Web Application Vulnerability Assesment Report

Target Application :	http://testphp.vulnweb.com
Prepared for	**:** Future Interns - Cyber Security Task 1 (2026)
Prepared by	**:** Nandamudi Harika Naga Padmini Priya
Date	**:** 23 February 2026

Executive Summary

A read-only vulnerability assessment was conducted on the public web application hosted at http://testphp.vulnweb.com. The objective of this assessment was to identify security misconfigurations and exposure risks through passive analysis techniques without performing exploitation or intrusive testing.

The assessment identified multiple security weaknesses, including the absence of HTTPS encryption, outdated server-side software, and missing critical security headers. These vulnerabilities increase the risk of data interception, cross-site scripting (XSS), and information disclosure.

While network-level exposure appears limited due to filtered ports, several application-level security controls are either missing or improperly configured. Immediate remediation is recommended to improve overall security posture and reduce potential risk exposure.

Engagement Overview

Objective :

The objective of this assessment was to:

- Identify publicly observable security weaknesses
- Classify risks based on severity
- Provide practical remediation recommendations
- Conduct testing within strict ethical and non-intrusive boundaries

Scope of Assesment :

In Scope

- Public-facing web pages
- Passive security configuration review
- HTTP response header analysis
- Network exposure analysis using service enumeration

Out of Scope

- Exploitation of vulnerabilities
- Brute force attacks
- Credential attacks
- Denial-of-Service testing
- SQL injection or XSS exploitation

This assessment strictly followed ethical guidelines and did not attempt to harm or disrupt the target system.

Methodology

The assessment was conducted in four structured phases:

Phase 1 – Reconnaissance

- Identification of target domain
- DNS resolution and IP address identification

Phase 2 – Network Exposure Analysis

- Nmap scan using -sV -Pn flags
- Service enumeration and version detection
- Open port identification

Phase 3 – Application Security Configuration Review

- HTTP response header inspection
- HTTPS enforcement validation
- Server software disclosure review

Phase 4 – Risk Classification

- Classification of vulnerabilities as High, Medium, or Low
- Business impact analysis
- Practical remediation guidance

No aggressive scanning, exploit frameworks, or vulnerability exploitation tools were used during this assessment.

Tools Used

- Nmap 7.95
- Kali Linux
- Browser Developer Tools
- SecurityHeaders.com

Only passive and non-intrusive tools were used.

Risk Rating Framework

Severity	**Description**
High	Immediate risk of compromise or data exposure
Medium	Weakness that increases attack surface
Low	Minor misconfiguration or information disclosure

Summary of Findings

ID	Vulnerability	Severity	Status
01	Website served over HTTP	High	Open
02	Outdated PHP Version (5.6)	High	Open
03	Missing Content Security Policy	Medium	Open
04	Missing X-Frame-Options	Medium	Open
05	Missing X-Content-Type-Options	Low-Medium	Open
06	Server Version Disclosure	Low	Open

Detailed Findings

Finding ID: 01

Title: Website Served Over HTTP

Severity: High

Description

The web application is accessible over HTTP (port 80) and does not enforce HTTPS encryption. Port 443 (HTTPS) is not open, and no automatic redirection to HTTPS is configured.

Technical Evidence

- Nmap scan confirms port 80 open
- No HTTPS redirection observed
- SecurityHeaders scan indicates site served over HTTP

Risk Explanation

Unencrypted HTTP traffic can be intercepted or modified by attackers performing Man-in-the-Middle (MITM) attacks.

Business Impact

Sensitive user information, session data, or credentials transmitted over the network could be exposed. This may result in data compromise, reputational damage, and regulatory non-compliance.

Recommendation

- Implement SSL/TLS certificate
- Enable HTTPS (port 443)
- Redirect all HTTP traffic to HTTPS
- Enable Strict-Transport-Security (HSTS)

Finding ID: 02

Title: Outdated PHP Version (PHP 5.6.40)

Severity: High

Description

The server discloses usage of PHP version 5.6.40, which is End-of-Life (EOL) and no longer supported with security updates.

Technical Evidence

- Response header: X-Powered-By: PHP/5.6.40

Risk Explanation

Outdated software may contain known vulnerabilities that attackers can exploit.

Business Impact

Use of unsupported software significantly increases the risk of compromise and security breaches.

Recommendation

- Upgrade PHP to a currently supported version (e.g., PHP 8.x)
- Implement regular patch management procedures

Finding ID: 03

Title: Missing Content Security Policy (CSP)

Severity: Medium

Description

The application does not implement a Content-Security-Policy header.

Risk Explanation

Without CSP, the application is more vulnerable to Cross-Site Scripting (XSS) attacks.

Business Impact

Attackers may inject malicious scripts affecting users and potentially stealing data.

Recommendation

- Implement a strict CSP policy, for example:

  ```
  Content-Security-Policy: default-src 'self';
  ```

Finding ID: 04

Title: Missing X-Frame-Options Header

Severity: Medium

Description

The X-Frame-Options header is not configured.

Risk Explanation

This exposes the application to clickjacking attacks.

Business Impact

Users could be tricked into performing unintended actions.

Recommendation

- Set the header: X-Frame-Options: SAMEORIGIN

Finding ID: 05

Title: Missing X-Content-Type-Options Header

Severity: Low-Medium

Description

The X-Content-Type-Options header is not configured.

Risk Explanation

Browsers may perform MIME-sniffing, which can lead to unintended content execution.

Business Impact

May increase the risk of malicious file execution.

Recommendation

Set the header: X-Content-Type-Options: nosniff

Finding ID: 06

Title: Server Version Disclosure

Severity: Low

Description

The server reveals detailed software version information including:

- nginx 1.19.0
- PHP 5.6.40

Risk Explanation

Version disclosure provides attackers with information that may assist in targeted exploitation attempts.

Business Impact

Increases reconnaissance effectiveness for malicious actors.

Recommendation

- Disable or modify Server header
- Remove X-Powered-By header
- Configure nginx with server_tokens off;

Positive Security Observations

- 999 TCP ports were filtered, indicating active firewall protection
- Only one service (HTTP) exposed
- Limited network attack surface

These controls reduce the overall network-level exposure.

Conclusion

The assessment identified several high and medium risk security misconfigurations within the target web application. The absence of HTTPS encryption and use of outdated PHP software represent the most critical risks.

Although the network exposure appears limited, application-level security controls require improvement. Immediate remediation of high-severity findings is strongly recommended, followed by periodic reassessment to ensure ongoing security compliance.

Appendix

Appendix A – Nmap Output (Raw Scan Evidence)

1. **Full Nmap Command Used**

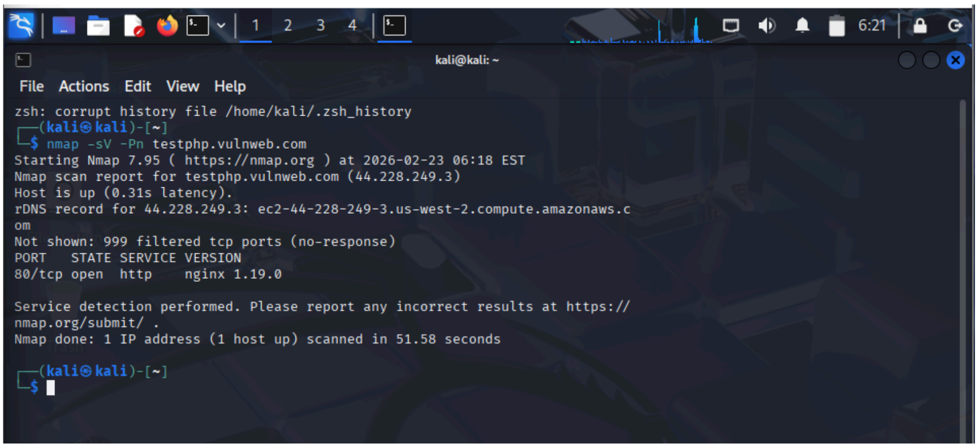
```
nmap -sV -Pn testphp.vulnweb.com
```

2. **Complete Output (Cleaned, Not Edited)**

```
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kali) [~]
 └─$ nmap -sV -Pn testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-23 06:18 EST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.315 latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.c
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
80/tcp   open  http    nginx 1.19.0

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 51.58 seconds
(kali㉿kali) [~]
```

Screenshot:



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-23 06:18 EST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.31s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.c
om
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.19.0

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.58 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Appendix B – Raw Response Headers

Raw Headers :

HTTP/1.1	200 OK
Server	nginx/1.19.0
Date	Tue, 24 Feb 2026 14:01:23 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

Missing Headers :

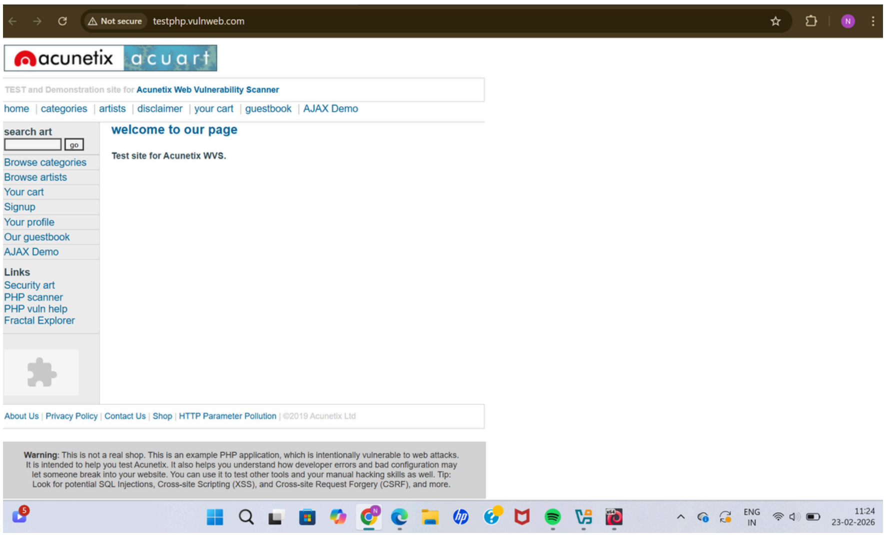
Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
X-Frame-Options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

Appendix C – Screenshot Evidence

Figure 1 – Website Homepage

Description:

Screenshot of the public homepage confirming accessibility of the target application.



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.

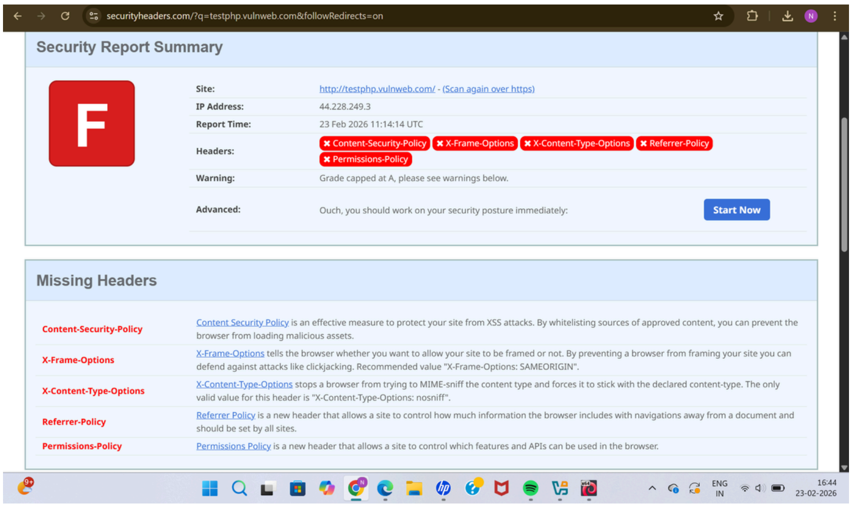
About Us | Privacy Policy | Contact Us | Shop | HTTP Parameter Pollution | ©2019 Acunetix Ltd

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.

Figure 2 – Security Headers Scan Result

Description:

SecurityHeaders.com scan result showing missing security headers and HTTP usage.



securityheaders.com/?q=testphp.vulnweb.com&followRedirects=on
F
Start Now
16:44
23-02-2026
ENG
IN

Security Report Summary

Site:	http://testphp.vulnweb.com/ - (Scan again over https)
IP Address:	44.228.249.3
Report Time:	23 Feb 2026 11:14:14 UTC
Headers:	✖ Content-Security-Policy ✖ X-Frame-Options ✖ X-Content-Type-Options ✖ Referrer-Policy ✖ Permissions-Policy
Warning:	Grade capped at A, please see warnings below.
Advanced:	Ouch, you should work on your security posture immediately:

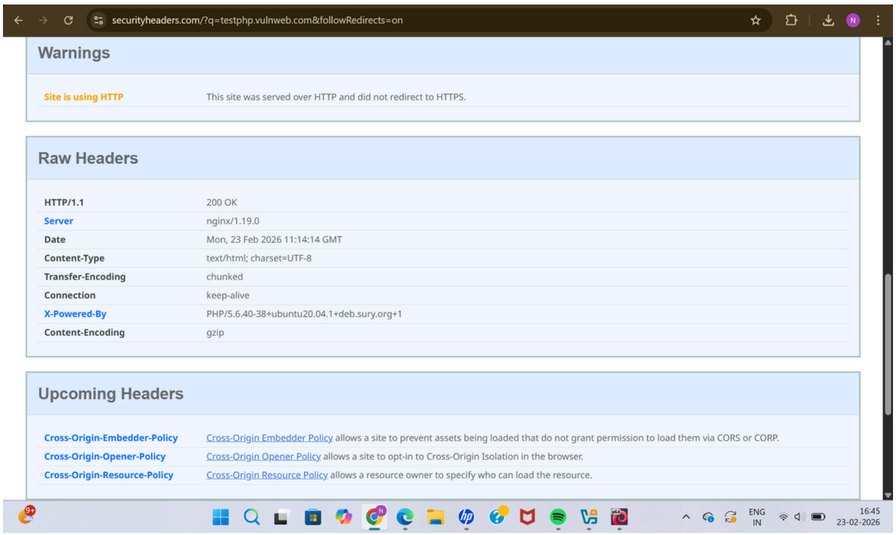
Missing Headers

Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.
X-Frame-Options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN".
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

Figure 3 – Response Headers (Browser DevTools)

Description:

Raw HTTP response headers displaying server version disclosure and missing security headers.



securityheaders.com/?q=testphp.vulnweb.com&followRedirects=on

Warnings

Site is using HTTP	This site was served over HTTP and did not redirect to HTTPS.

Raw Headers

HTTP/1.1	200 OK
Server	nginx/1.19.0
Date	Mon, 23 Feb 2026 11:14:14 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

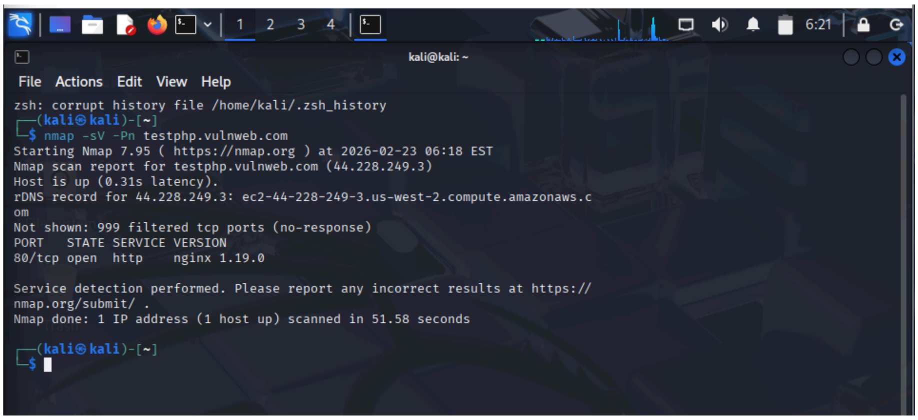
Upcoming Headers

Cross-Origin-Embedder-Policy	Cross-Origin Embedder Policy allows a site to prevent assets being loaded that do not grant permission to load them via CORS or CORP.
Cross-Origin-Opener-Policy	Cross-Origin Opener Policy allows a site to opt-in to Cross-Origin Isolation in the browser.
Cross-Origin-Resource-Policy	Cross-Origin Resource Policy allows a resource owner to specify who can load the resource.

Figure 4 – Nmap Scan Output

Description:

Nmap service version detection scan confirming open port 80 and nginx 1.19.0.



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-23 06:18 EST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.31s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.c
om
Not shown: 999 filtered tcp ports (no-response)
PORT    STATE SERVICE VERSION
80/tcp open  http    nginx 1.19.0

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.58 seconds

┌──(kali㉿kali)-[~]
└─$ 
```