Vulnerability Assessment & Penetration Testing (VAPT) Report

Target: testphp.vulnweb.com

1. Executive Summary

This document presents the findings of a vulnerability assessment conducted against the web application testphp.vulnweb.com. The evaluation employed non-destructive automated techniques (Nmap, Nikto, Gobuster) and passive inspection via an HTTP proxy (Burp Suite). No active exploitation was performed. During the assessment, no interactive input fields suitable for SQL Injection or XSS validation tests were identified; therefore, injection testing was not performed. The primary focus of this review was on server configuration, component disclosures, and HTTP security headers.

2. Scope & Authorization

Scope: External assessment of testphp.vulnweb.com (HTTP service). Authorization: The target is a designated
practice site intended for security testing; permission for lab-based testing is assumed. Limitations: No authenticated scans were conducted, and no destructive actions were undertaken.

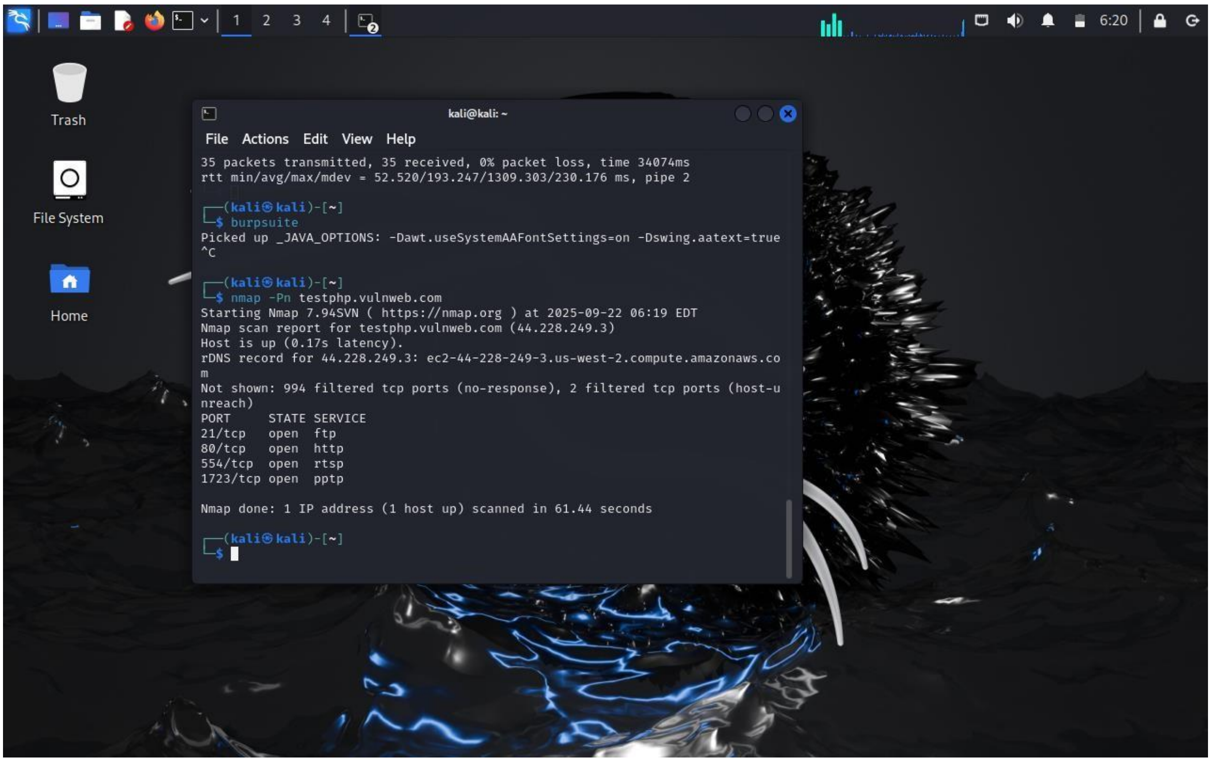
3. Methodology & Tools

Approach and tools employed: -
Nmap: identification of open ports and running services.
- Nikto: automated analysis of web server and application misconfigurations.
- Burp Suite (proxy, Repeater): interception and passive inspection of HTTP traffic.
- Gobuster: enumeration of common directories and files.

All activities were executed within an isolated laboratory environment (Kali Linux VM).

Network Scanning with Nmap:

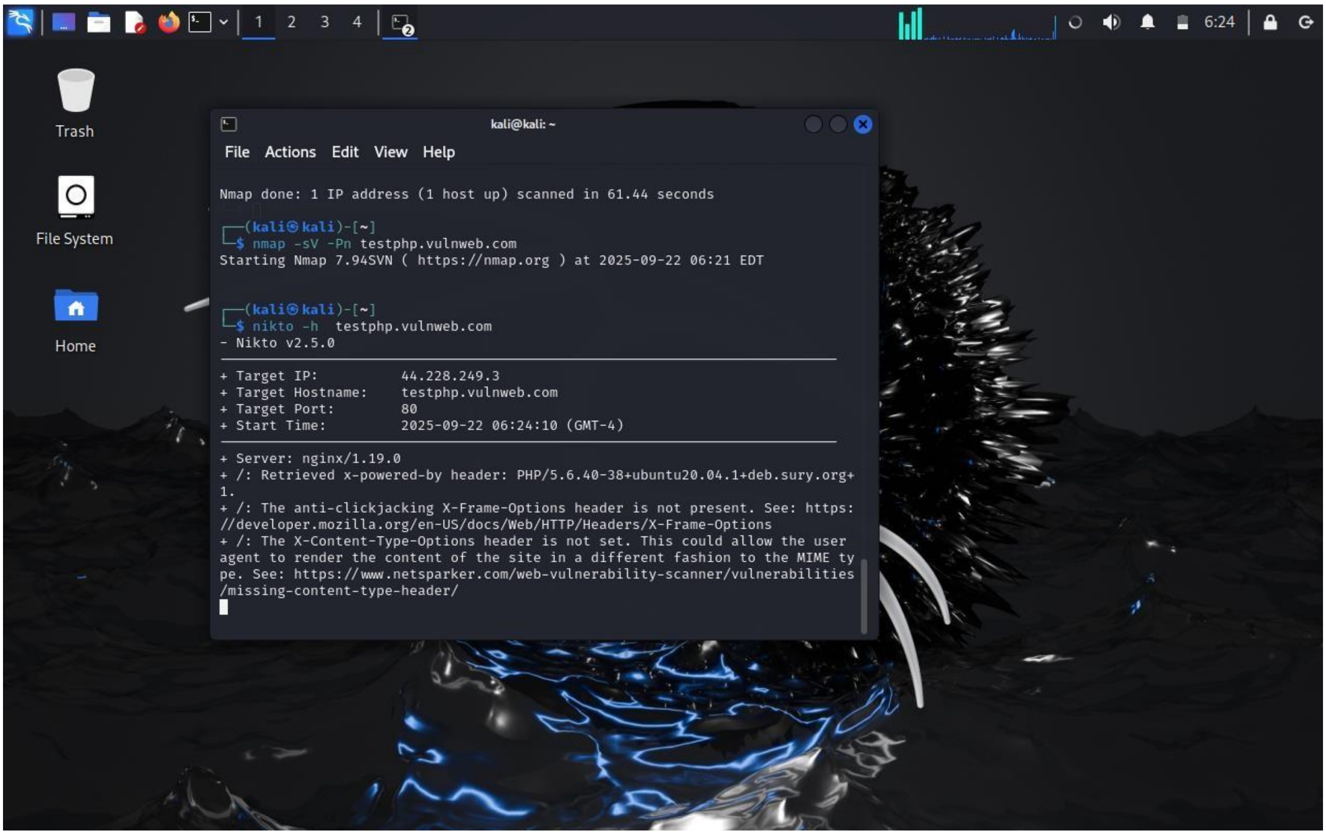
Running Nmap to perform a network scan on "testphp.vulnweb.com" to identify open ports and services.



```
35 packets transmitted, 35 received, 0% packet loss, time 34074ms
rtt min/avg/max/mdev = 52.520/193.247/1309.303/230.176 ms, pipe 2

┌──(kali㉿kali)-[~]
└─$ burpsuite
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
^C

┌──(kali㉿kali)-[~]
└─$ nmap -Pn testphp.vulnweb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-22 06:19 EDT
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.17s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.co
m
Not shown: 994 filtered tcp ports (no-response), 2 filtered tcp ports (host-u
nreach)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
554/tcp  open  rtsp
1723/tcp open  pptp

Nmap done: 1 IP address (1 host up) scanned in 61.44 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Automated WebApplication

Scanning with Nikto:

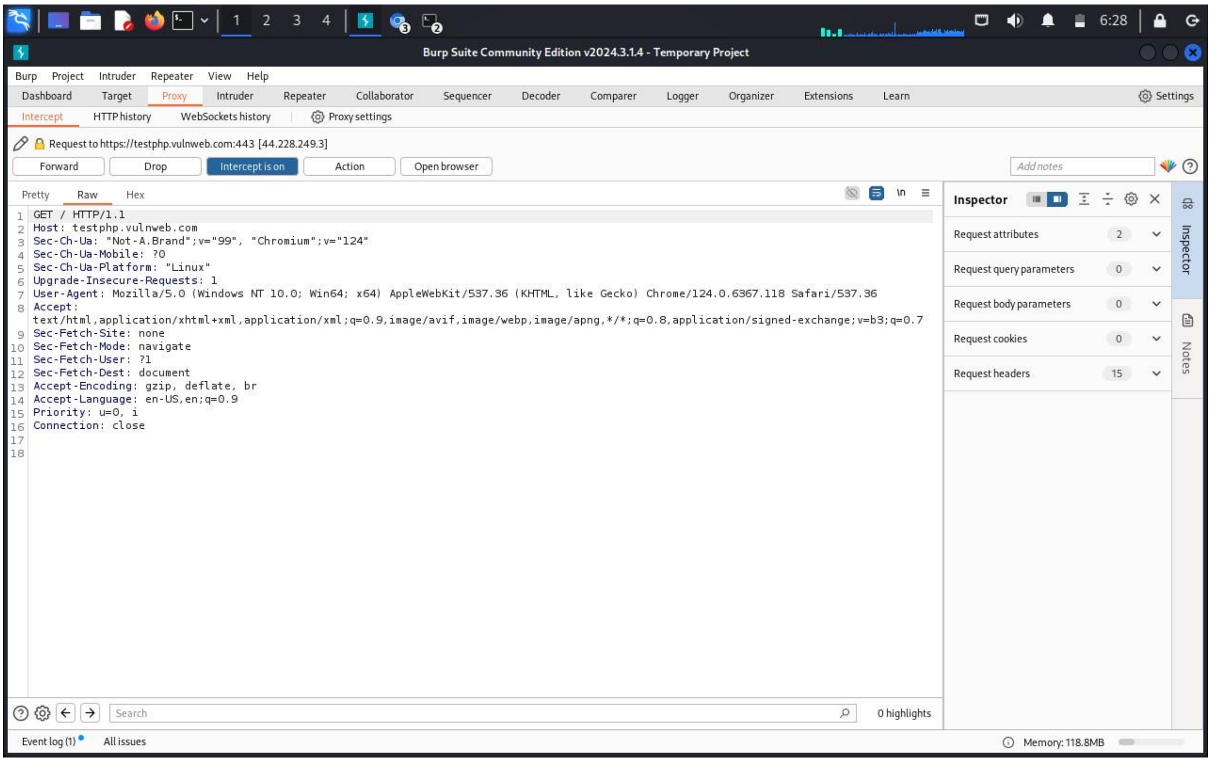


```
Nmap done: 1 IP address (1 host up) scanned in 61.44 seconds

┌──(kali㉿kali)-[~]
└─$ nmap -sV -Pn testphp.vulnweb.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-22 06:21 EDT


┌──(kali㉿kali)-[~]
└─$ nikto -h  testphp.vulnweb.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          44.228.249.3
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:        80
+ Start Time:         2025-09-22 06:24:10 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx/1.19.0
+ /: Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+
1.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https:
//developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user
agent to render the content of the site in a different fashion to the MIME ty
pe. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities
/missing-content-type-header/
```

WebApplication Assessment:

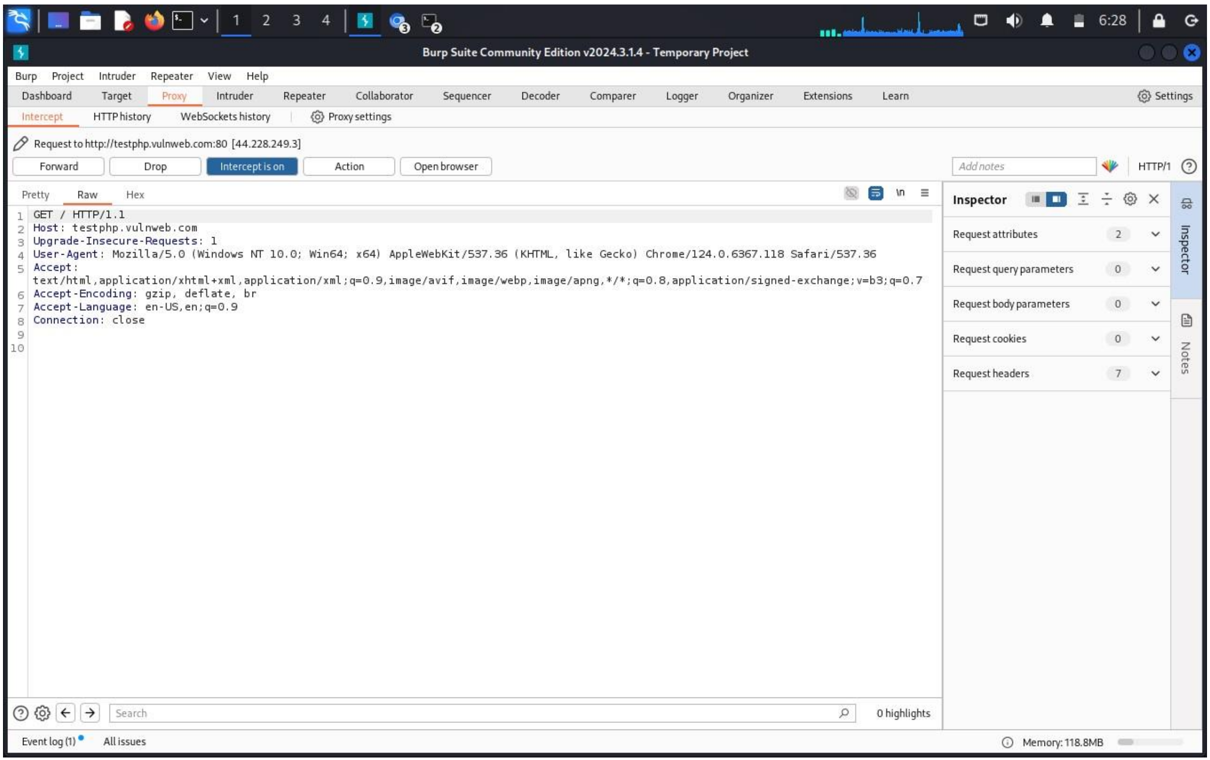
Manual WebApplication Assessment with Burpsuite:

Launched Burpsuite and configured browser to use it as a proxy. Navigated to "testphp.vulnweb.com" and intercept the traffic using Burpsuite.


Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Add notes
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 0
Request headers 15
Notes
Search
0 highlights
Event log (1) All issues
Memory: 118.8MB

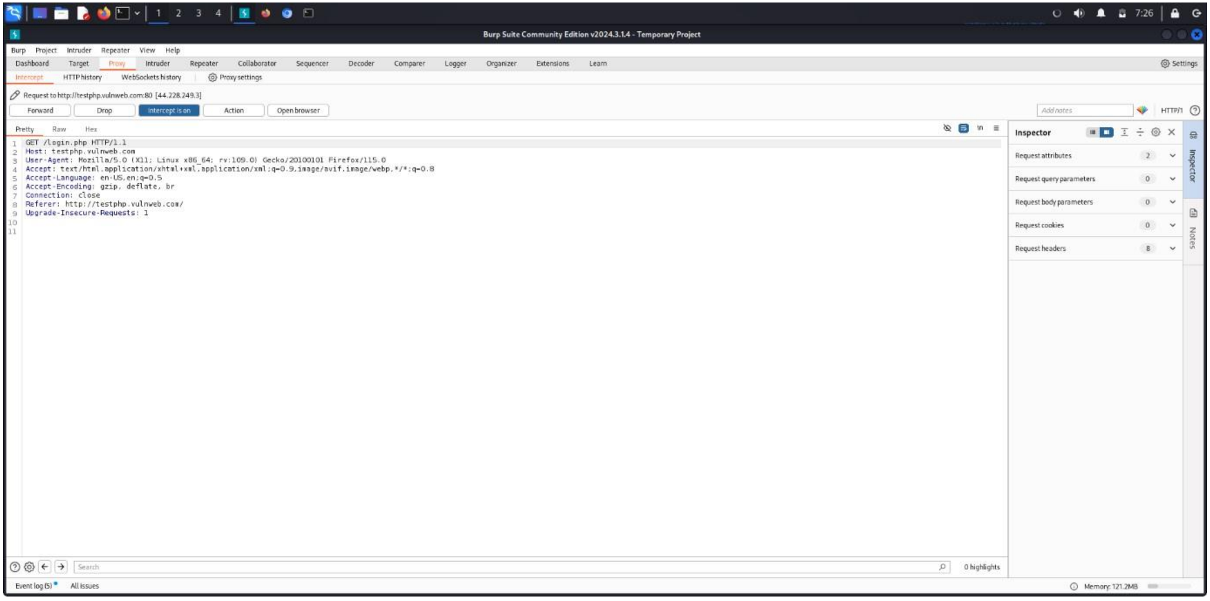
Request to https://testphp.vulnweb.com:443 [44.228.249.3]

```
GET / HTTP/1.1
Host: testphp.vulnweb.com
Sec-Ch-Ua: "Not-A.Brand";v="99", "Chromium";v="124"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
Connection: close


```


Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Add notes HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 0
Request headers 7
Notes
Search
0 highlights
Event log (1) All issues
Memory: 118.8MB

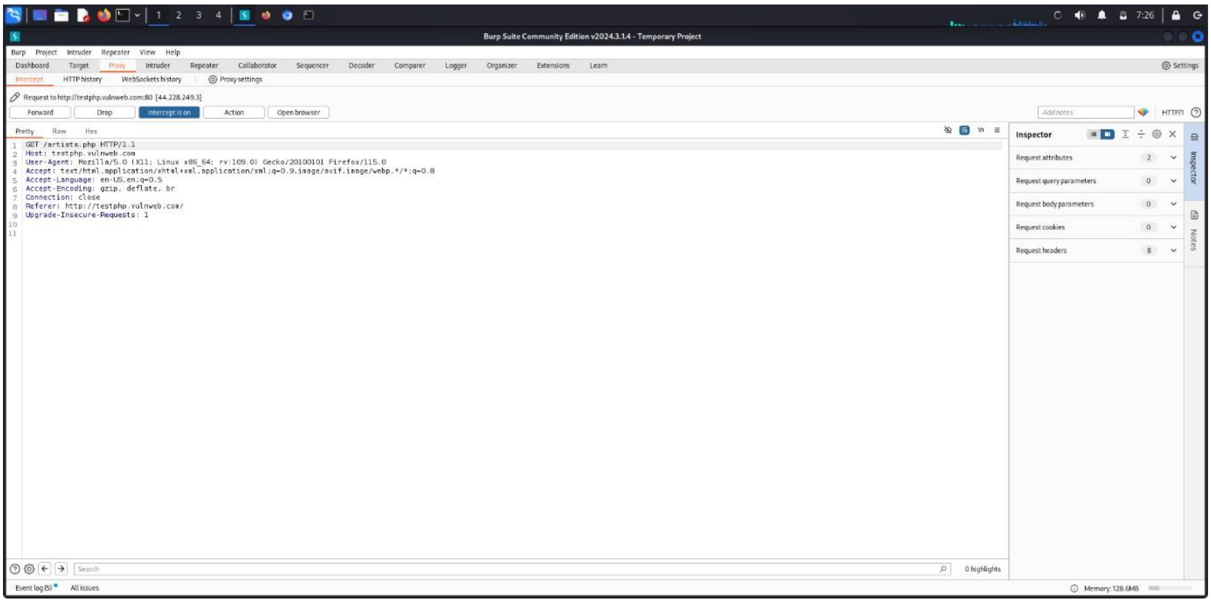
Request to http://testphp.vulnweb.com:80 [44.228.249.3]

```
GET / HTTP/1.1
Host: testphp.vulnweb.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
```


Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Add notes HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 0
Request headers 8
Notes
Search
0 highlights
Event log (5) All issues
Memory: 121.2MB

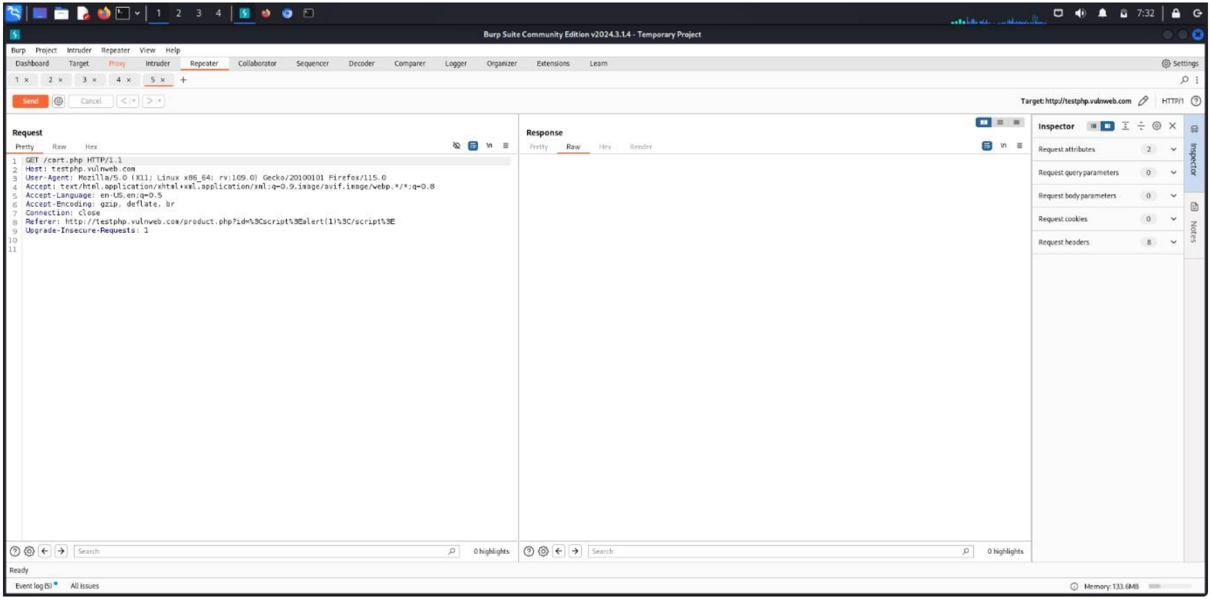
Request to http://testphp.vulnweb.com:80 [44.228.249.3]

```
GET /login.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://testphp.vulnweb.com/
Upgrade-Insecure-Requests: 1
```



Request to http://testphp.vulnweb.com:80 [44.228.249.3]

```
GET /artists.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://testphp.vulnweb.com/
Upgrade-Insecure-Requests: 1
```



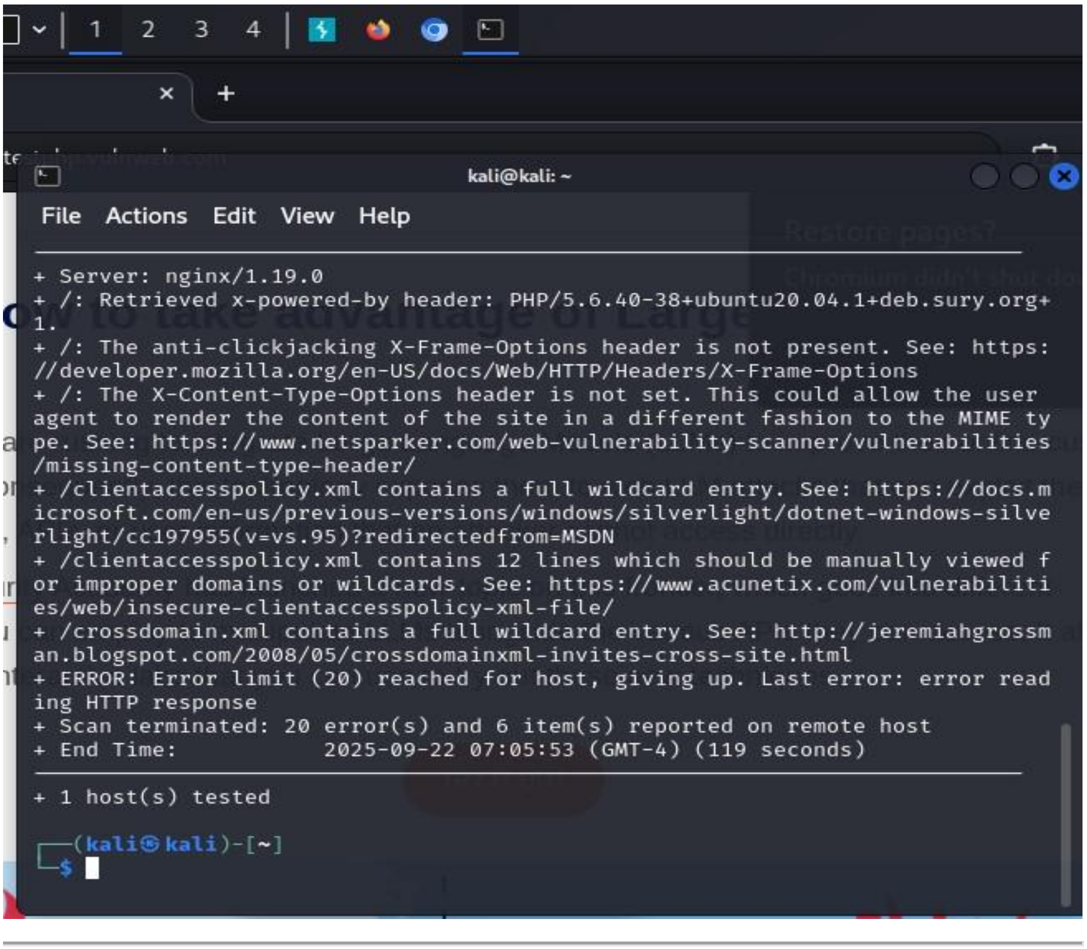
```
GET /cart.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://testphp.vulnweb.com/product.php?id=%3Cscript%3Ealert(1)%3C/script%3E
Upgrade-Insecure-Requests: 1
```

OWASP Top 10 Findings (Mapped)

#	Finding (quote)	OWASP Category	Severity	Impact (1 line)	Recommendation (one line)	Evidence (which screenshot)
1	Server: nginx/1.19.0 (server banner)	A09: Using Components with Known Vulnerabilities	High	Exposes an outdated server version; attackers can target known CVEs for that version.	Upgrade nginx to a supported version; hide server tokens (server_tokens off;) and remove version disclosure.	Screenshot: Nikto output line showing `Server: nginx/1.19.0`
2	Retrieved x-powered-by header: PHP/5.6.40-...	A09: Using Components with Known Vulnerabilities	High	Reveals old PHP version (EOL); likely to have public CVEs that enable RCE or info disclosure.	Upgrade PHP to a supported release (8.x) and disable X-Powered-By header in server/PHP config.	Screenshot: Nikto output showing `X-Powered-By`
3	The anti-clickjacking X-Frame-Options header is not present.	A05: Security Misconfiguration	Medium	Site is vulnerable to clickjacking (UI redress) attacks that can trick users.	Add header X-Frame-Options: DENY or SAMEORIGIN (nginx: add_header X-	Screenshot: Nikto line about X-Frame-Options missing

					Frame-Options "DENY" always;).	
4	The X-Content-Type-Options header is not set.	A05: Security Misconfiguration	Medium	Browser may incorrectly sniff content types — could enable some injection or XSS vectors.	Add header X-Content-Type-Options: nosniff (nginx add_header X-Content-Type-Options "nosniff" always;).	Screenshot: Nikto line about X-Content-Type-Options
5	clientaccesspolicy.xml contains a full wildcard entry	A05 / A06: Security Misconfiguration / Sensitive Data Exposure	Medium	Wildcard cross-domain policy allows any domain to access resources — may expose data to third parties.	Replace wildcard with explicit trusted domains or remove the file if not needed.	Screenshot: Nikto lines about clientaccesspolicy.xml
6	crossdomain.xml contains a full wildcard entry	A05 / A06	Medium	Same as above for Adobe Flash / cross-domain policies.	Restrict domains or remove.	Screenshot: Nikto lines about crossdomain.xml
7	ERROR: Error limit (20) reached... (scan errors)	N/A (scan artifact)	Info	Some scan requests failed — re-run with higher timeout to capture full results.	Re-run Nikto with higher timeout or use additional scanning (gobuster/nma	Screenshot: Nikto output showing error limit

					p) to gather missing data.	

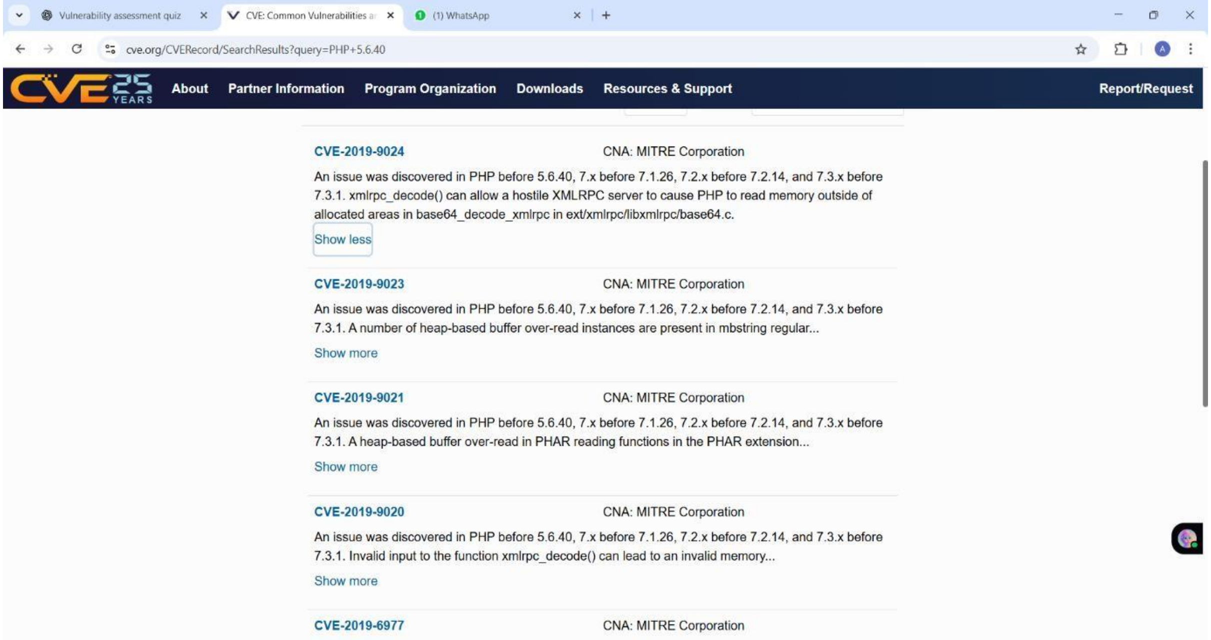


```
+ Server: nginx/1.19.0
+ /: Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+
1.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https:
//developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user
agent to render the content of the site in a different fashion to the MIME ty
pe. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities
/missing-content-type-header/
+ /clientaccesspolicy.xml contains a full wildcard entry. See: https://docs.m
icrosoft.com/en-us/previous-versions/windows/silverlight/dotnet-windows-silve
rlight/cc197955(v=vs.95)?redirectedfrom=MSDN
+ /clientaccesspolicy.xml contains 12 lines which should be manually viewed f
or improper domains or wildcards. See: https://www.acunetix.com/vulnerabiliti
es/web/insecure-clientaccesspolicy-xml-file/
+ /crossdomain.xml contains a full wildcard entry. See: http://jeremiahgrossm
an.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html
+ ERROR: Error limit (20) reached for host, giving up. Last error: error read
ing HTTP response
+ Scan terminated: 20 error(s) and 6 item(s) reported on remote host
+ End Time:           2025-09-22 07:05:53 (GMT-4) (119 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(kali㉿kali)-[~]
└─$ 
```

SQL Injection, Cross-Site Scripting (XSS),

During this assessment, automated scans and manual inspection did not reveal input vectors (such as search boxes, comment fields, or URL parameters) suitable for SQL Injection and XSS testing. If in future assessments interactive input points are present, the following steps are recommended: 1. Identify all client-controllable inputs (GET and POST parameters, form fields, headers). 2. Test reflected XSS by submitting simple payloads such as `alert(1)` and observe whether responses render unsanitized HTML. 3. For stored XSS, test inputs that persist and are rendered to other users (comments, profiles). 4. If XSS is confirmed, prioritize output encoding and input validation; implement Content Security Policy (CSP) and ensure proper HTML escaping at the server side.

CVE and CWE Analysis:.



CVE-2019-9024 CNA: MITRE Corporation

An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. xmlrpc_decode() can allow a hostile XMLRPC server to cause PHP to read memory outside of allocated areas in base64_decode_xmlrpc in ext/xmlrpc/libxmlrpc/base64.c.

Show less

CVE-2019-9023 CNA: MITRE Corporation

An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A number of heap-based buffer over-read instances are present in mbstring regular...

Show more

CVE-2019-9021 CNA: MITRE Corporation

An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A heap-based buffer over-read in PHAR reading functions in the PHAR extension...

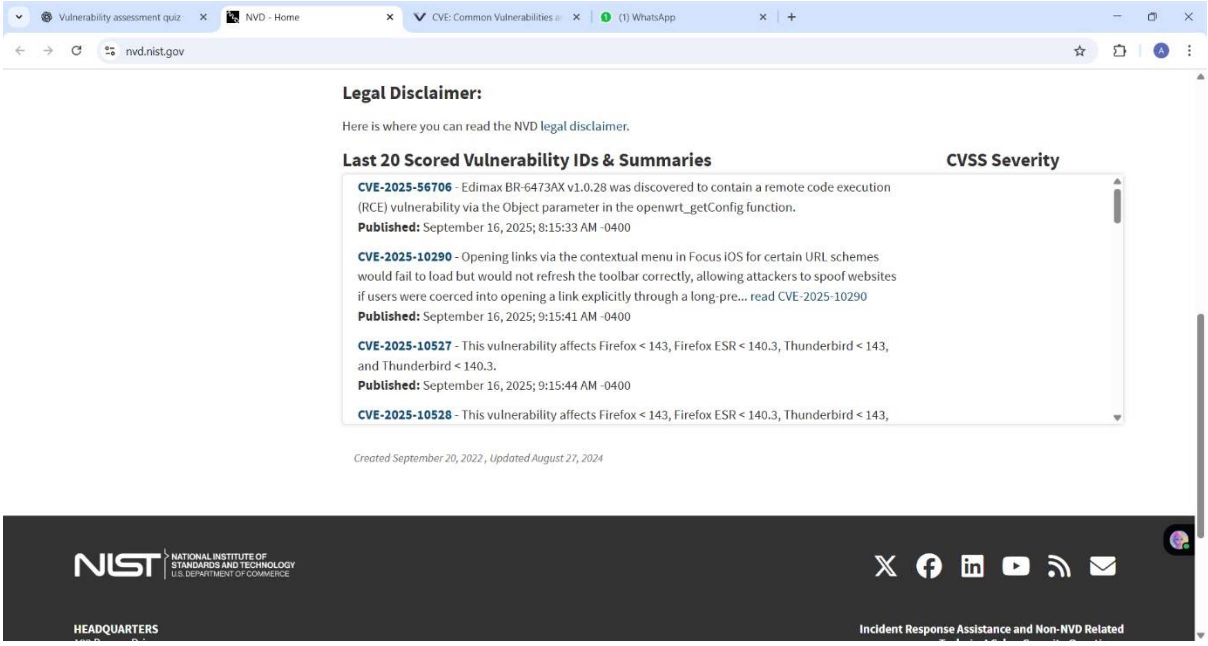
Show more

CVE-2019-9020 CNA: MITRE Corporation

An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. Invalid input to the function xmlrpc_decode() can lead to an invalid memory...

Show more

CVE-2019-6977 CNA: MITRE Corporation



Legal Disclaimer:

Here is where you can read the NVD legal disclaimer.

Last 20 Scored Vulnerability IDs & Summaries **CVSS Severity**

CVE-2025-56706 - Edimax BR-6473AX v1.0.28 was discovered to contain a remote code execution (RCE) vulnerability via the Object parameter in the openwrt_getConfig function.
Published: September 16, 2025; 8:15:33 AM -0400

CVE-2025-10290 - Opening links via the contextual menu in Focus iOS for certain URL schemes would fail to load but would not refresh the toolbar correctly, allowing attackers to spoof websites if users were coerced into opening a link explicitly through a long-pre... read CVE-2025-10290
Published: September 16, 2025; 9:15:41 AM -0400

CVE-2025-10527 - This vulnerability affects Firefox < 143, Firefox ESR < 140.3, Thunderbird < 143, and Thunderbird < 140.3.
Published: September 16, 2025; 9:15:44 AM -0400

CVE-2025-10528 - This vulnerability affects Firefox < 143, Firefox ESR < 140.3, Thunderbird < 143,

Created September 20, 2022 , Updated August 27, 2024

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

HEADQUARTERS

Incident Response Assistance and Non-NVD Related