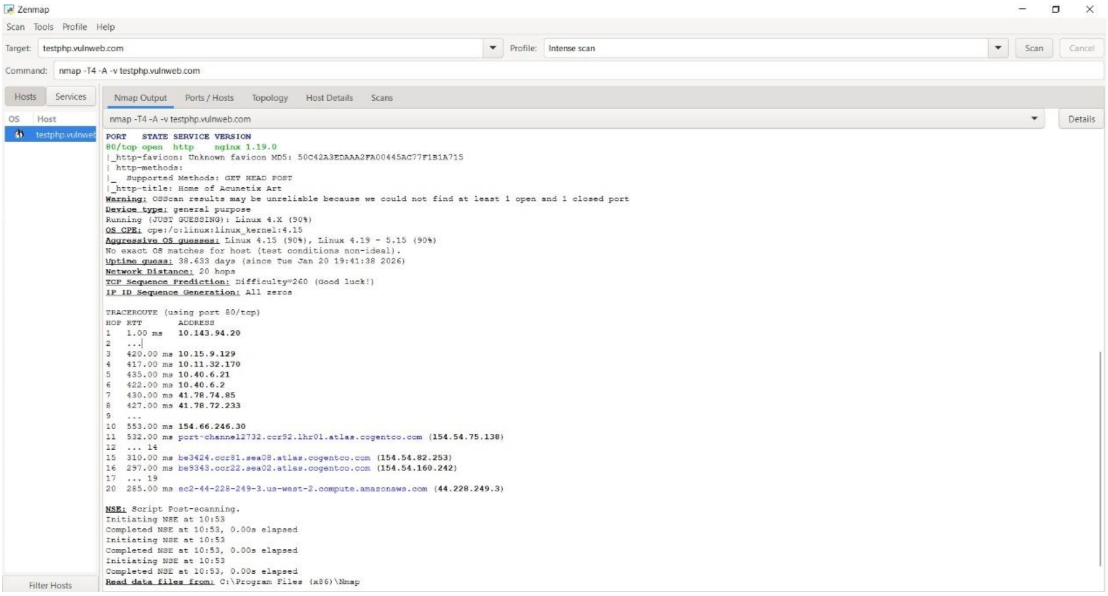


Target: testphp.vulnweb.com

Profile: Intense scan

Command: nmap -T4 -A -v testphp.vulnweb.com

```
nmap -T4 -A -v testphp.vulnweb.com
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-28 10:51 -0800
NSE: Loaded 158 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:51
Completed NSE at 10:51, 0.02s elapsed
Initiating NSE at 10:51
Completed NSE at 10:51, 0.00s elapsed
Initiating NSE at 10:51
Completed NSE at 10:51, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 10:51
Completed Parallel DNS resolution of 1 host. at 10:51, 0.53s elapsed
Initiating Ping Scan at 10:51
Scanning testphp.vulnweb.com (44.228.249.3) [4 ports]
Completed Ping Scan at 10:51, 0.32s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:51
Completed Parallel DNS resolution of 1 host. at 10:51, 0.13s elapsed
Initiating SYN Stealth Scan at 10:51
Scanning testphp.vulnweb.com (44.228.249.3) [1000 ports]
Discovered open port 80/tcp on 44.228.249.3
Discovered open port 80/tcp on 44.228.249.3
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
SYN Stealth Scan Timing: About 40.20% done; ETC: 10:52 (0:00:46 remaining)
Completed SYN Stealth Scan at 10:52, 53.80s elapsed (1000 total ports)
Initiating Service scan at 10:52
Scanning 1 service on testphp.vulnweb.com (44.228.249.3)
Completed Service scan at 10:52, 18.23s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against testphp.vulnweb.com (44.228.249.3)
Retrying OS detection (try #2) against testphp.vulnweb.com (44.228.249.3)
Initiating Traceroute at 10:52
Completed Traceroute at 10:52, 3.59s elapsed
Initiating Parallel DNS resolution of 11 hosts. at 10:52
Completed Parallel DNS resolution of 11 hosts. at 10:52, 4.21s elapsed
NSE: Script scanning 44.228.249.3.
Initiating NSE at 10:52
Completed NSE at 10:52, 8.63s elapsed
Initiating NSE at 10:52
Completed NSE at 10:53, 1.36s elapsed
Initiating NSE at 10:53
Completed NSE at 10:53, 0.00s elapsed
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.36s 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)
```

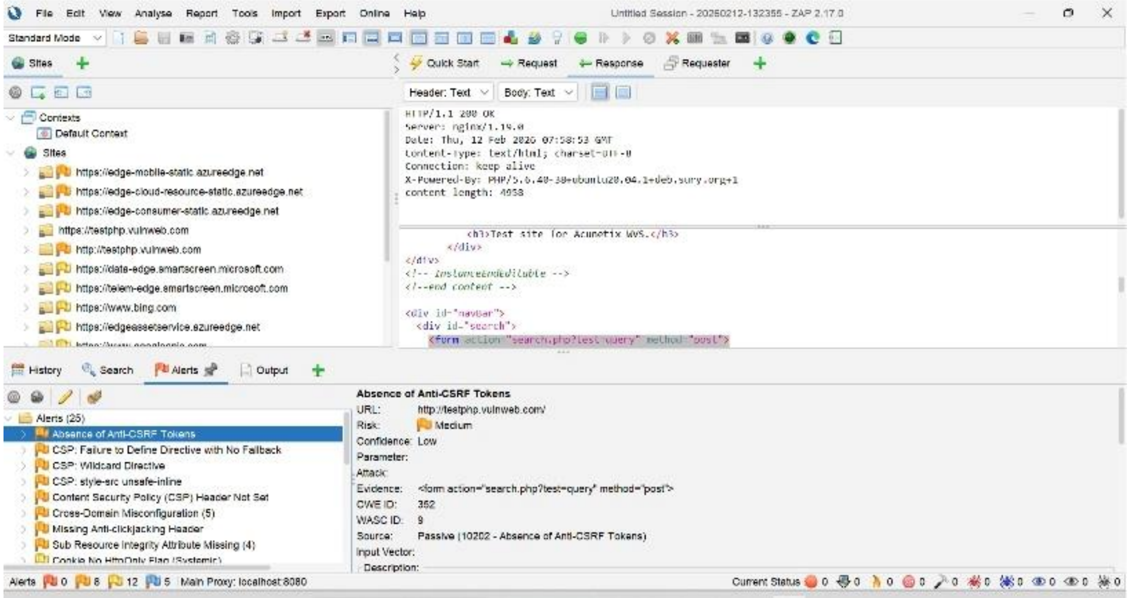


Target: testphp.vulnweb.com

Profile: Intense scan

Command: nmap -T4 -A -v testphp.vulnweb.com

```
nmap -T4 -A -v testphp.vulnweb.com
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.19.0
|_http-favicon: Unknown favicon MD5: 50C42A3EDAAA2FA00445AC77F1B1A715
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-title: Home of Acunetix Art
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 4.X (90%)
OS CPE: cpe:/o:linux:linux_kernel:4.15
Aggressive OS guesses: Linux 4.15 (90%), Linux 4.19 - 5.15 (90%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 38.633 days (since Tue Jan 20 19:41:38 2026)
Network Distance: 20 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   1.00 ms   10.143.94.20
2   ...
3   420.00 ms 10.15.9.129
4   417.00 ms 10.11.32.170
5   435.00 ms 10.40.6.21
6   422.00 ms 10.40.6.2
7   430.00 ms 41.78.74.85
8   427.00 ms 41.78.72.233
9   ...
10  553.00 ms 154.66.246.30
11  532.00 ms port-channel2732.ccr92.lhr01.atlas.cogentco.com (154.54.75.138)
12  ... 14
15  310.00 ms be3424.ccr81.sea08.atlas.cogentco.com (154.54.82.253)
16  297.00 ms be9343.ccr22.sea02.atlas.cogentco.com (154.54.160.242)
17  ... 19
20  285.00 ms ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)

NSE: Script Post-scanning.
Initiating NSE at 10:53
Completed NSE at 10:53, 0.00s elapsed
Initiating NSE at 10:53
Completed NSE at 10:53, 0.00s elapsed
Initiating NSE at 10:53
Completed NSE at 10:53, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
```


File Edit View Analyse Report Tools Import Export Online Help
Untitled Session - 20260212-132355 - ZAP 2.17.0
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
History
Search
Alerts
Output

Contexts
Default Context
Sites
https://edge-mobile-static.azureedge.net
https://edge-cloud-resource-static.azureedge.net
https://edge-consumer-static.azureedge.net
https://testphp.vulnweb.com
http://testphp.vulnweb.com
https://data-edge.smartscreen.microsoft.com
https://telem-edge.smartscreen.microsoft.com
https://www.bing.com
https://edgeassetservice.azureedge.net

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Thu, 12 Feb 2026 07:58:53 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
```

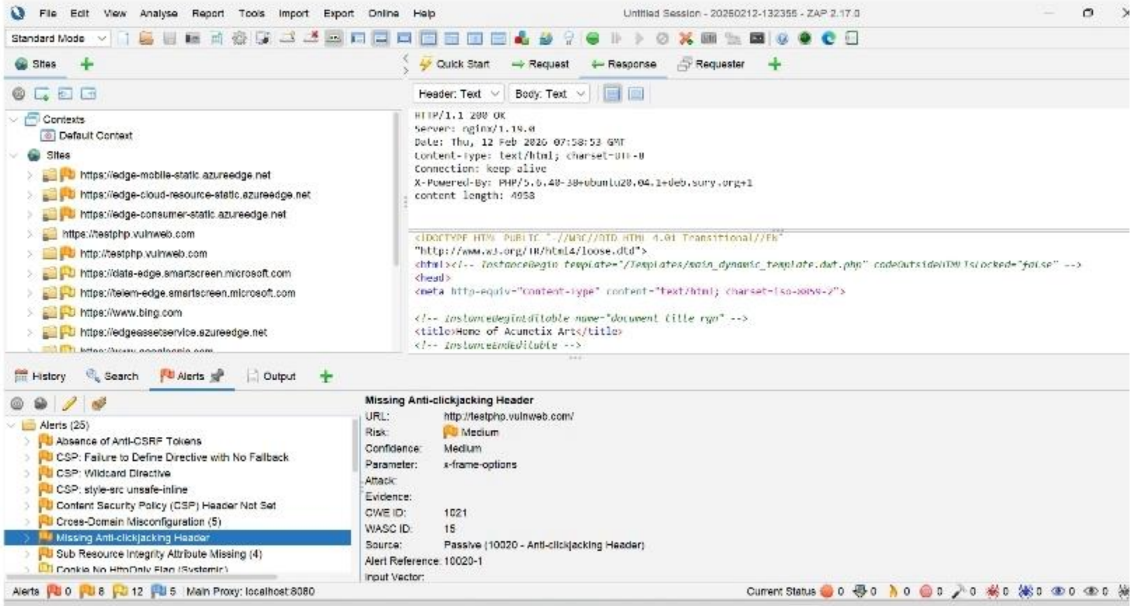
```
            <h3>Test site for Acunetix WVS.</h3>
        </div>
</div>
<!-- InstanceEndEditable -->
<!--end content -->

<div id="navbar">
  <div id="search">
    <form action="search.php?test=query" method="post">
```

Alerts (25)
- Absence of Anti-CSRF Tokens
- CSP: Failure to Define Directive with No Fallback
- CSP: Wildcard Directive
- CSP: style-src unsafe-inline
- Content Security Policy (CSP) Header Not Set
- Cross-Domain Misconfiguration (5)
- Missing Anti-clickjacking Header
- Sub Resource Integrity Attribute Missing (4)
- Cookie No HttpOnly Flag (Systemic)

Absence of Anti-CSRF Tokens

URL: http://testphp.vulnweb.com/
Risk: Medium
Confidence: Low
Parameter:
Attack:
Evidence: <form action="search.php?test=query" method="post">
CWE ID: 352
WASC ID: 9
Source: Passive (10202 - Absence of Anti-CSRF Tokens)
Input Vector:
Description:

Alerts 0 8 12 5 Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0


File Edit View Analyse Report Tools Import Export Online Help
Untitled Session - 20260212-132355 - ZAP 2.17.0
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
History
Search
Alerts
Output

Contexts
Default Context
Sites
https://edge-mobile-static.azureedge.net
https://edge-cloud-resource-static.azureedge.net
https://edge-consumer-static.azureedge.net
https://testphp.vulnweb.com
http://testphp.vulnweb.com
https://data-edge.smartscreen.microsoft.com
https://telem-edge.smartscreen.microsoft.com
https://www.bing.com
https://edgeassetservice.azureedge.net

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Thu, 12 Feb 2026 07:58:53 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" -->
<title>Home of Acunetix Art</title>
<!-- InstanceEndEditable -->
```

Alerts (25)
- Absence of Anti-CSRF Tokens
- CSP: Failure to Define Directive with No Fallback
- CSP: Wildcard Directive
- CSP: style-src unsafe-inline
- Content Security Policy (CSP) Header Not Set
- Cross-Domain Misconfiguration (5)
- Missing Anti-clickjacking Header
- Sub Resource Integrity Attribute Missing (4)
- Cookie No HttpOnly Flag (Systemic)

Missing Anti-clickjacking Header

URL: http://testphp.vulnweb.com/
Risk: Medium
Confidence: Medium
Parameter: x-frame-options
Attack:
Evidence:
CWE ID: 1021
WASC ID: 15
Source: Passive (10020 - Anti-clickjacking Header)
Alert Reference: 10020-1
Input Vector:

Alerts 0 8 12 5 Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0

Prepared by: Mohamed Dahir Mohamed

Organization: Future interns

Task: Cyber security Task1