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.

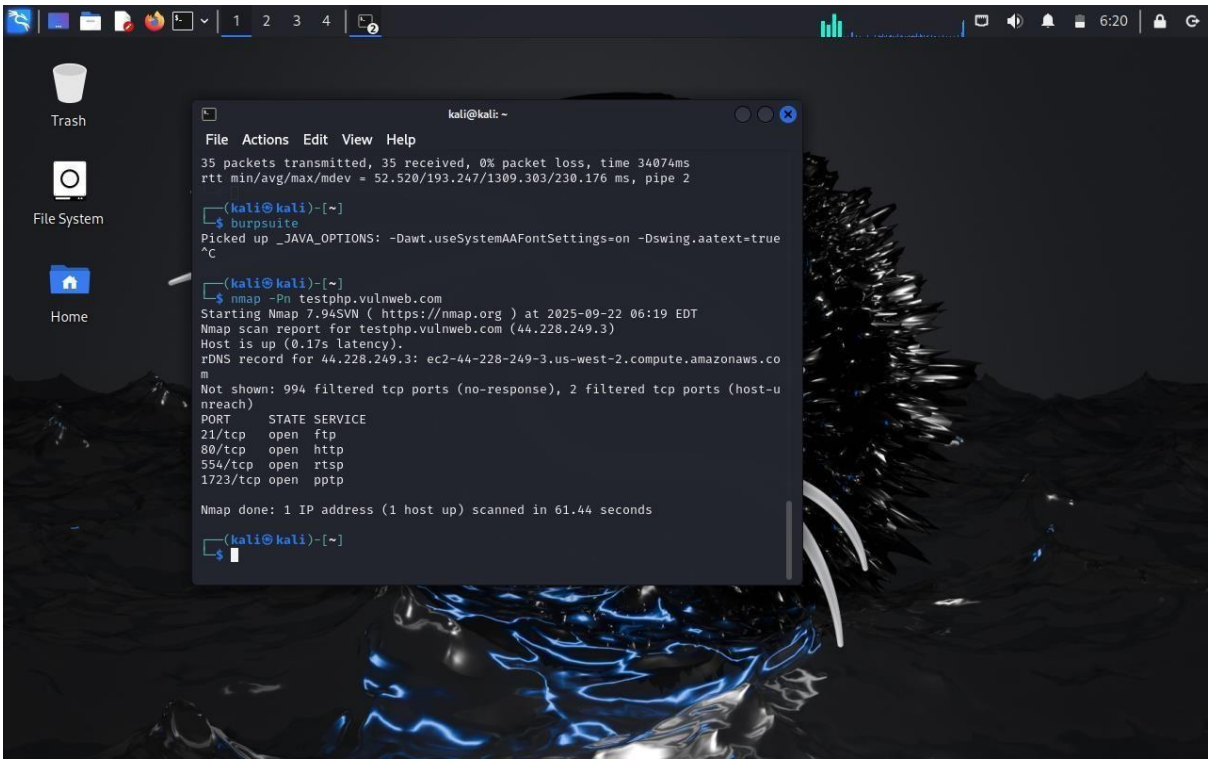
3. Methodology & Tools

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).

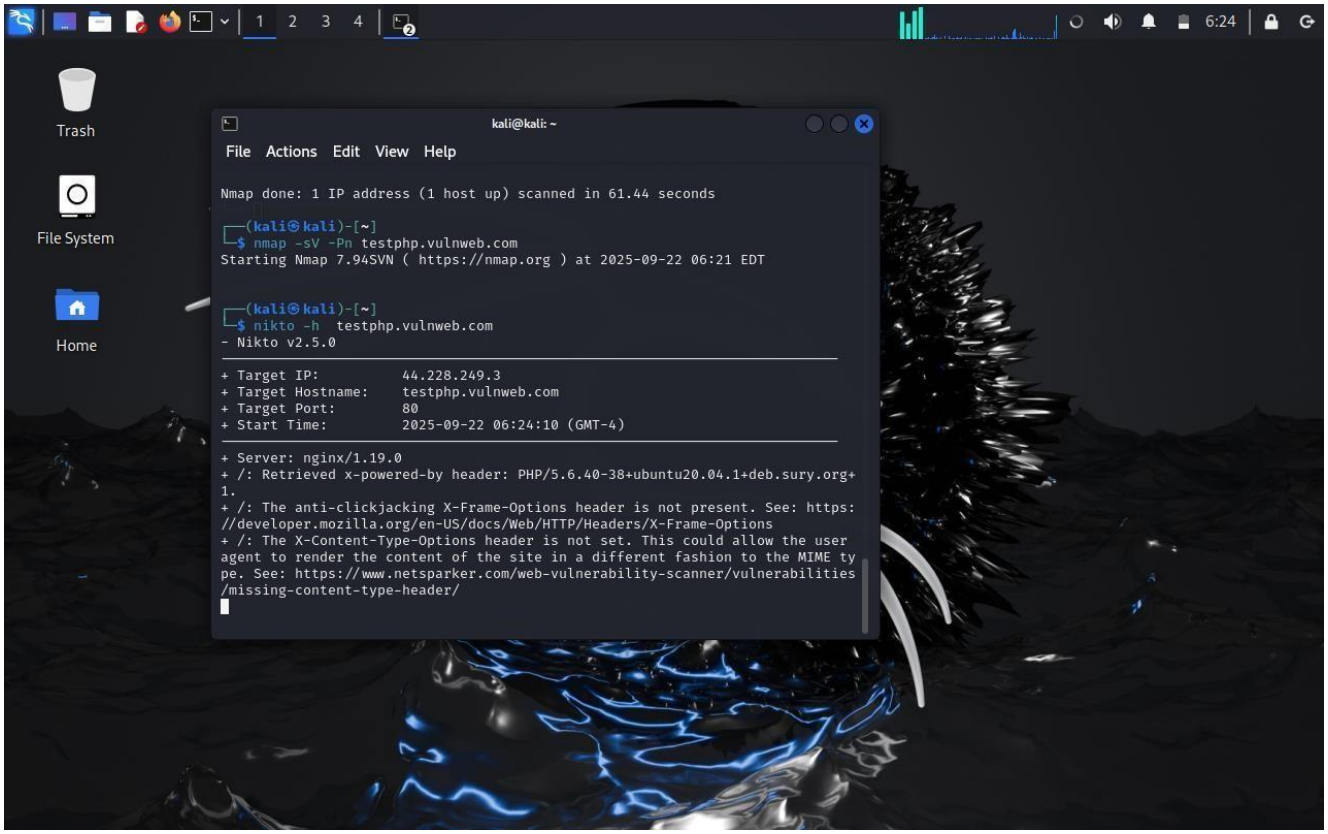
Network Scanning with Nmap:

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



Automated WebApplication Scanning

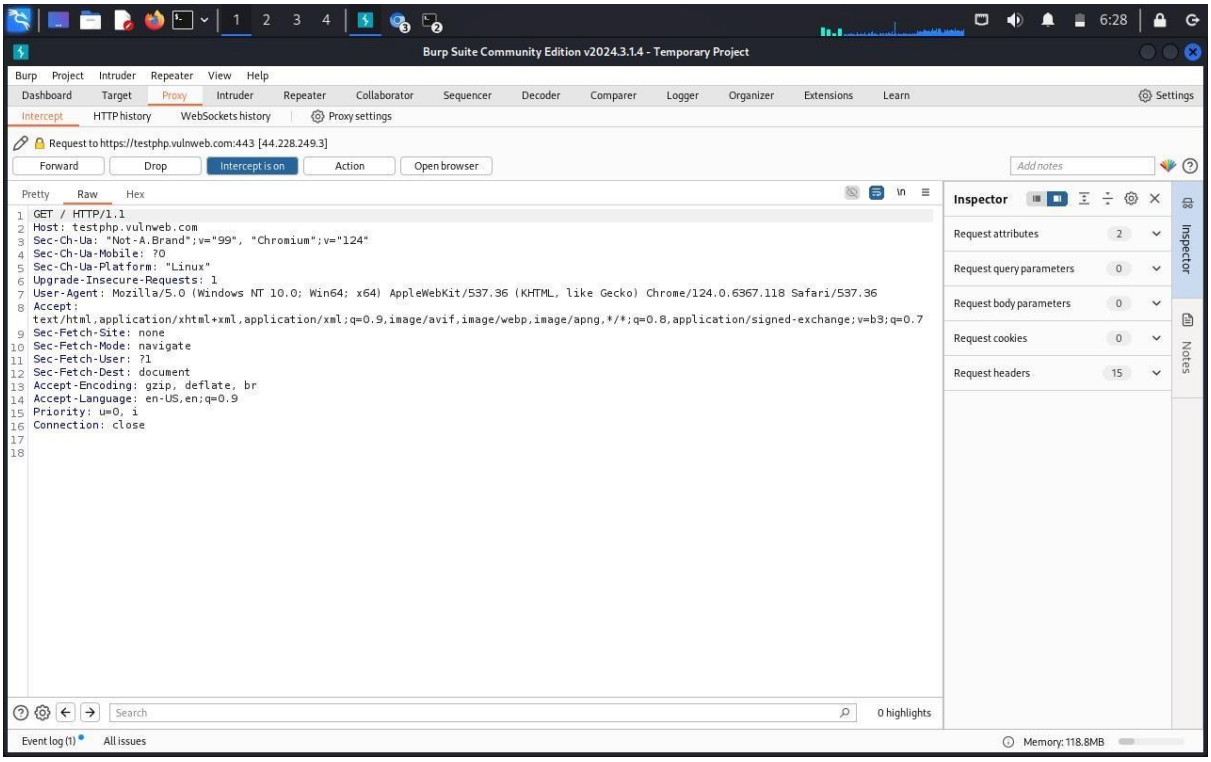
with Nikto:

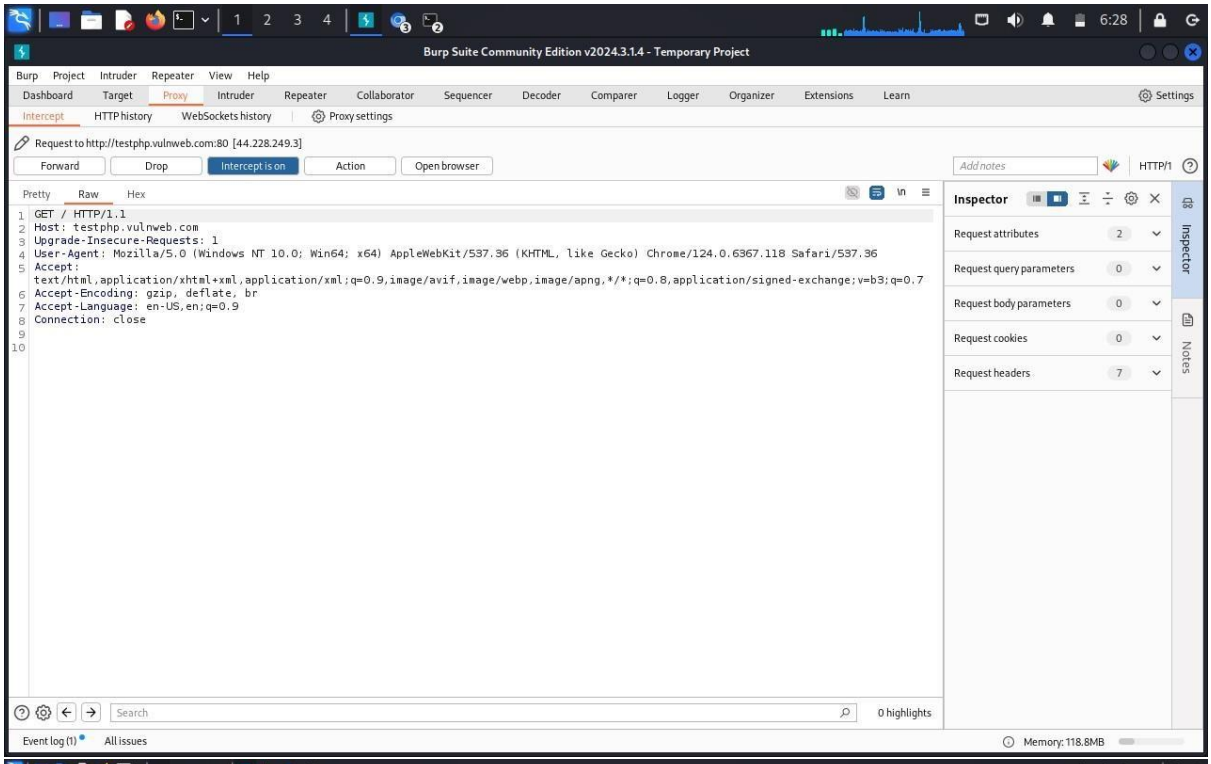


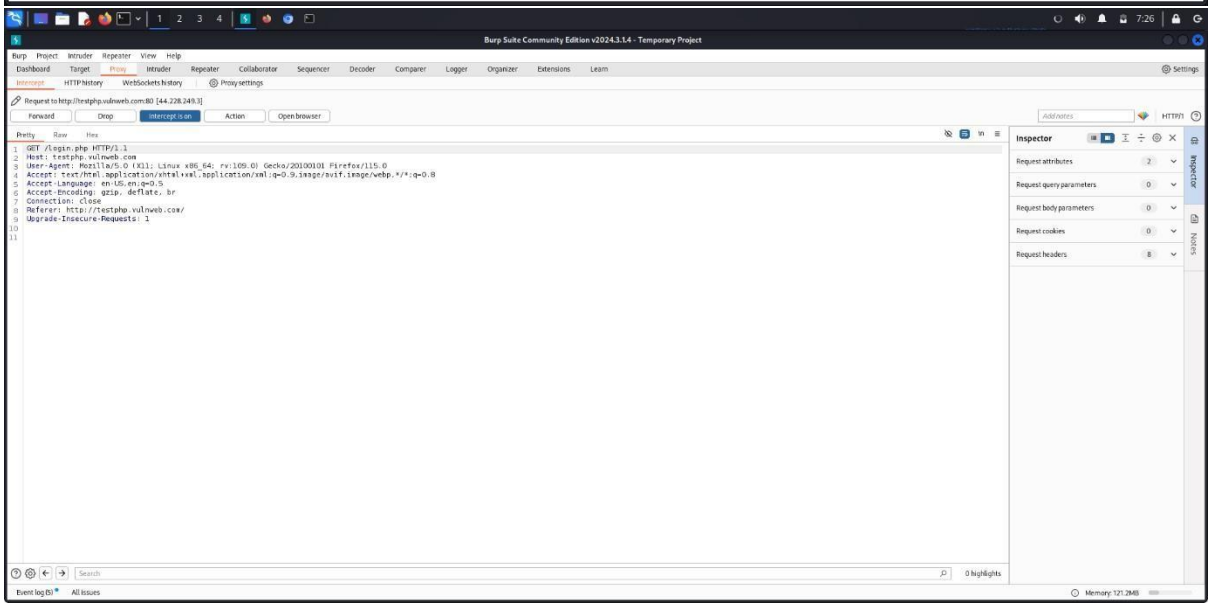
WebApplication Assessment:

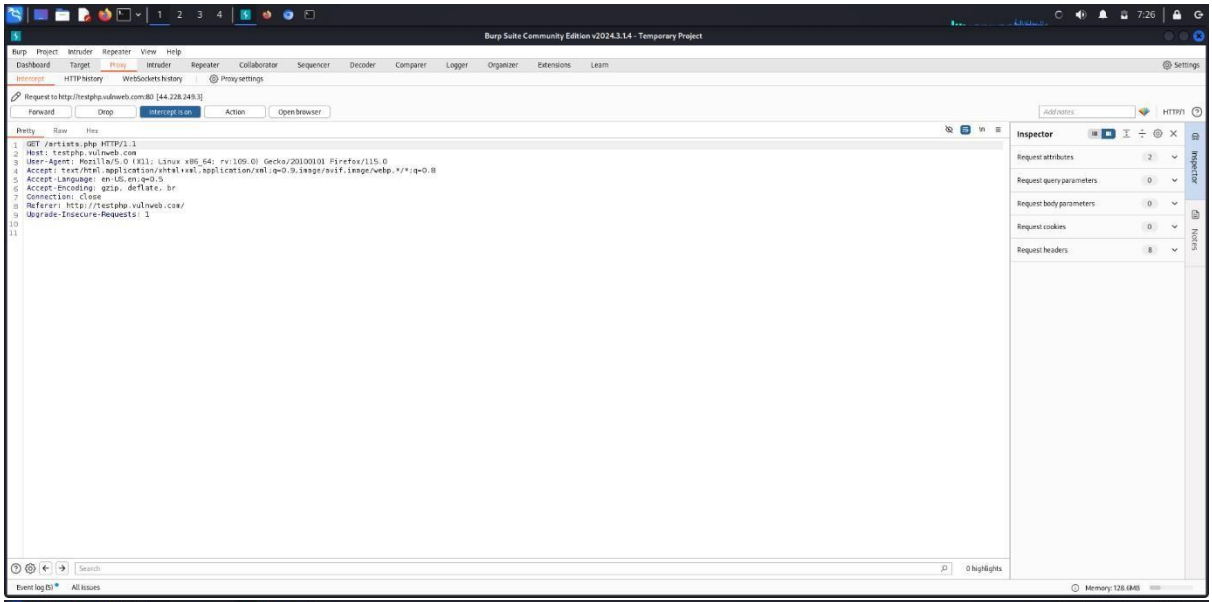
Manual WebApplication Assessment with Burpsuite:

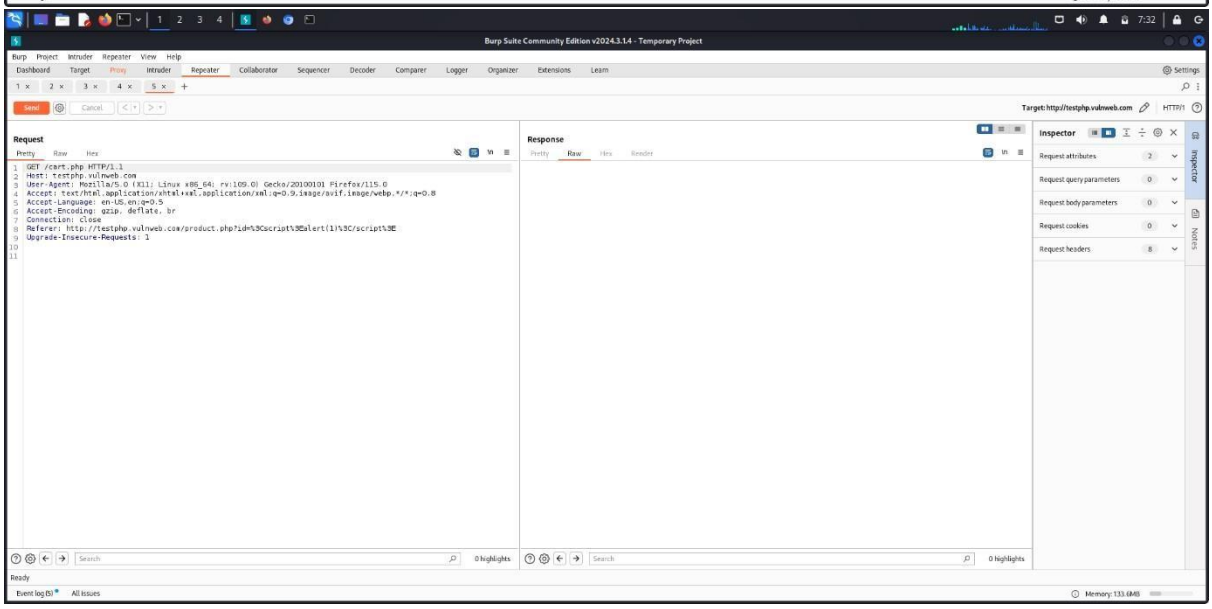
Launched Burpsuite and configured browser to use it as a proxy. Navigated to "testphp.vulnweb.com" and intercept the traffic using Burpsuite.




Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Request to http://testphp.vulnweb.com:80 [44.228.249.3]
Forward
Drop
Intercept is on
Action
Open browser
Pretty
Raw
Hex
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
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Notes
Search
0 highlights
Event log (1)
All issues
Memory: 118.8MB


Burp Suite Community Edition v2024.3.1.4 - Temporary Project
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
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Notes
0 highlights
Memory: 121.2MB


Burp Suite Community Edition v2024.3.1.4 - Temporary Project
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
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers

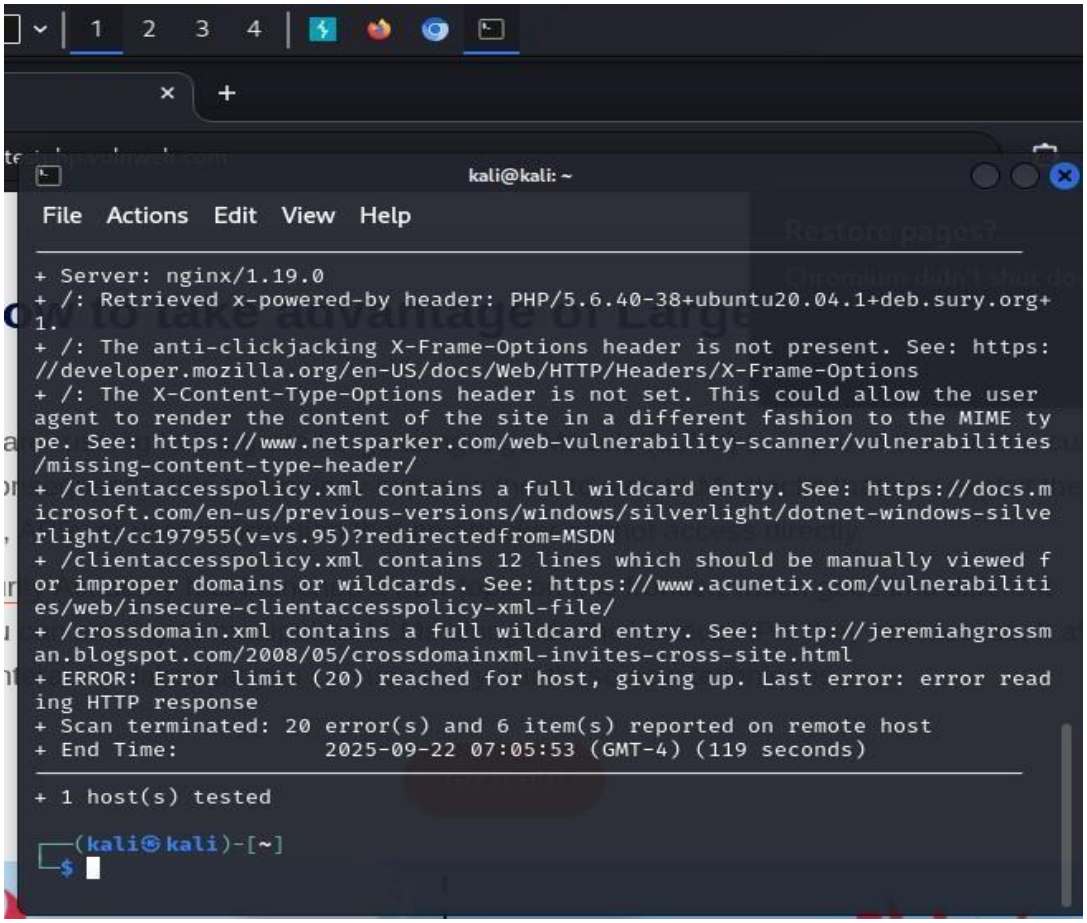

Burp Suite Community Edition v2024.3.1.4 - Temporary Project
Request
GET /cart.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: 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
Response
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers

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 xpowered-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 anticlickjacking XFrame-Options header is not present.	A05: Security Misconfig uration	M e d i u m	Site is vulnerable to clickjacking (UI redress) attacks that can trick users.	Add header X-FrameOptions : DENY or SAMEO RIGIN (nginx: add_he ader X-	Screens hot: Nikto line about X-FrameOptions missing
					FrameOptions "DENY" always;) .	
4	The X-ContentType-Options header is not set.	A05: Security Misconfig uration	M e d i u m	Browser may incorrectly sniff content types — could enable some injection or XSS vectors.	Add header X-Content -TypeOptions : nosniff (nginx add_he ader XContent -TypeOptions "nosniff " always;) .	Screens hot: Nikto line about X-Content -TypeOptions
5	clientaccesspoli cy.xml contains a full wildcard entry	A05 / A06: Security Misconfig uration / Sensitive Data Exposure	M e d i u m	Wildcard crossdomain policy allows any domain to access resources — may expose data to third parties.	Replace wildcar d with explicit trusted domain s or remove the file if not needed.	Screens hot: Nikto lines about clientac cesspoli cy.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/nmap) to gather missing data.	Screenshot: Nikto output showing error limit



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:.