

# Vulnerability Assessment and Penetration Testing Report

<b>Client / Website Tested</b>
testphp.vulnweb.com ( <i>Public demo website</i> )
<b>Assessment Type</b>
Vulnerability Assessment and penetration Testing
<b>Intern Name</b>
Rushikesh Borse Cyber Security Intern – Future Interns (2026)
<b>Assessment Date</b>
February 2026

• The assessment was carried out using: Tools
• Browser Developer Tools
• Nmap (basic exposure analysis)
• OWASP ZAP (Passive Scan only)

1. No authentication bypass, brute-force attempts, or denial-of-service activities were performed.

<b>1. Executive Summary</b>
<b>This Vulnerability Assessment was conducted to identify common security weaknesses present on a publicly accessible website using non-intrusive and ethical methods.</b>
<b>The objective of this assessment is not to exploit or attack the website, but to provide clarity to a business owner about potential security risks and recommend practical remediation steps.</b>

## Finding 1: Missing Security Headers

### Tool Used: Browser DevTools

#### What is the issue?

The website is accessible over HTTP, which means data is transmitted without encryption.

The screenshot shows a browser window with the URL `http://testphp.vulnweb.com/`. The Network tab in the developer tools is active, showing a list of requests. One request for the homepage is selected. The Headers section of the Network tab shows the following response headers:

Name	Value
Request URL	<code>http://testphp.vulnweb.com/</code>
Request Method	GET
Status Code	200 OK
Remote Address	44.228.249.3:80
Referrer Policy	strict-origin-when-cross-origin
Response Headers	Raw
Connection	keep-alive
Content-Encoding	gzip
Content-Type	text/html; charset=UTF-8
Date	Thu, 05 Feb 2026 16:31:27 GMT
Server	nginx/1.19.0
Transfer-Encoding	chunked
X-Powered-By	PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding	gzip, deflate
Accept-Language	en-US,en;q=0.9,hi;q=0.8
Cache-Control	max-age=0

#### Why does it matter?

Without encryption, sensitive information such as login details or user data can be intercepted by attackers. This reduces user trust and may lead to data exposure.

#### Risk Level :- High

#### Suggested Remediation (Business-Friendly Fix)

- Enable HTTPS using an SSL/TLS certificate
- Redirect all HTTP traffic to HTTPS
- Ensure secure communication for all users

A close-up view of the Headers section in the Network tab of the developer tools. The General section is expanded, showing the following information:

Request URL	Value
Request URL	<code>http://testphp.vulnweb.com/</code>
Request Method	GET
Status Code	200 OK

**Observed Missing Headers:**

- Content-Security-Policy (CSP)
- X-Frame-Options
- X-Content-Type-Options

**Why This Matters:**

Missing headers increase the risk of:

- Clickjacking
- Cross-Site Scripting (XSS)
- Content injection attacks

Risk Level: Medium

**Recommended Remediation:**

- Implement standard security headers at the server level

## Finding 2: Open HTTP Port (Port 80)

Tool Used: Nmap

Command Example: nmap -F testphp.vulnweb.com

```
kali [Running] - Oracle VirtualBox
Session Actions Edit View Help
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali] ChatGPT
# nmap -F testphp.vulnweb.com

Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-06 10:44 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.39s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 99 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 8.32 seconds
#
```

### What was checked?

- Scanned the most commonly used ports to quickly identify exposed services.

**Identified Issue :-** Common web service ports are open and reachable

**Why does it matter? :-** Open ports increase the attack surface if not properly secured

**Risk Level :- Medium**

### Clear Remediation Steps

- Close unused ports
- Restrict access using firewall rules

## Nmap 2: Default Nmap Scan

**Tool Used:** Nmap

**Command Example:** nmap testphp.vulnweb.com

The screenshot shows a terminal window on a Kali Linux system. The command \$ nmap testphp.vulnweb.com is run, resulting in the following output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-06 11:58 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.29s 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 22.78 seconds
```

Below the terminal window, there is a sidebar with various links and a "Normal Scan (More Details)" button.

### What was checked?

- A standard scan to identify **open ports** and **basic service exposure** on the target server.
- **Why does it matter?**
- **Port 80 (HTTP) is open and publicly accessible**  
**Web service is exposed without enforced encryption**

### Identified Issue

- **Port 80 (HTTP) is open and publicly accessible**
- **Web service is exposed without enforced encryption**

### Risk Level :- Medium

### Clear Remediation Steps

- Redirect all HTTP traffic to HTTPS
- Allow only required ports to remain open

## Nmap 2 : Operating System Detection

Tool Used: Nmap

Command Example: nmap -O testphp.vulnweb.com

The screenshot shows a terminal window titled 'kali:kali ~'. The command entered is '\$ nmap -O testphp.vulnweb.com'. The output of the scan is displayed, showing the host is up with 0.29s latency, an rDNS record for ec2-44-228-249-3.us-west-2.compute.amazonaws.com, and a single open port 80/tcp for http. OS detection results show aggressive guesses for various Linux versions from 4.15 to 5.15, with 91% confidence. A note states 'No exact OS matches for host (test conditions non-ideal)'. The scan took 32.23 seconds.

```
(kali㉿kali)-[~]
$ nmap -O testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-06 12:08 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.29s 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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 4.15 (97%), Linux 2.6.32 (91%), Linux 2.6.32 - 3.13 (91%), Linux 3.10 - 4.11 (91%), Linux 3.2 - 4.14 (91%), Linux 3.4 - 3.10 (91%), Linux 4.15 - 5.19 (91%), Linux 4.19 (91%), Linux 5.0 - 5.14 (91%), Linux 5.1 - 5.15 (91%)
No exact OS matches for host (test conditions non-ideal).g System Detection (information Disclosure)

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.23 seconds
```

### What was checked?

- Attempted to identify the operating system of the server.
- Why does it matter?

OS fingerprinting information may be inferred

### Identified Issue

- Knowing the operating system helps attackers craft targeted attacks.

### Risk Level :- Low

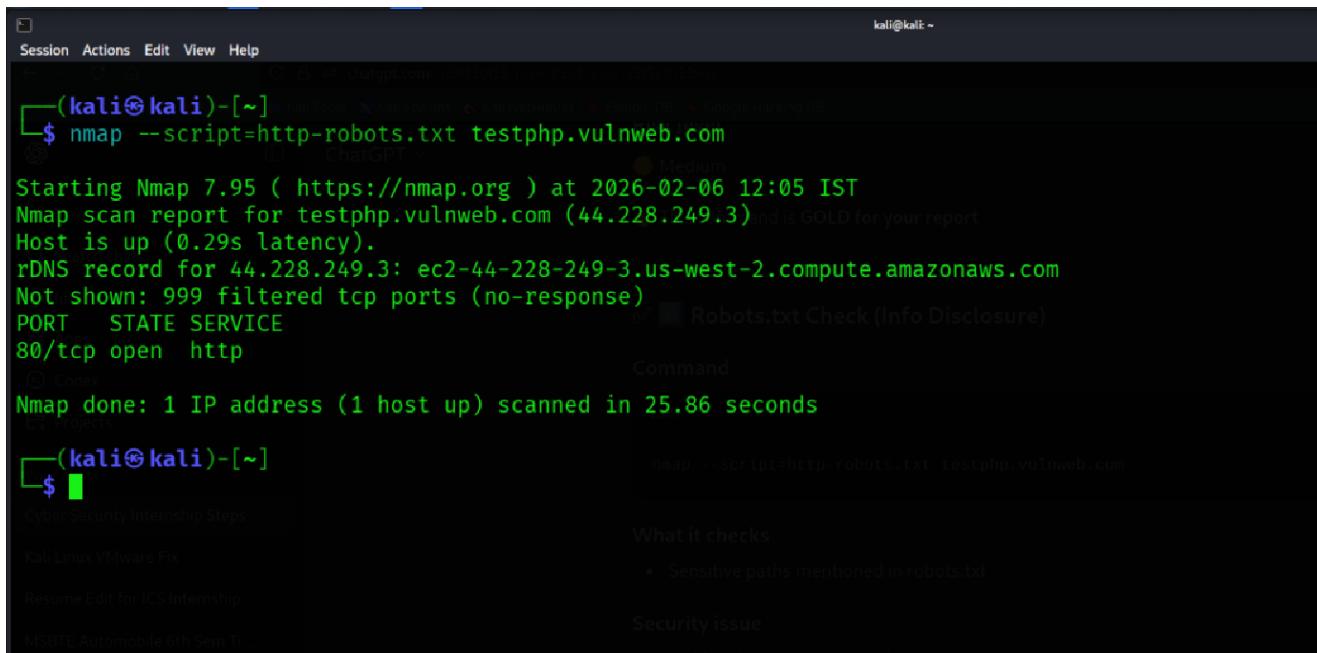
### Clear Remediation Steps

- Implement firewall and intrusion prevention rules
- Apply OS hardening measures
- Keep OS patches up to date

## Nmap 3 : robots.txt Information Disclosure

Tool Used: Nmap

Command Example: nmap --script=http-robots.txt  
testphp.vulnweb.com



```
kali㉿kali:[~] $ nmap --script=http-robots.txt testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-06 12:05 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.29s 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 25.86 seconds
```

### What was checked?

- Reviewed the robots.txt file for exposed paths.
- Why does it matter?  
**robots.txt file is publicly accessible and reveals internal paths**

### Identified Issue

- Attackers can use these paths to locate hidden or sensitive sections of the website.

### Risk Level :- Low

### Clear Remediation Steps

- Avoid listing sensitive directories in robots.txt
- Use authentication and access control instead
- Review robots.txt regularly
- 

Finding: - 3

## OWASP ZAP Vulnerability Assessment (Passive Scan)

- **Tool Used:** OWASP ZAP (Zed Attack Proxy)
- **Scan Type:** Passive Scan (Read-Only)
- **Target Website:** testphp.vulnweb.com
- **Testing Approach:** Non-intrusive, ethical security analysis

### Methodology

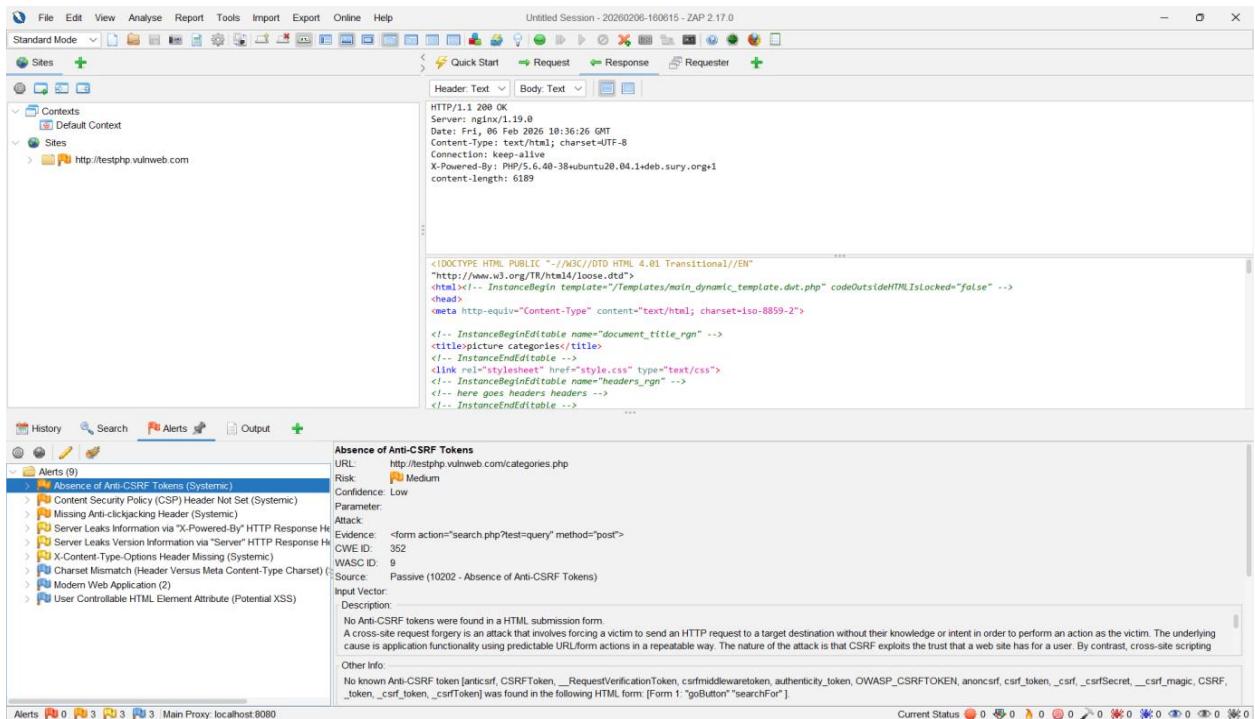
OWASP ZAP was used as a **passive security analysis tool** to monitor traffic between the browser and the website.

The tool identified common web security misconfigurations and weaknesses **without sending malicious requests**.

**Owasp zap 1 : Missing Content Security Policy (CSP)**

## Tool Used: Owasp zap

Command Example: nmap --script=http-robots.txt  
testphp.vulnweb.com



## What was checked?

- The website does not implement a Content Security Policy (CSP) header.

- Why does it matter?

Without CSP, attackers may inject malicious scripts into the website, potentially leading to data theft or page manipulation.

### Identified Issue

- Attackers can use these paths to locate hidden or sensitive sections of the website.

### Risk Level :- medium

### Clear Remediation Steps

- Implement a Content-Security-Policy header
- Review and update CSP rules during application changes

## Finding 2: Missing X-Frame-Options Header

### What is the issue?

The website does not include the **X-Frame-Options** header.

### Why does it matter?

This can allow attackers to embed the website inside a malicious page, leading to **clickjacking attacks**.

### Risk Level :- Medium

### Suggested Remediation

- Set X-Frame-Options to DENY or SAMEORIGIN
- Prevent unauthorized framing of the website

The screenshot shows the ZAP 2.17.0 interface with the following details:

- Header Text:** HTTP/1.1 200 OK  
Server: nginx/1.19.0  
Date: Fri, 06 Feb 2026 10:36:26 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: 6169
- Body Text:**

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template:/Templates/main_dynamic_template.dwt.php -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">
<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>picture categories</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
```
- Alerts (9):**
  - Absence of Anti-CSRF Tokens (Systemic)
  - Content Security Policy (CSP) Header Not Set (Systemic)
  - Missing Anti-clickjacking Header (Systemic)
  - Server Leaks Version Information via "Server" HTTP Response Header (Systemic)
  - X-Content-Type-Options Header Missing (Systemic)
  - Charset Mismatch (Header Versus Meta Content-Type Charset)
  - Modern Web Application (2)
  - User Controllable HTML Element Attribute (Potential XSS)
- Current Status:** 0 errors, 0 warnings, 0 info, 0 alerts, 0 notices, 0 vulnerabilities, 0 risks.