



# **VULNERABILITY ASSESSMENT**

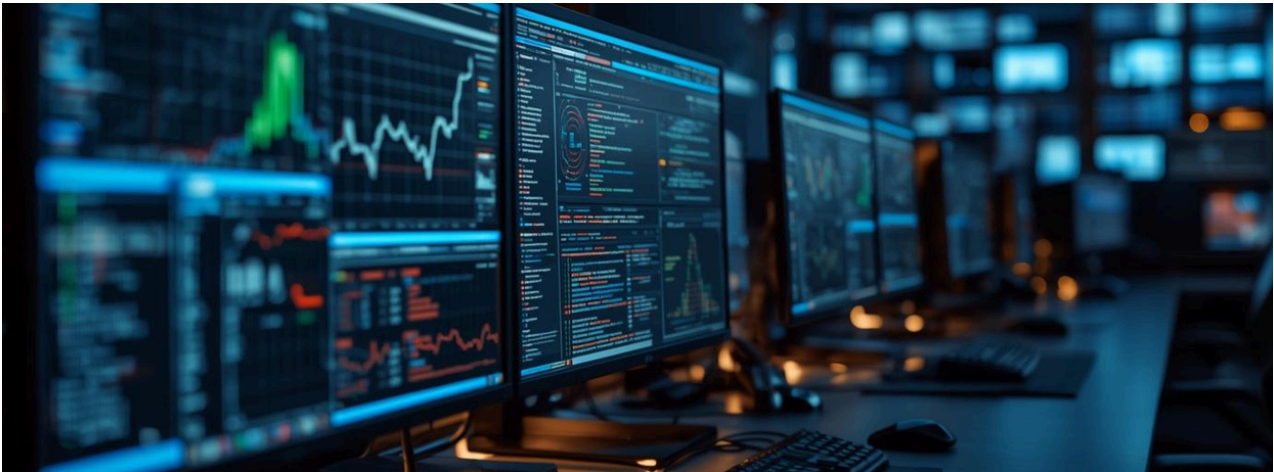
Report for a Live Website

PRESENTED BY

VINUTHA C S

CIN ID: FIT/JAN26/CS5645

# 1. EXECUTIVE SUMMARY



This report documents a vulnerability assessment conducted on a publicly available test website. The assessment, focusing on identifying potential security misconfigurations and exposed components without exploiting any vulnerabilities. The target selected was <http://testphp.vulnweb.com>, a deliberately vulnerable test application provided for security training and demonstration. Industry-standard tools such as Nmap, Browser Developer Tools, and OWASP ZAP (Passive Scan) were used.

## 2. SCOPE OF ASSESSMENT

- Target Website: <http://testphp.vulnweb.com>
- Assessment Type: Vulnerability Assessment (Passive & Read-Only)
- Tools Used:
  - oNmap
  - oWeb Browser (Manual Inspection)
  - oBrowser Developer Tools
  - oOWASP ZAP (Passive Scan)

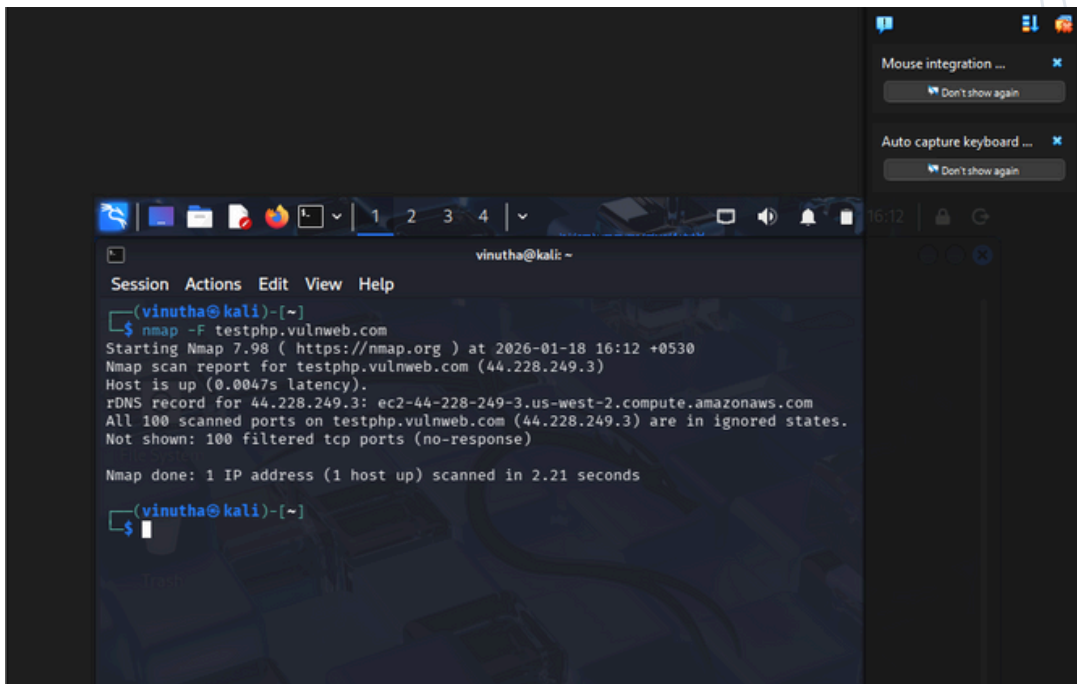
## 3. STEP 1: TARGET SELECTION

The target website was selected from approved test platforms to ensure legal and ethical compliance.

Reason for Selection: - Publicly available - Intentionally vulnerable for learning - No real users or sensitive data



## 4. STEP 2: NETWORK EXPOSURE SCAN (NMAP)

A screenshot of a Kali Linux terminal window. The terminal shows a command prompt where the user has entered 'nmap -F testphp.vulnweb.com'. The output of the scan is displayed, indicating that the host is up and that all 100 scanned ports are in ignored states. The terminal window has a dark theme and a menu bar at the top. On the right side of the terminal, there are two notification pop-ups: 'Mouse integration ...' and 'Auto capture keyboard ...', both with 'Don't show again' buttons.

```
vinutha@kali ~  
Session Actions Edit View Help  
$ nmap -F testphp.vulnweb.com  
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-18 16:12 +0530  
Nmap scan report for testphp.vulnweb.com (44.228.249.3)  
Host is up (0.0047s latency).  
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com  
All 100 scanned ports on testphp.vulnweb.com (44.228.249.3) are in ignored states.  
Not shown: 100 filtered tcp ports (no-response)  
  
Nmap done: 1 IP address (1 host up) scanned in 2.21 seconds  
  
$
```

Nmap was used to identify open ports and exposed services using safe scanning techniques.

Command Used:

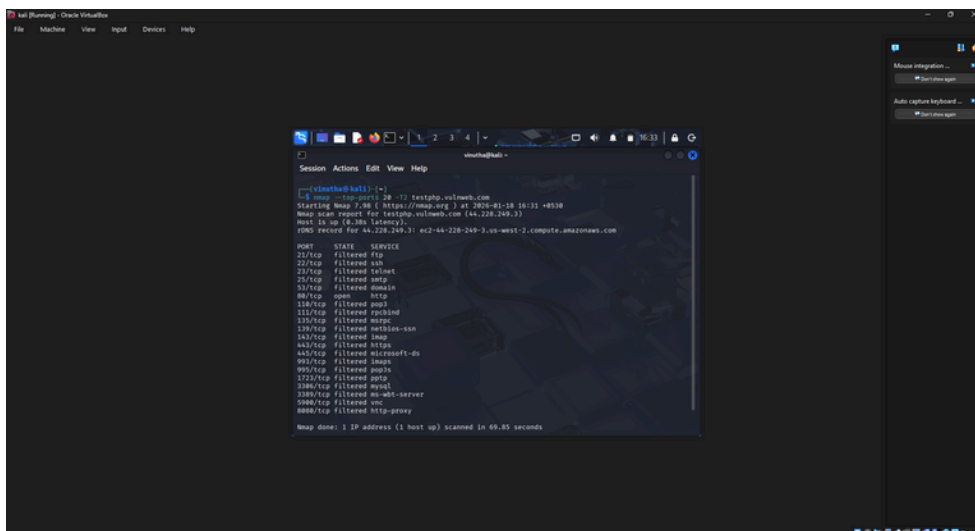
```
nmap -F testphp.vulnweb.com
```

Analysis:

The scan confirmed that the website is accessible via standard HTTP services. No critical network-level vulnerabilities were detected during this read-only scan.

## Commands:

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



## 6. STEP 7: MANUAL BROWSER-BASED INSPECTION

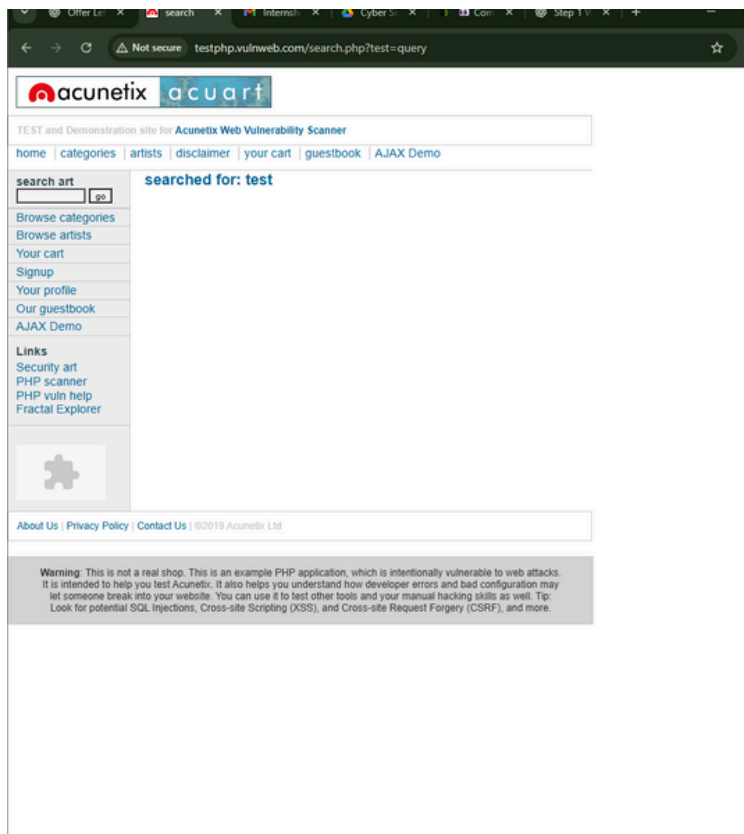
The website was manually explored using a standard web browser.

Observations:

- Search input field available
- URL parameters visible (e.g., search.php?test=query)
- Multiple forms and navigation links

Security Relevance:

Visible parameters can be potential attack vectors if not properly validated on the server side.

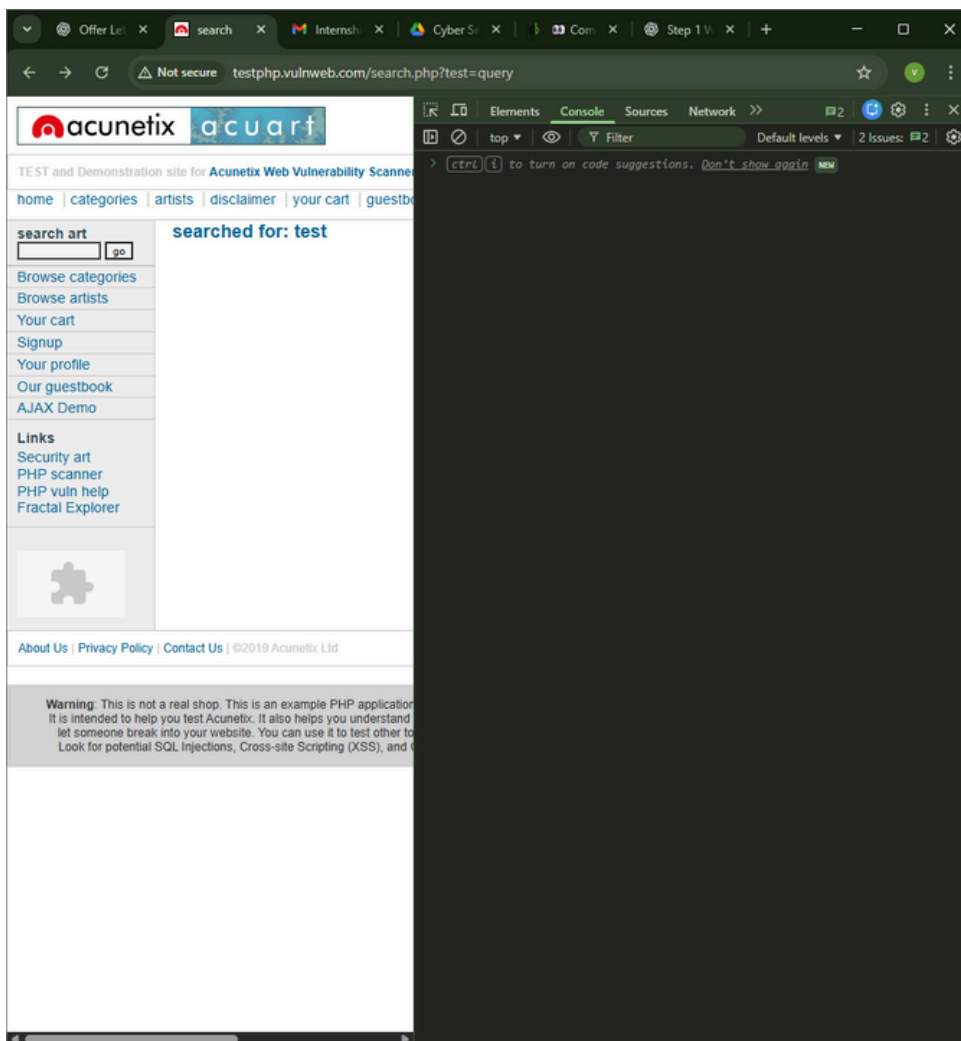


## 7. STEP 8: BROWSER DEVELOPER TOOLS ANALYSIS

Browser Developer Tools (F12) were used to analyze client-side behavior.

Console Tab:

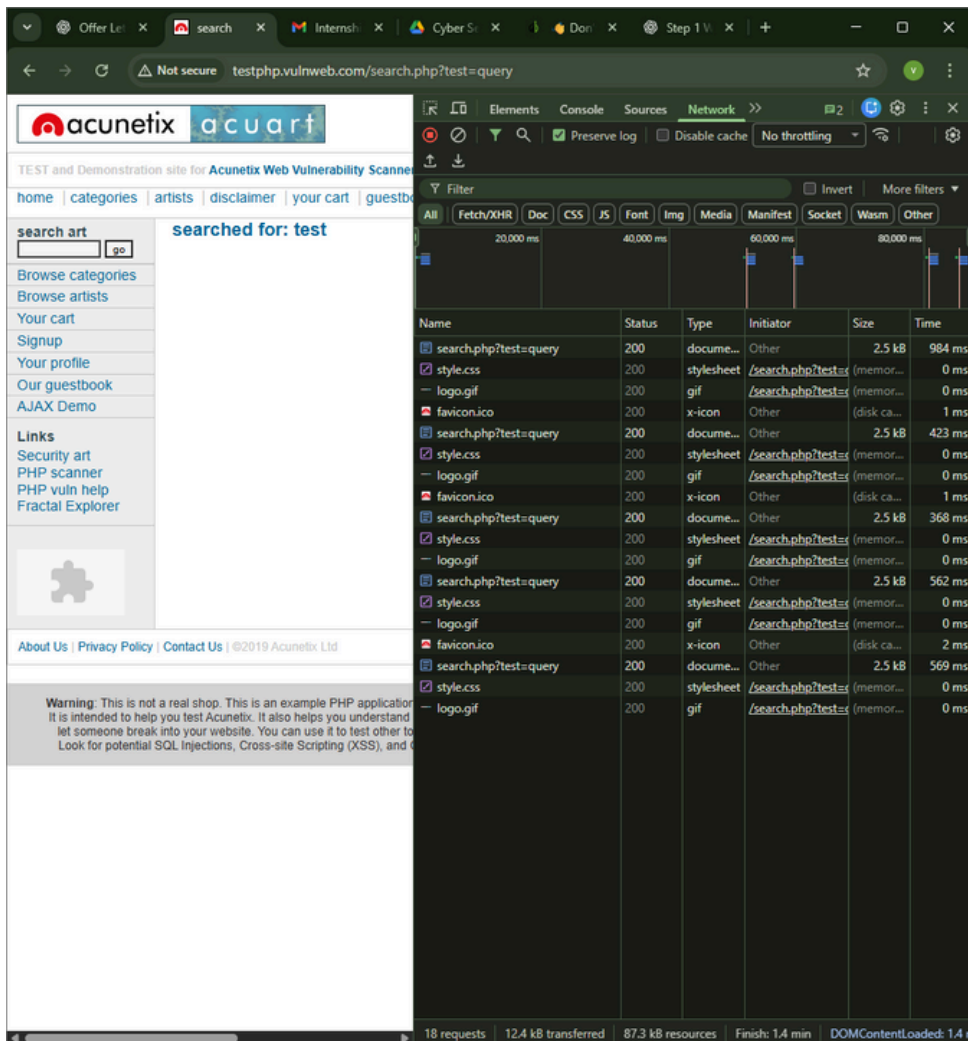
- Minor JavaScript warnings
- No critical runtime errors





## NETWORK TAB:

- HTTP requests observed
- Parameters transmitted via GET requests

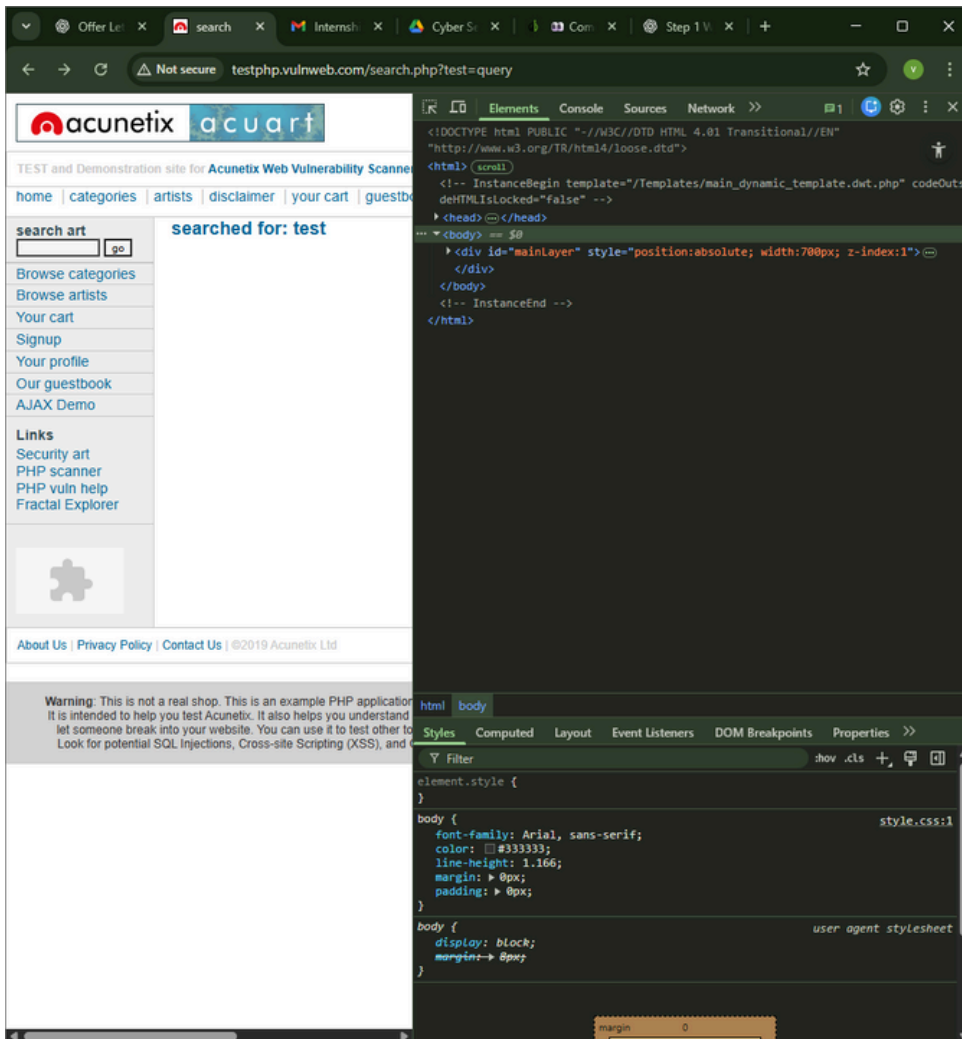


| Name                  | Status | Type       | Initiator              | Size         | Time   |
|-----------------------|--------|------------|------------------------|--------------|--------|
| search.php?test=query | 200    | document   | Other                  | 2.5 kB       | 984 ms |
| style.css             | 200    | stylesheet | /search.php?test=query | (memory)     | 0 ms   |
| logo.gif              | 200    | gif        | /search.php?test=query | (memory)     | 0 ms   |
| favicon.ico           | 200    | x-icon     | Other                  | (disk cache) | 1 ms   |
| search.php?test=query | 200    | document   | Other                  | 2.5 kB       | 423 ms |
| style.css             | 200    | stylesheet | /search.php?test=query | (memory)     | 0 ms   |
| logo.gif              | 200    | gif        | /search.php?test=query | (memory)     | 0 ms   |
| favicon.ico           | 200    | x-icon     | Other                  | (disk cache) | 1 ms   |
| search.php?test=query | 200    | document   | Other                  | 2.5 kB       | 368 ms |
| style.css             | 200    | stylesheet | /search.php?test=query | (memory)     | 0 ms   |
| logo.gif              | 200    | gif        | /search.php?test=query | (memory)     | 0 ms   |
| search.php?test=query | 200    | document   | Other                  | 2.5 kB       | 562 ms |
| style.css             | 200    | stylesheet | /search.php?test=query | (memory)     | 0 ms   |
| logo.gif              | 200    | gif        | /search.php?test=query | (memory)     | 0 ms   |
| favicon.ico           | 200    | x-icon     | Other                  | (disk cache) | 2 ms   |
| search.php?test=query | 200    | document   | Other                  | 2.5 kB       | 569 ms |
| style.css             | 200    | stylesheet | /search.php?test=query | (memory)     | 0 ms   |
| logo.gif              | 200    | gif        | /search.php?test=query | (memory)     | 0 ms   |

18 requests | 12.4 kB transferred | 87.3 kB resources | Finish: 1.4 min | DOMContentLoaded: 1.4 min

## ELEMENTS TAB:

- HTML structure reviewed
- No sensitive credentials found in DOM



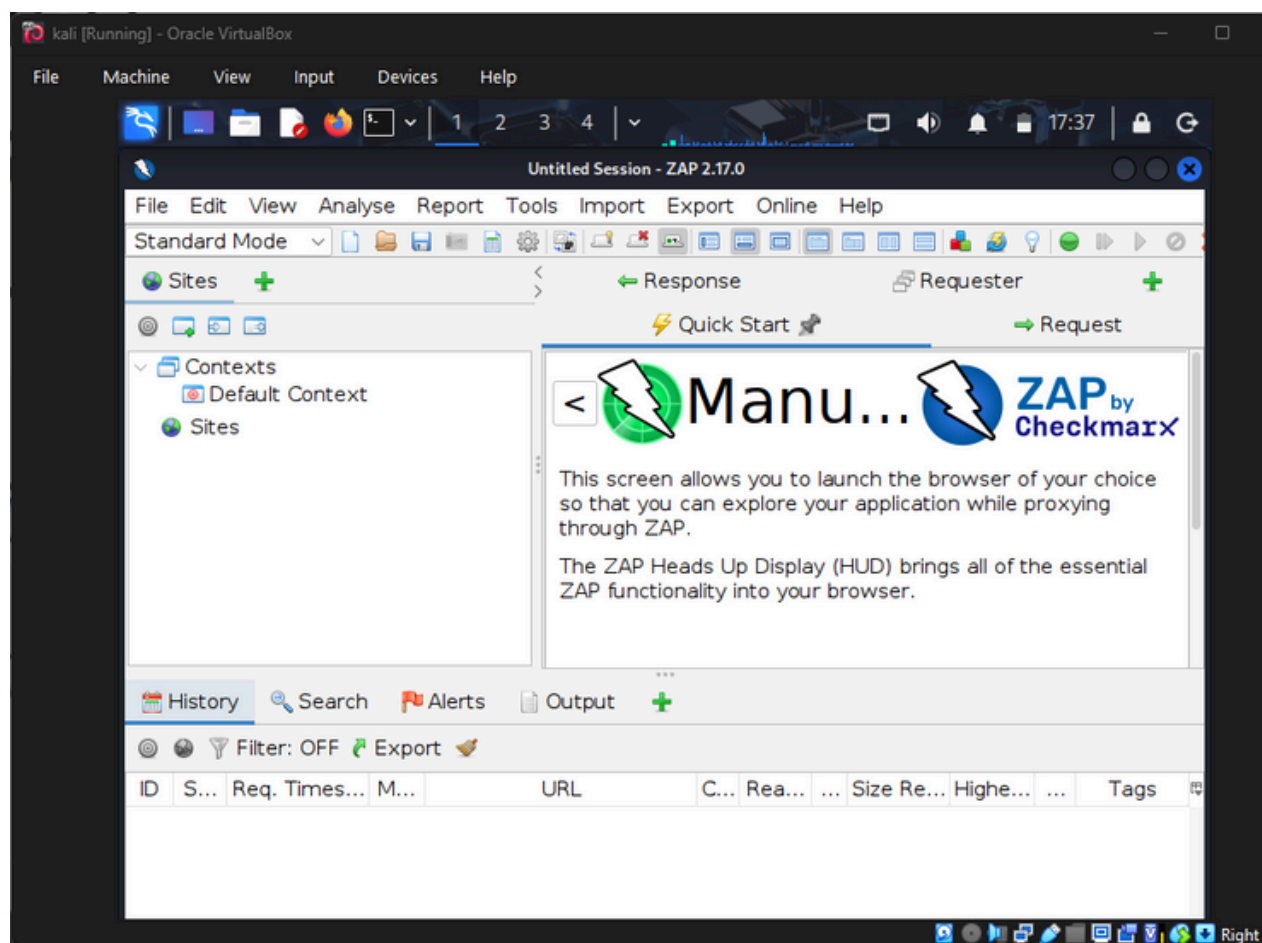
## 8. STEP 9: OWASP ZAP PASSIVE SCAN

OWASP ZAP was used in Standard Mode to perform a passive vulnerability scan while browsing the site.

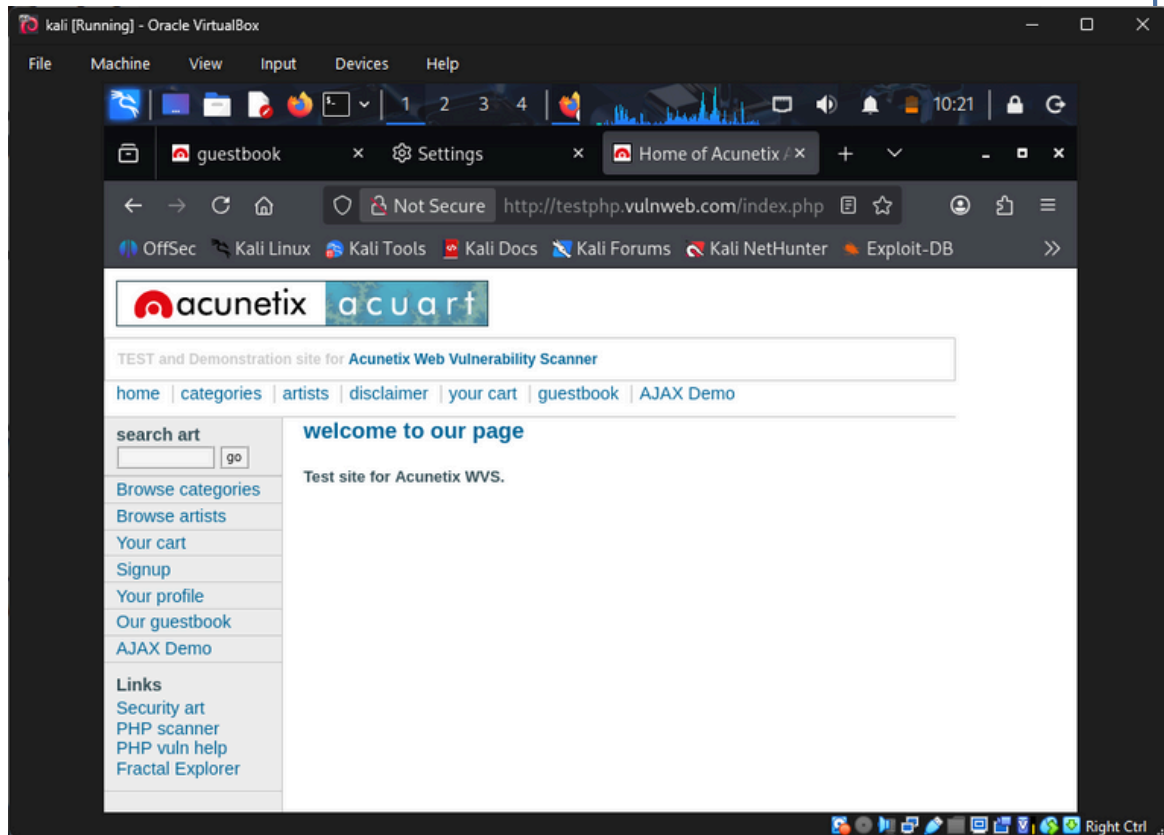
Identified Vulnerabilities:

| Vulnerability                   | Risk Level | Description                |
|---------------------------------|------------|----------------------------|
| Absence of Anti-CSRF Tokens     | Medium     | Forms lack CSRF protection |
| Content Security Policy Not Set | Low        | CSP header missing         |

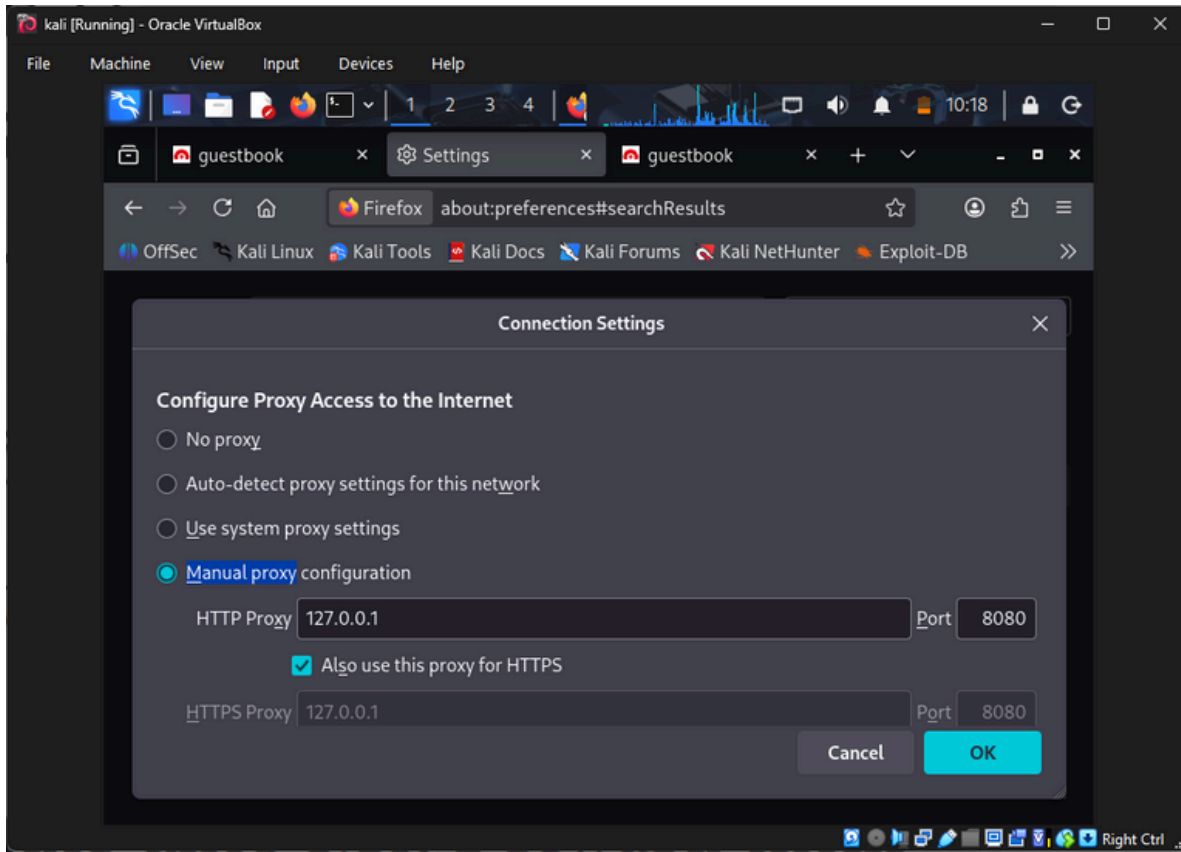
Zaproxy:



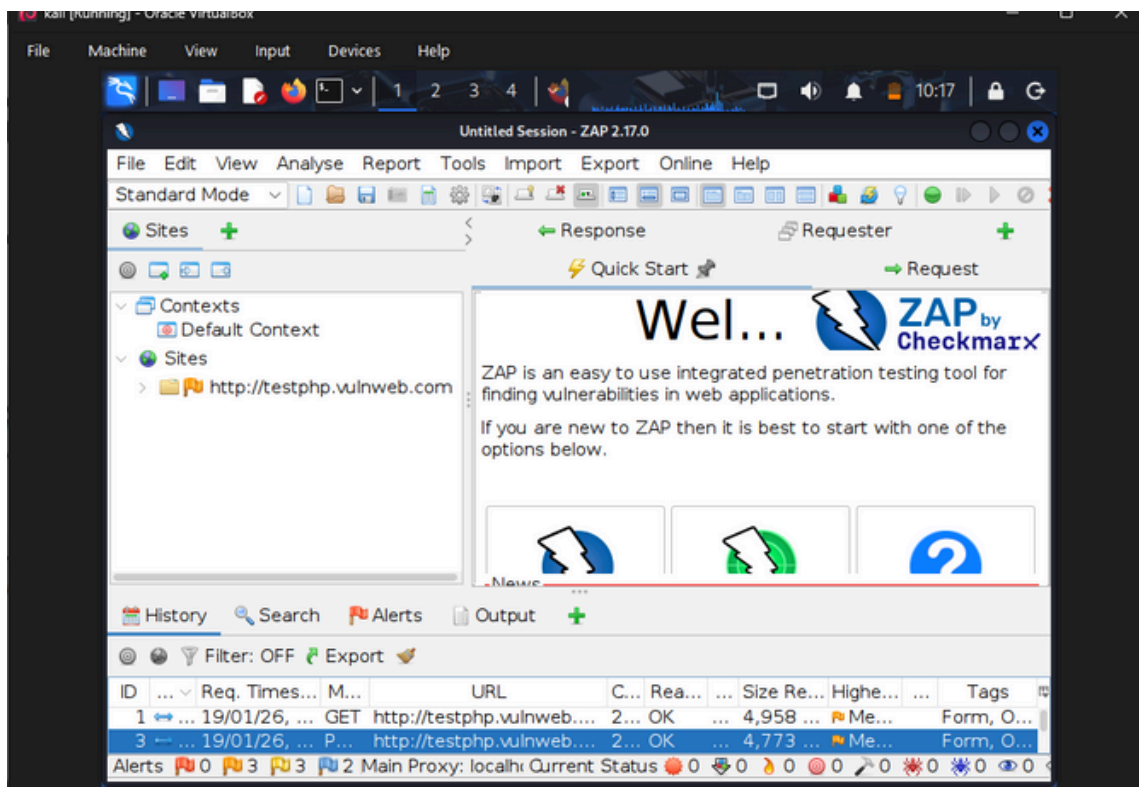
## WEBSITE FOR TESTING:



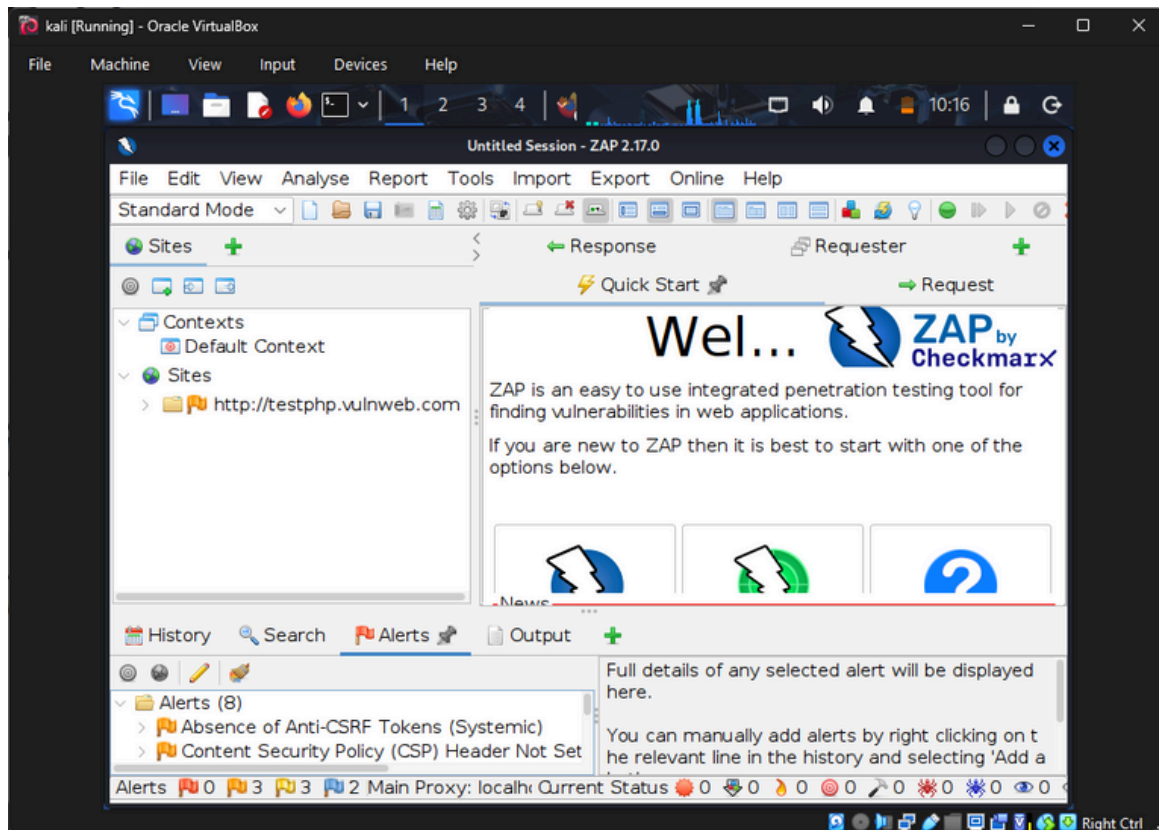
## MANUAL PROXY SETTING:



## HISTORY:



## ALERTS:



## ANALYSIS:

These findings indicate missing security headers and protections that could increase exposure to common web attacks if exploited.

## 9. CONCLUSION

The vulnerability assessment identified low to medium risk security misconfigurations, primarily related to missing security controls rather than active exploits. No critical vulnerabilities were exploited or tested.