

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:
 - Nmap
 - Web Browser (Manual Inspection)
 - Browser Developer Tools
 - OWASP ZAP (Passive Scan)

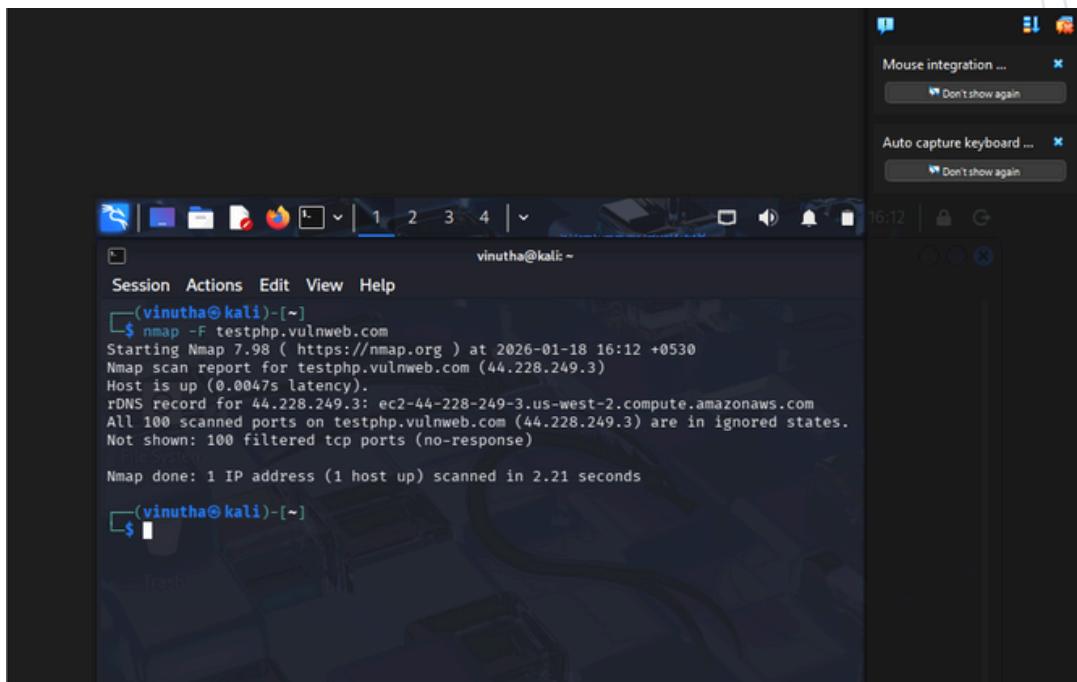
3. STEP 1: TARGET SELECTION

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 terminal window on a Kali Linux desktop. The terminal shows the command \$ nmap -F testphp.vulnweb.com being run. The output indicates that the host is up and all scanned ports are in ignored states. No critical vulnerabilities were detected.

```
$ 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.

5. STEP 3: ADDITIONAL NMAP ENUMERATION

Additional safe commands were executed to gather more exposure information.

Commands:

```
nmap --top-ports 20 testphp.vulnweb.com
```

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

```
vimothy@kali: ~
$ nmap --top-ports 20 testphp.vulnweb.com
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-18 16:22 +0530
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.001s latency).
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
22/tcp    filtered ssh
22/tcp    filtered netcat
23/tcp    filtered telnet
25/tcp    filtered smtp
53/tcp    filtered domain
80/tcp    filtered http
137/tcp   filtered netbios-dgm
138/tcp   filtered netbios-ssn
139/tcp   filtered netbios-ssn
443/tcp   filtered http
445/tcp   filtered microsoft-ds
993/tcp   filtered imap
995/tcp   filtered imap
1723/tcp  filtered pptp
2308/tcp  filtered mybase
3300/tcp  filtered vnc
5900/tcp  filtered rdp-server
5900/tcp  filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 2.21 seconds

[+] vimothy@kali: ~
$ nmap -sV testphp.vulnweb.com
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-18 16:23 +0530
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.001s latency).
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
22/tcp    filtered ssh
22/tcp    filtered netcat
23/tcp    filtered telnet
25/tcp    filtered smtp
53/tcp    filtered domain
80/tcp    filtered http
137/tcp   filtered netbios-dgm
138/tcp   filtered netbios-ssn
139/tcp   filtered netbios-ssn
443/tcp   filtered http
445/tcp   filtered microsoft-ds
993/tcp   filtered imap
995/tcp   filtered imap
1723/tcp  filtered pptp
2308/tcp  filtered mybase
3300/tcp  filtered vnc
5900/tcp  filtered rdp-server
5900/tcp  filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 6.30 seconds

[+] vimothy@kali: ~
$ nmap -v --version-list testphp.vulnweb.com
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-18 16:24 +0530
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.001s latency).
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
22/tcp    filtered ssh
22/tcp    filtered netcat
23/tcp    filtered telnet
25/tcp    filtered smtp
53/tcp    filtered domain
80/tcp    filtered http
137/tcp   filtered netbios-dgm
138/tcp   filtered netbios-ssn
139/tcp   filtered netbios-ssn
443/tcp   filtered http
445/tcp   filtered microsoft-ds
993/tcp   filtered imap
995/tcp   filtered imap
1723/tcp  filtered pptp
2308/tcp  filtered mybase
3300/tcp  filtered vnc
5900/tcp  filtered rdp-server
5900/tcp  filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 9.72 seconds

[+] vimothy@kali: ~
```

```
vimothy@kali: ~
$ nmap -v --version-list 20 -T2 testphp.vulnweb.com
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-18 16:31 +0530
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.001s latency).
PORT      STATE SERVICE
22/tcp    filtered ssh
22/tcp    filtered netcat
23/tcp    filtered telnet
25/tcp    filtered smtp
53/tcp    filtered domain
80/tcp    filtered http
137/tcp   filtered netbios-dgm
138/tcp   filtered netbios-ssn
139/tcp   filtered netbios-ssn
443/tcp   filtered http
445/tcp   filtered microsoft-ds
993/tcp   filtered imap
995/tcp   filtered imap
1723/tcp  filtered pptp
2308/tcp  filtered mybase
3300/tcp  filtered vnc
5900/tcp  filtered rdp-server
5900/tcp  filtered http-proxy

Nmap done: 1 IP address (1 host up) scanned in 69.85 seconds

[+] vimothy@kali: ~
```

6. STEP 7: MANUAL BROWSER-BASED INSPECTION

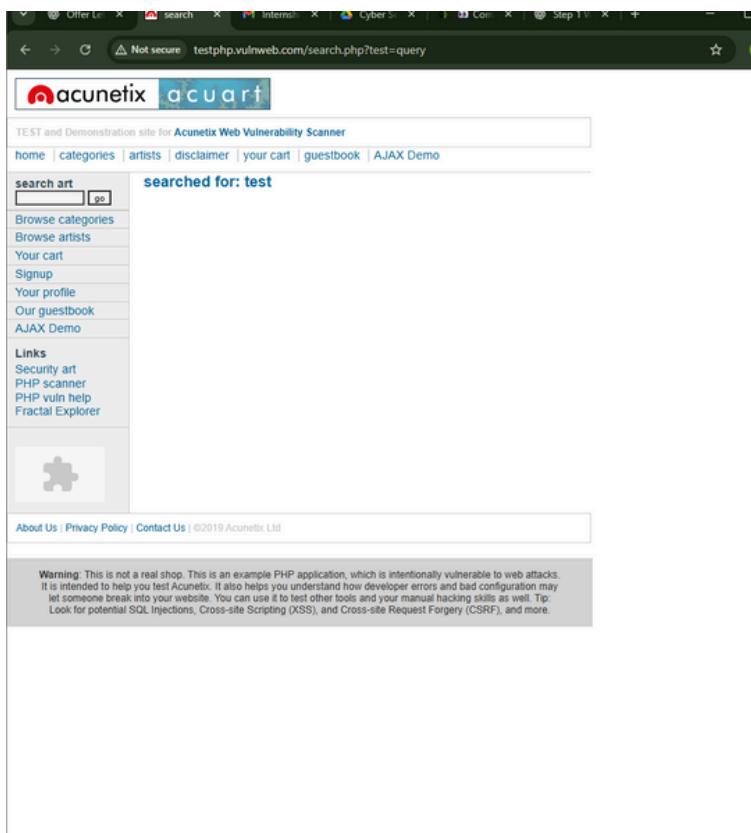
The website was manually explored using a standard web browser.

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.

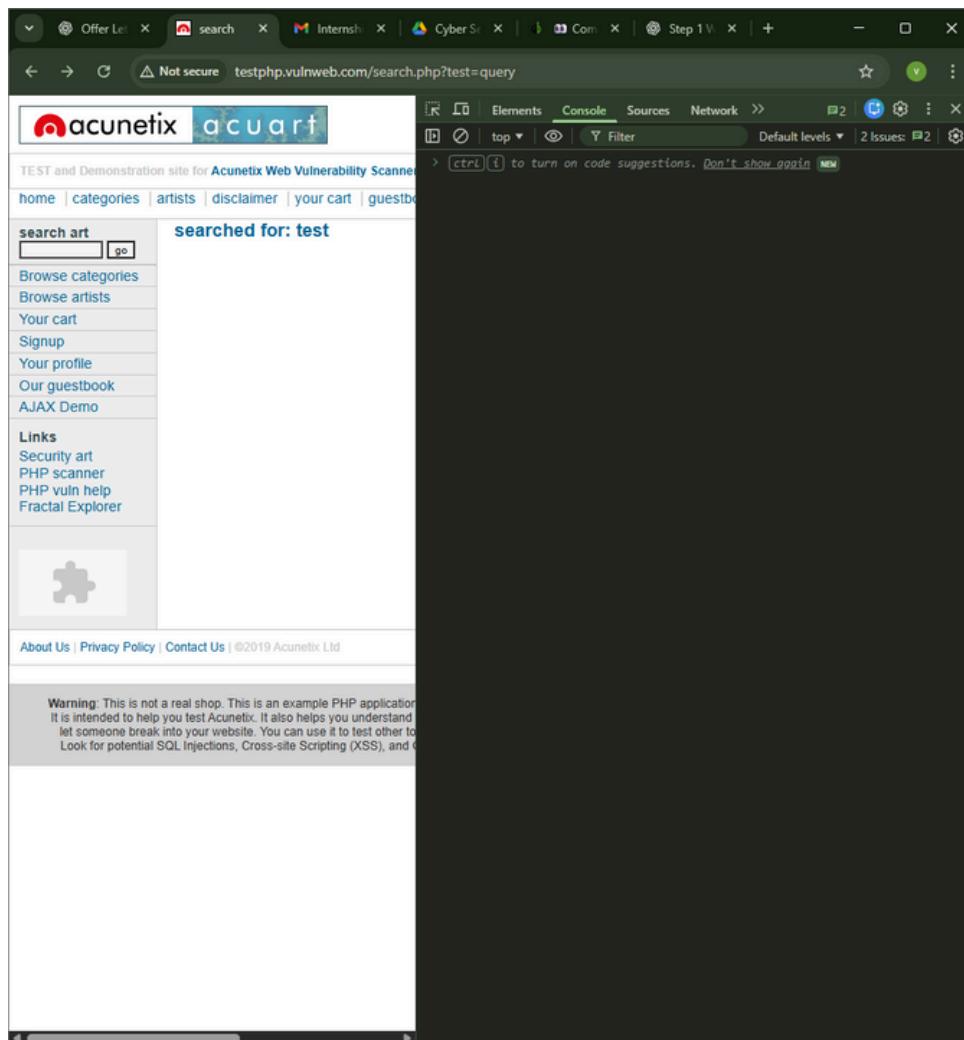


7. STEP 8: BROWSER DEVELOPER TOOLS ANALYSIS

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

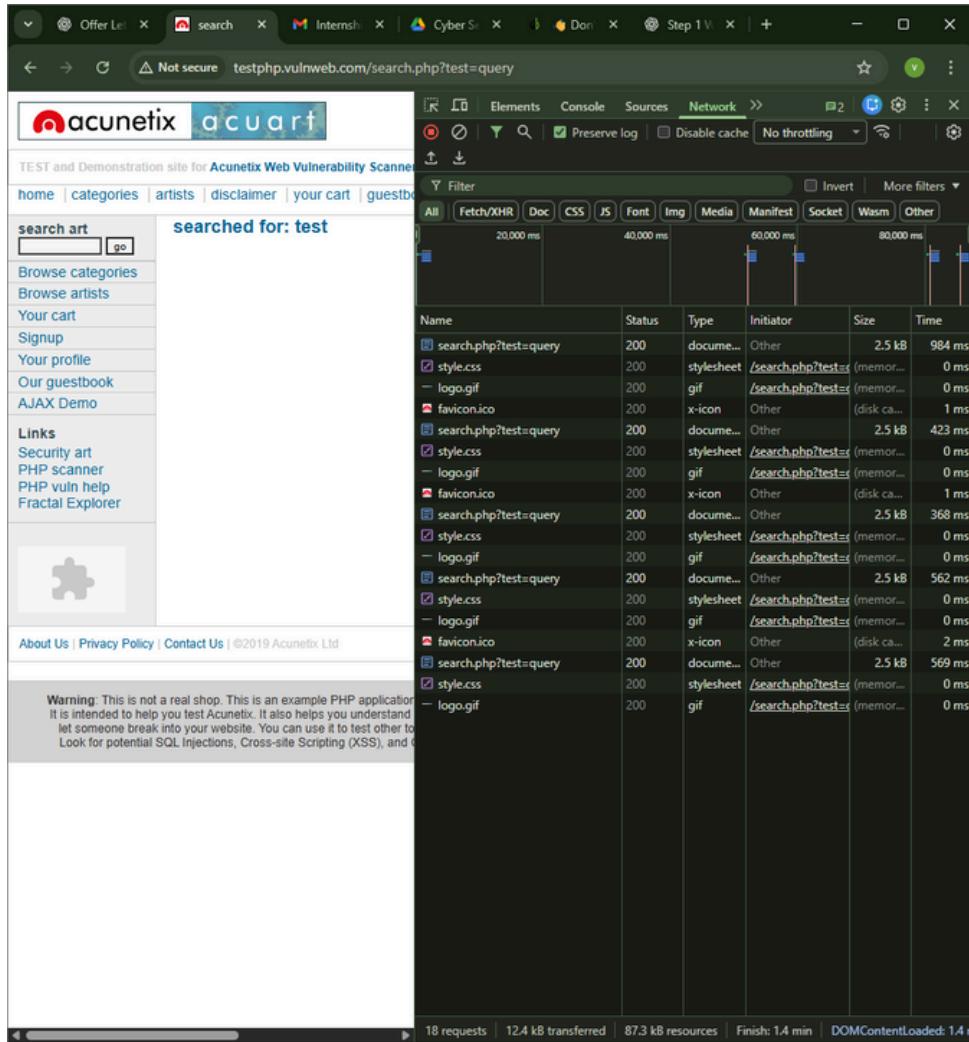
Console Tab:

- Minor JavaScript warnings
- No critical runtime errors



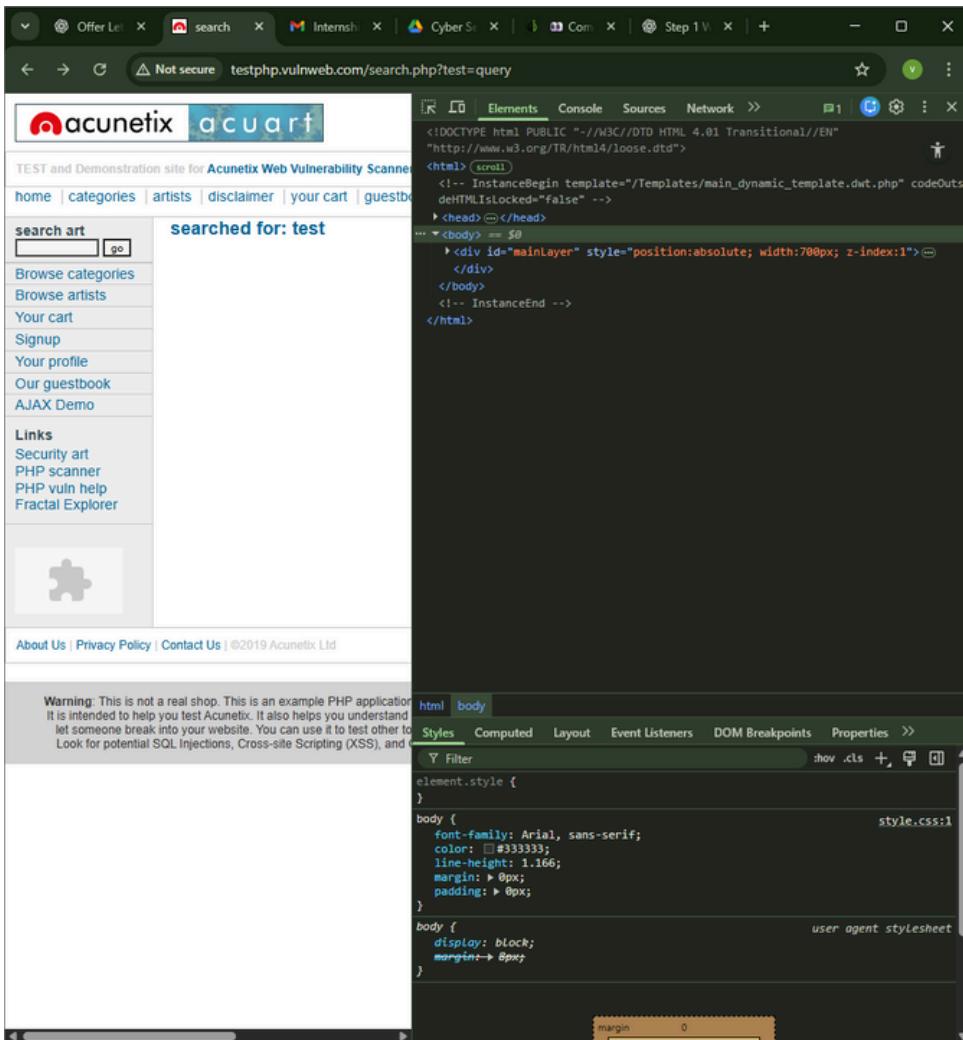
NETWORK TAB:

- HTTP requests observed
- Parameters transmitted via GET requests



ELEMENTS TAB:

- HTML structure reviewed
- No sensitive credentials found in DOM



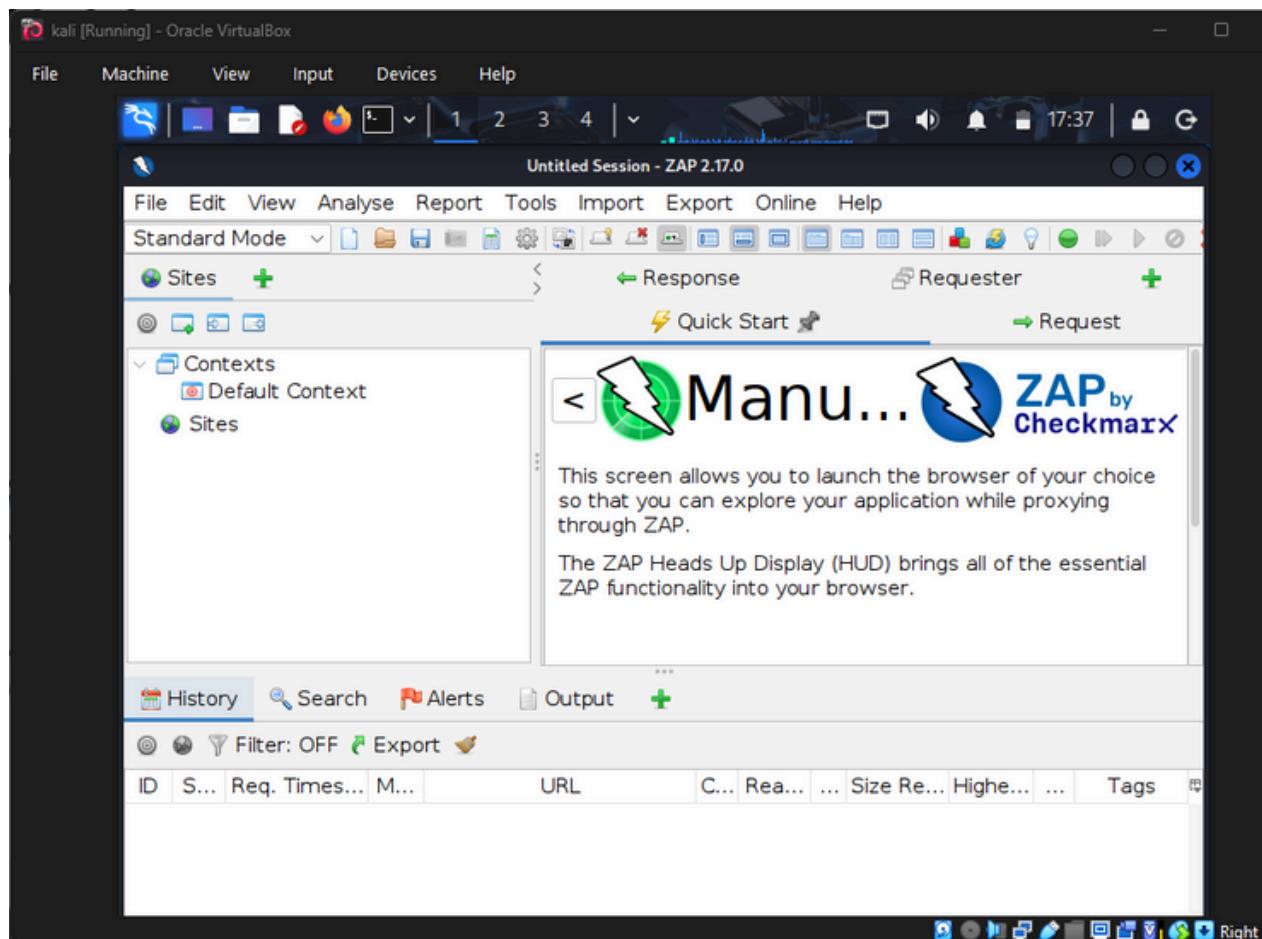
8. STEP 9: OWASP ZAP PASSIVE SCAN

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

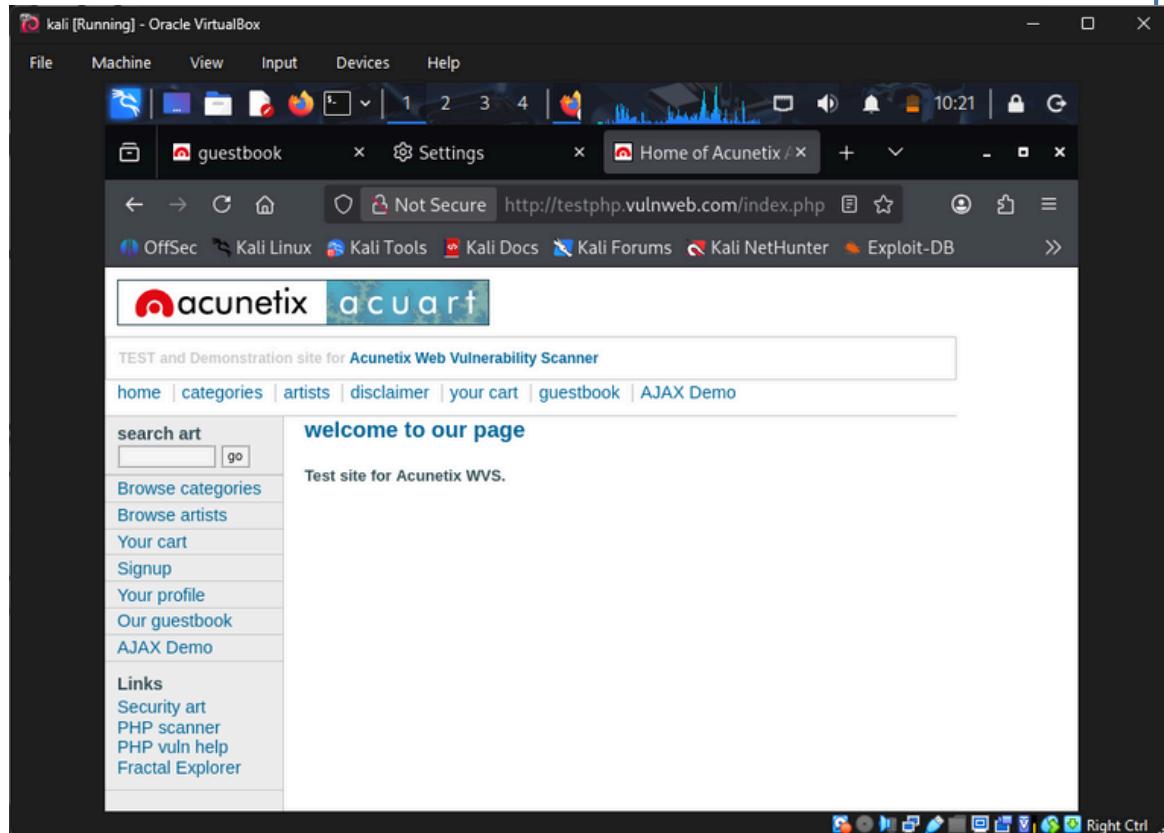
Identified Vulnerabilities:

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

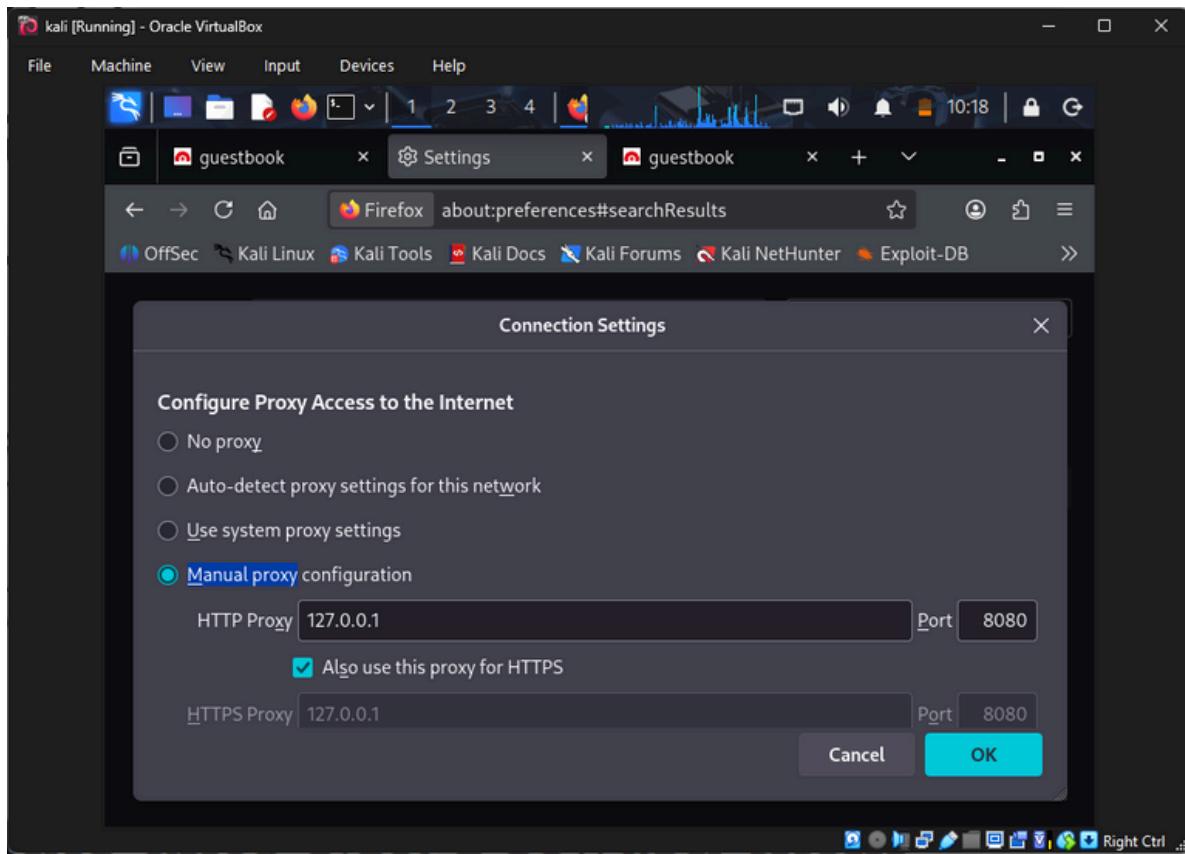
Zaproxy:



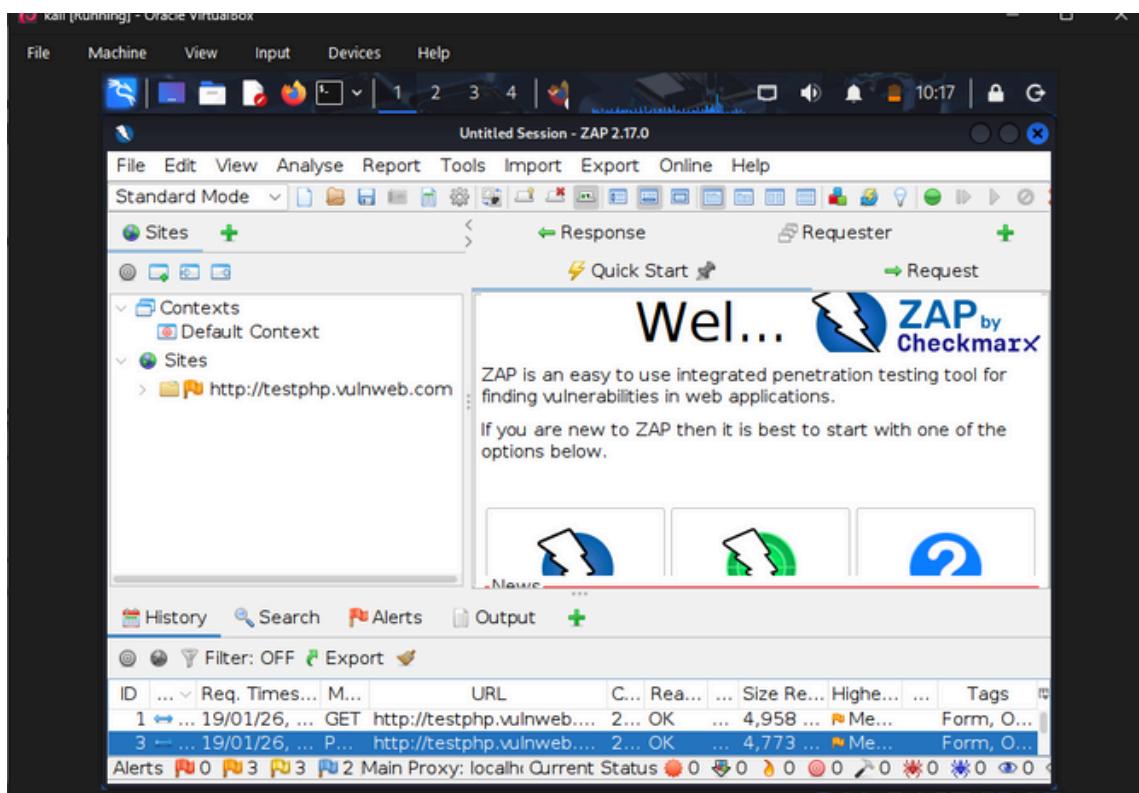
WEBSITE FOR TESTING:



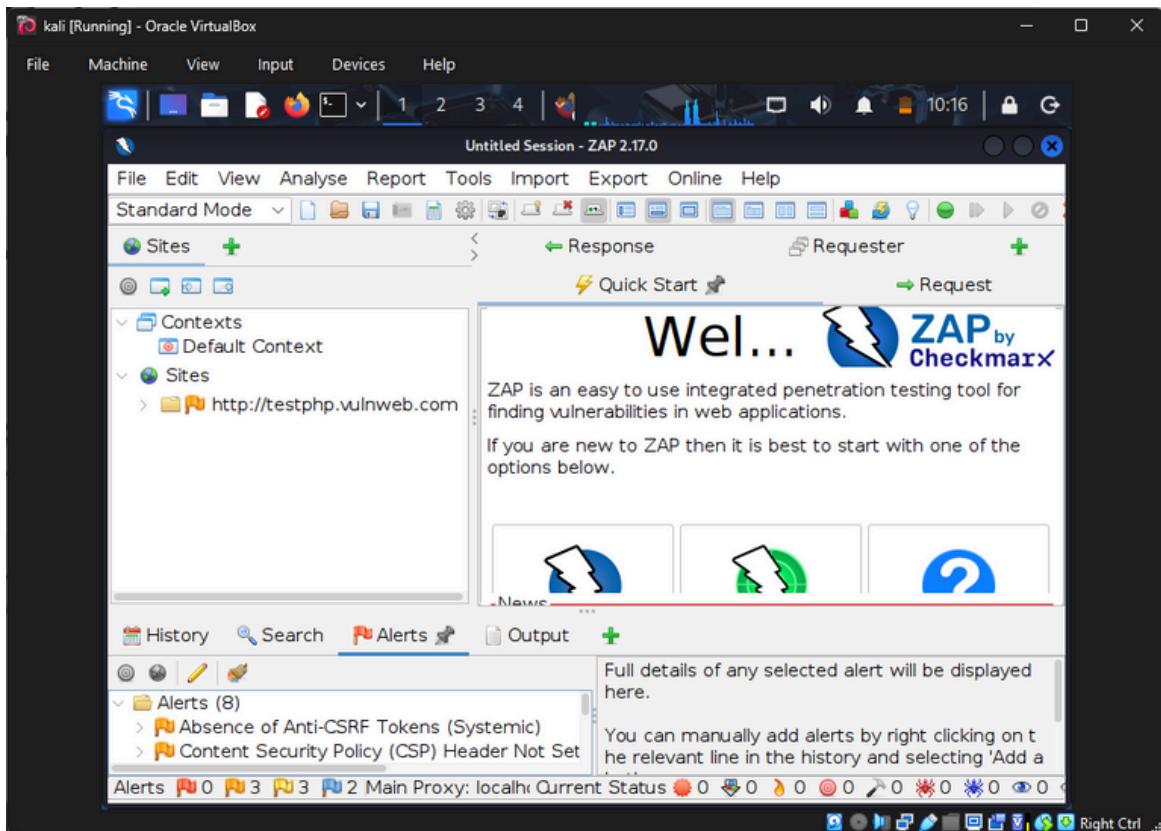
MANUAL PROXY SETTING:



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.