VULNERABILITY ASSESSMENT REPORT

Security Review – Read-Only Assessment

Website Assessed: http://testphp.vulnweb.com

Prepared By: Vaishnavi.S

Program: Future Interns – Cyber Security Track

1. Executive Summary

A passive vulnerability assessment was conducted on the publicly accessible website testphp.vulnweb.com to evaluate its external security posture.

The objective of this assessment was to identify publicly visible security weaknesses without performing exploitation, authentication bypass, brute force attacks, or intrusive testing.

The assessment identified multiple security misconfigurations including:

- Exposure of unencrypted HTTP service
- Server and software version disclosure
- Missing critical security headers
- Use of outdated PHP version

Although no exploitation was performed, the identified weaknesses increase the potential risk of web-based attacks such as cross-site scripting (XSS), clickjacking, information disclosure, and traffic interception.

Immediate remediation is recommended to reduce the attack surface and improve overall security posture.

2. Scope of Assessment

This assessment strictly followed ethical and read-only testing guidelines.
Included in Scope:

- Public-facing pages only
- Service identification and exposure analysis
- HTTP header inspection
- Configuration review
- Passive testing only

Excluded from Scope:

- SQL Injection exploitation
- Authentication bypass attempts
- Brute force attacks
- Denial-of-Service testing
- Any intrusive or disruptive activity

This report reflects the security posture at the time of testing only.

3. Methodology

The assessment was conducted using industry-standard passive security testing techniques.
Tools used:

- Nmap – Service and port identification
- Browser Developer Tools – HTTP header inspection
- Manual configuration review

Testing principles were inspired by:

- OWASP Testing Guide (Passive Review Principles)
- NIST Security Assessment Guidelines

4. Severity Rating Definition

Severity	Description
High	Significant weakness that may lead to compromise if exploited
Medium	Security misconfiguration increasing attack surface
Low	Informational disclosure assisting reconnaissance
Informational	Security improvement recommendation

5. Vulnerability Summary

ID	Vulnerability	Severity
V-01	Unencrypted HTTP Service (Port 80)	Medium
V-02	Server Version Disclosure	Low
V-03	Outdated PHP Version Disclosure	Medium
V-04	Missing X-Frame-Options Header	Medium
V-05	Missing Content-Security-Policy	High
V-06	Missing HSTS Header	Medium

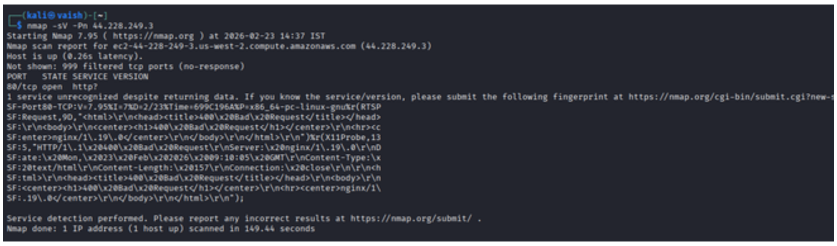
6. Detailed Findings

V-01: Unencrypted HTTP Service (Port 80)

Severity:
Medium

Description:
Port 80 (HTTP) is publicly accessible, allowing unencrypted communication between users and the web server.

Business Impact:
Unencrypted traffic may be intercepted on public networks, potentially exposing sensitive data such as login credentials or session information.



```
┌──(kali㉿vaish)-[~]
└─$ nmap -sV -Pn 44.228.249.3
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-23 14:37 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.26s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-s
SF-Port80-TCP:V=7.95%I=7%D=2/23%Time=699C196A%P=x86_64-pc-linux-gnu%r(RTSP
SF:Request,9D,"<html>\r\n<head><title>400\x20Bad\x20Request</title></head>
SF:\r\n<body>\r\n<center><h1>400\x20Bad\x20Request</h1></center>\r\n<hr><c
SF:enter>nginx/1\.19\.0</center>\r\n</body>\r\n</html>\r\n")%r(X11Probe,13
SF:5,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nServer:\x20nginx/1\.19\.0\r\nD
SF:ate:\x20Mon,\x2023\x20Feb\x202026\x2009:10:05\x20GMT\r\nContent-Type:\x
SF:20text/html\r\nContent-Length:\x20157\r\nConnection:\x20close\r\n\r\n<h
SF:tml>\r\n<head><title>400\x20Bad\x20Request</title></head>\r\n<body>\r\n
SF:<center><h1>400\x20Bad\x20Request</h1></center>\r\n<hr><center>nginx/1\
SF:.19\.0</center>\r\n</body>\r\n</html>\r\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 149.44 seconds
```

Figure 1: Nmap Service Detection Output

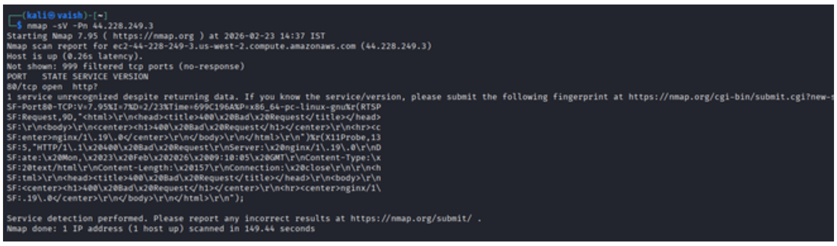
Recommendation:
- Enforce HTTPS redirection
- Disable unnecessary HTTP access
- Implement SSL/TLS encryption

V-02: Server Version Disclosure

Severity:
Low

Description:
The server discloses its software version in HTTP response headers:
 nginx/1.19.0

Business Impact:
Exposing server version information allows attackers to identify known vulnerabilities associated with that specific version. This increases the likelihood of targeted exploitation attempts.



```
┌──(kali㉿vaish)-[~]
└─$ nmap -sV -Pn 44.228.249.3
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-23 14:37 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.26s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-s
SF-Port80-TCP:V=7.95%I=7%D=2/23%Time=699C196A%P=x86_64-pc-linux-gnu%r(RTSP
SF:Request,9D,"<html>\r\n<head><title>400\x20Bad\x20Request</title></head>
SF:\r\n<body>\r\n<center><h1>400\x20Bad\x20Request</h1></center>\r\n<hr><c
SF:enter>nginx/1\.19\.0</center>\r\n</body>\r\n</html>\r\n")%r(X11Probe,13
SF:5,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nServer:\x20nginx/1\.19\.0\r\nD
SF:ate:\x20Mon,\x2023\x20Feb\x202026\x2009:10:05\x20GMT\r\nContent-Type:\x
SF:20text/html\r\nContent-Length:\x20157\r\nConnection:\x20close\r\n\r\n<h
SF:tml>\r\n<head><title>400\x20Bad\x20Request</title></head>\r\n<body>\r\n
SF:<center><h1>400\x20Bad\x20Request</h1></center>\r\n<hr><center>nginx/1\
SF:.19\.0</center>\r\n</body>\r\n</html>\r\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 149.44 seconds
```

Figure 2: Server Version Disclosure in HTTP Headers

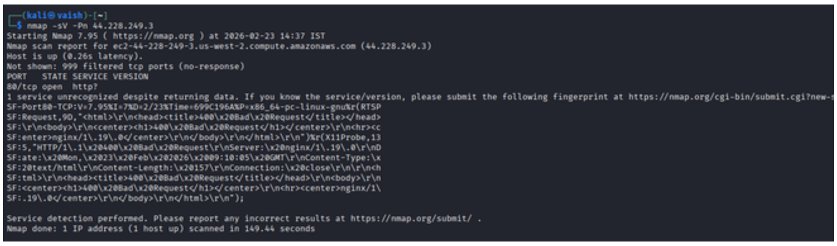
Recommendation:
• Disable server version disclosure using:
 server_tokens off;
 • Regularly update web server software

V-03: Outdated PHP Version Disclosure

Severity:
Medium

Description:
The application exposes the PHP version in HTTP response headers:
 PHP 5.6.40
PHP 5.6 has reached end-of-life and no longer receives security updates.

Business Impact:
Outdated software increases exposure to publicly known vulnerabilities. Attackers may leverage unpatched weaknesses to gain unauthorized access or disrupt services.



```
┌──(kali㉿vaish)-[~]
└─$ nmap -sV -Pn 44.228.249.3
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-23 14:37 IST
Nmap scan report for ec2-44-228-249-3.us-west-2.compute.amazonaws.com (44.228.249.3)
Host is up (0.26s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-s
SF-Port80-TCP:V=7.95%I=7%D=2/23%Time=699C196A%P=x86_64-pc-linux-gnu%r(RTSP
SF:Request,9D,"<html>\r\n<head><title>400\x20Bad\x20Request</title></head>
SF:\r\n<body>\r\n<center><h1>400\x20Bad\x20Request</h1></center>\r\n<hr><c
SF:enter>nginx/1\.19\.0</center>\r\n</body>\r\n</html>\r\n")%r(X11Probe,13
SF:5,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nServer:\x20nginx/1\.19\.0\r\nD
SF:ate:\x20Mon,\x2023\x20Feb\x202026\x2009:10:05\x20GMT\r\nContent-Type:\x
SF:20text/html\r\nContent-Length:\x20157\r\nConnection:\x20close\r\n\r\n<h
SF:tml>\r\n<head><title>400\x20Bad\x20Request</title></head>\r\n<body>\r\n
SF:<center><h1>400\x20Bad\x20Request</h1></center>\r\n<hr><center>nginx/1\
SF:.19\.0</center>\r\n</body>\r\n</html>\r\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 149.44 seconds
```

Figure 3: Outdated PHP Version Disclosure

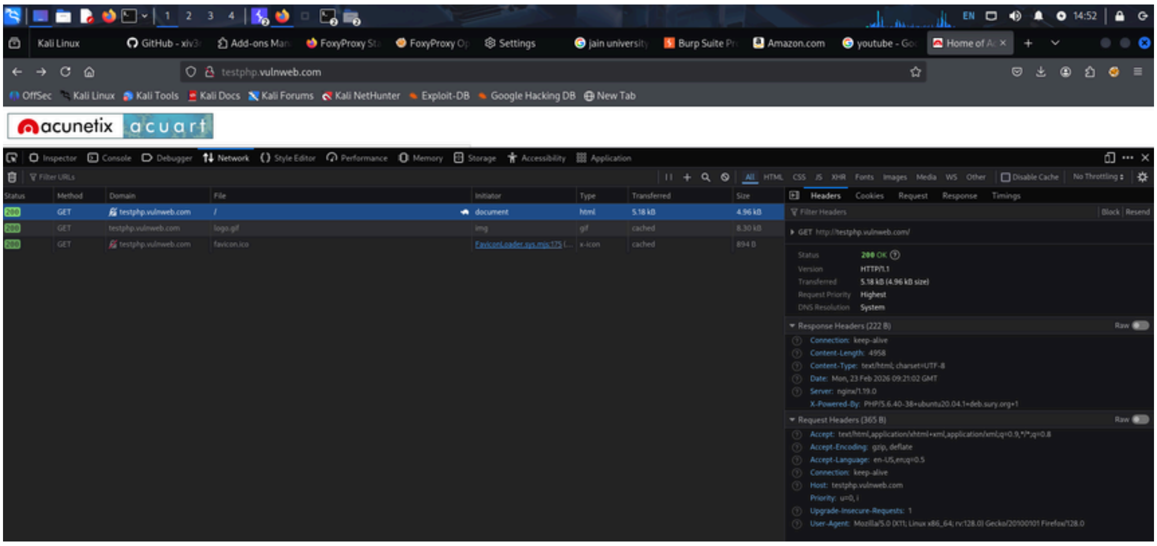
Recommendation:
• Upgrade to PHP 8.x (supported version)
 • Disable version disclosure in configuration
 • Implement regular patch management

V-04: Missing X-Frame-Options Header

Severity:
Medium

Description:
The application does not include the X-Frame-Options security header.

Business Impact:
This may allow clickjacking attacks, where malicious websites embed the application within invisible frames to trick users into performing unintended actions.



Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	testphp.vulnweb.com	/	document	html	5.18 kB	4.96 kB
200	GET	testphp.vulnweb.com	logo.gif	img	gif	cached	8.30 kB
200	GET	testphp.vulnweb.com	favicon.ico	FaviconLoader.sys.mjs:175 (...	x-icon	cached	894 B

```
GET http://testphp.vulnweb.com/

Status              200 OK
Version             HTTP/1.1
Transferred         5.18 kB (4.96 kB size)
Request Priority    Highest
DNS Resolution      System

Response Headers (222 B)
Connection: keep-alive
Content-Length: 4958
Content-Type: text/html; charset=UTF-8
Date: Mon, 23 Feb 2026 09:21:02 GMT
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1

Request Headers (365 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
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
```

Figure 4: Missing X-Frame-Options Header

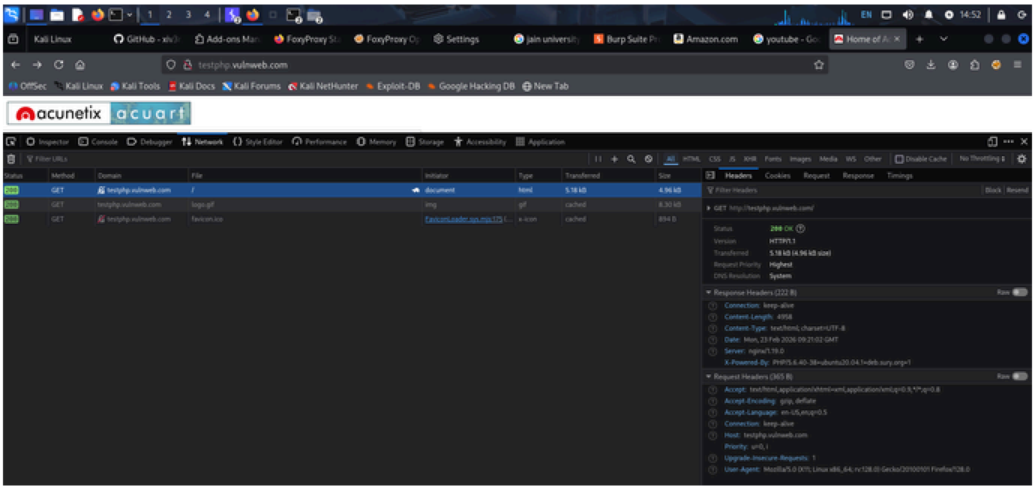
Recommendation:
Add the following header configuration:
X-Frame-Options: SAMEORIGIN
This prevents the website from being embedded in external frames.

V-05: Missing Content-Security-Policy (CSP)

Severity:
High

Description:
No Content-Security-Policy (CSP) header was detected during header inspection.

Business Impact:
Without CSP, the application is more vulnerable to Cross-Site Scripting (XSS) attacks. Malicious scripts injected into the application may execute in users' browsers, potentially leading to session hijacking or data theft.



Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	testphp.vulnweb.com	/	document	html	5.18 kB	4.96 kB
200	GET	testphp.vulnweb.com	logo.gif	img	gif	cached	8.30 kB
200	GET	testphp.vulnweb.com	favicon.ico	FaviconLoader.sys.mjs:175 (...	x-icon	cached	894 B

```
GET http://testphp.vulnweb.com/

Status            200 OK
Version           HTTP/1.1
Transferred       5.18 kB (4.96 kB size)
Request Priority  Highest
DNS Resolution    System

Response Headers (222 B)
Connection: keep-alive
Content-Length: 4958
Content-Type: text/html; charset=UTF-8
Date: Mon, 23 Feb 2026 09:21:02 GMT
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1

Request Headers (365 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
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
```

Figure 5: Missing Content-Security-Policy Header

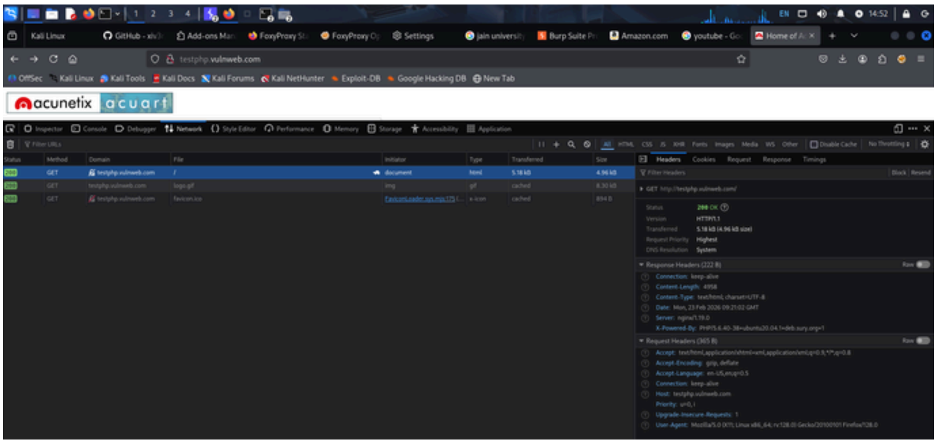
Recommendation:
Implement a strict Content Security Policy, such as:
Content-Security-Policy: default-src 'self';
This restricts the execution of untrusted scripts and resources.

V-06: Missing Strict-Transport-Security (HSTS)

Severity:
Medium

Description:
The website does not implement the Strict-Transport-Security (HSTS) header.

Business Impact:
Without HSTS, users may access the site via HTTP instead of HTTPS. This increases exposure to traffic interception and downgrade attacks.



Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	testphp.vulnweb.com	/	document	html	5.18 kB	4.96 kB
200	GET	testphp.vulnweb.com	logo.gif	img	gif	cached	6.30 kB
200	GET	testphp.vulnweb.com	favicon.ico	FaviconLoader.sys.mjs:175 (...	x-icon	cached	894 B

```
GET http://testphp.vulnweb.com/

Status              200 OK
Version             HTTP/1.1
Transferred         5.18 kB (4.96 kB size)
Request Priority    Highest
DNS Resolution      System

Response Headers (222 B)
Connection: keep-alive
Content-Length: 4958
Content-Type: text/html; charset=UTF-8
Date: Mon, 23 Feb 2026 09:21:02 GMT
Server: nginx/1.19.0
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1

Request Headers (365 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
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
```

Figure 6: Missing HSTS Header

Recommendation:
Enable HSTS using:
Strict-Transport-Security: max-age=31536000; includeSubDomains;
This forces browsers to communicate over secure HTTPS connections only.

Conclusion

The passive vulnerability assessment identified multiple security misconfigurations that increase the website’s exposure to web-based threats. Although no exploitation was performed, the presence of outdated software, missing security headers, and unencrypted communication indicates insufficient security hardening.

Implementing the recommended remediation measures will significantly reduce the attack surface and strengthen the application’s overall security posture. Regular vulnerability assessments and patch management practices are strongly recommended to maintain long-term protection.