Cyber Security Project – OWASP ZAP Vulnerability Assessment

1. Aim

To perform security testing of a web application using OWASP ZAP tool and identify common vulnerabilities and security misconfigurations.

2. Objectives

- Understand cyber security concepts and CIA Triad
- Learn about attack surface and threats
- Perform automated scan using OWASP ZAP
- Analyze vulnerabilities and suggest fixes

3. Theory

CIA Triad: Confidentiality, Integrity and Availability are the core principles of cyber security. Confidentiality protects data from unauthorized access, Integrity ensures data is not modified illegally, Availability ensures services are accessible to authorized users.

Attack Surface: The total number of entry points where an attacker can try to enter data or extract data from a system such as web apps, APIs, network ports and user inputs.

4. Tools Used

- OWASP ZAP
- Web Browser
- Local web application

5. Steps Performed

1. Installed and launched OWASP ZAP
2. Entered target URL
3. Performed automated scan
4. Reviewed alerts and evidence
5. Generated HTML report

6. Findings

Common vulnerabilities detected:
- Missing X-Frame-Options Header – Risk: Medium
- Cookie without HttpOnly flag – Risk: Low
- Content Security Policy missing – Risk: Medium

7. Recommendations

- Implement security headers
- Use HttpOnly and Secure cookies
- Apply Content Security Policy

8. Conclusion

The assessment helped to understand practical web vulnerabilities and how OWASP ZAP can be used to detect and remediate them.

Vulnerability Assessment Report using OWASP ZAP

This report contains the vulnerability assessment and security analysis of the target web application performed using OWASP ZAP tool. The scan was conducted to identify security weaknesses such as missing security headers, insecure cookies, and misconfigurations. The report includes risk levels, evidence, impact, and recommended remediation steps.

Site: http://testphp.vulnweb.com

Generated on Thu, 15 Jan 2026 16:55:13

ZAP Version: 2.17.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	0
Low	0
Informational	0

Insights

Level	Reason	Site	Description	Statistic
Medium	Exceeded High		Percentage of network failures	56 %
Low	Warning		ZAP errors logged - see the zap.log file for details	12
Low	Warning		ZAP warnings logged - see the zap.log file for details	2,736
Low	Exceeded High	http://testphp.vulnweb.com	Percentage of slow responses	100 %
Info	Informational	http://testphp.vulnweb.com	Percentage of responses with status code 2xx	90 %
Info	Informational	http://testphp.vulnweb.com	Percentage of responses with status code 3xx	3 %
Info	Exceeded Low	http://testphp.vulnweb.com	Percentage of responses with status code 4xx	6 %
Info	Informational	http://testphp.vulnweb.com	Percentage of endpoints with content type application/octet-stream	1 %
Info	Informational	http://testphp.vulnweb.com	Percentage of endpoints with content type application/x-shockwave-flash	1 %

Info	Informational	http://testphp.vulnweb.com	Percentage of endpoints with content type image/gif	2 %
Info	Informational	http://testphp.vulnweb.com	Percentage of endpoints with content type image/jpeg	5 %
Info	Informational	http://testphp.vulnweb.com	Percentage of endpoints with content type image/x-icon	1 %
Info	Informational	http://testphp.vulnweb.com	Percentage of endpoints with content type text/css	3 %
Info	Informational	http://testphp.vulnweb.com	Percentage of endpoints with content type text/html	76 %
Info	Informational	http://testphp.vulnweb.com	Percentage of endpoints with content type text/xml	8 %
Info	Informational	http://testphp.vulnweb.com	Percentage of endpoints with method GET	91 %
Info	Informational	http://testphp.vulnweb.com	Percentage of endpoints with method POST	8 %
Info	Informational	http://testphp.vulnweb.com	Count of total endpoints	85
Info	Informational	https://firefox-settings-attachments.cdn.mozilla.net	Percentage of responses with status code 2xx	100 %
Info	Informational	https://firefox-settings-attachments.cdn.mozilla.net	Percentage of endpoints with content type text/plain	100 %
Info	Informational	https://firefox-settings-attachments.cdn.mozilla.net	Percentage of endpoints with method GET	100 %
Info	Informational	https://firefox-settings-attachments.cdn.mozilla.net	Count of total endpoints	2
Info	Informational	https://firefox-settings-attachments.cdn.mozilla.net	Percentage of slow responses	80 %
Info	Informational	https://firefox.settings.services.mozilla.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://firefox.settings.services.mozilla.com	Percentage of endpoints with content type application/json	100 %
Info	Informational	https://firefox.settings.services.mozilla.com	Percentage of endpoints with method GET	100 %
Info	Informational	https://firefox.settings.services.mozilla.com	Count of total endpoints	1
Info	Informational	https://firefox.settings.services.mozilla.com	Percentage of slow responses	100 %
Info	Informational	https://www.acunetix.com	Percentage of responses with status code 2xx	100 %
Info	Informational	https://www.acunetix.com	Percentage of slow responses	100 %

Summary of Sequences

For each step: result (Pass/Fail) - risk (of highest alert(s) for the step, if any).

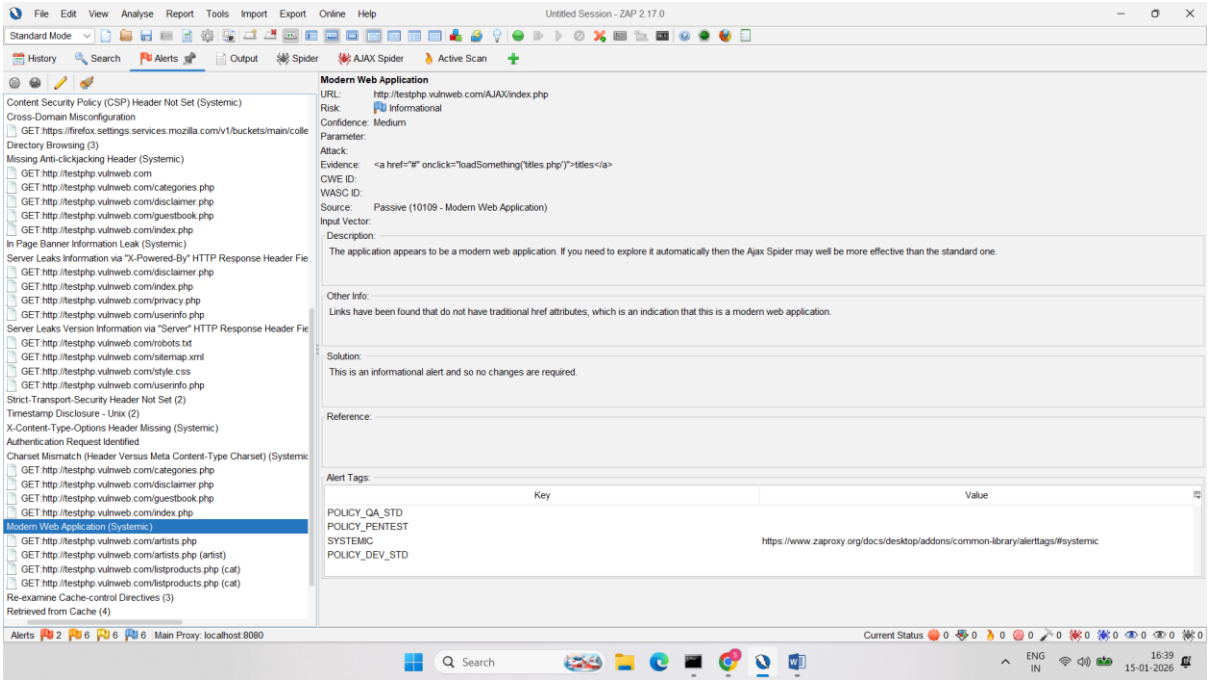
Alerts

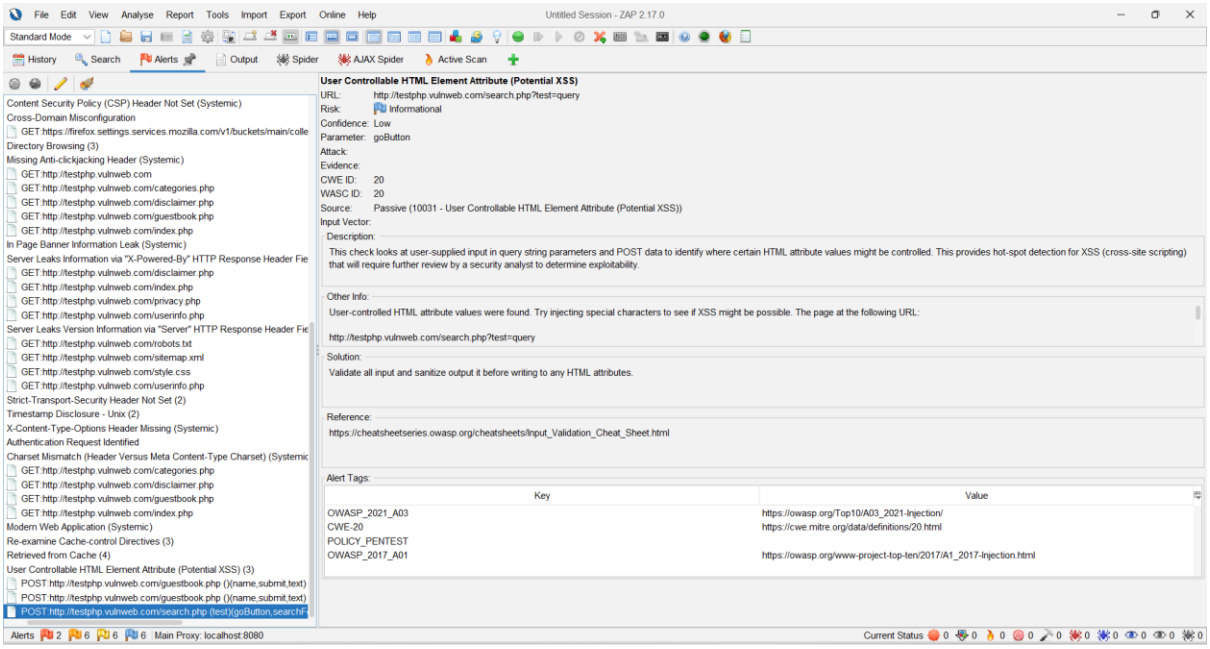
Name	Risk Level	Number of Instances

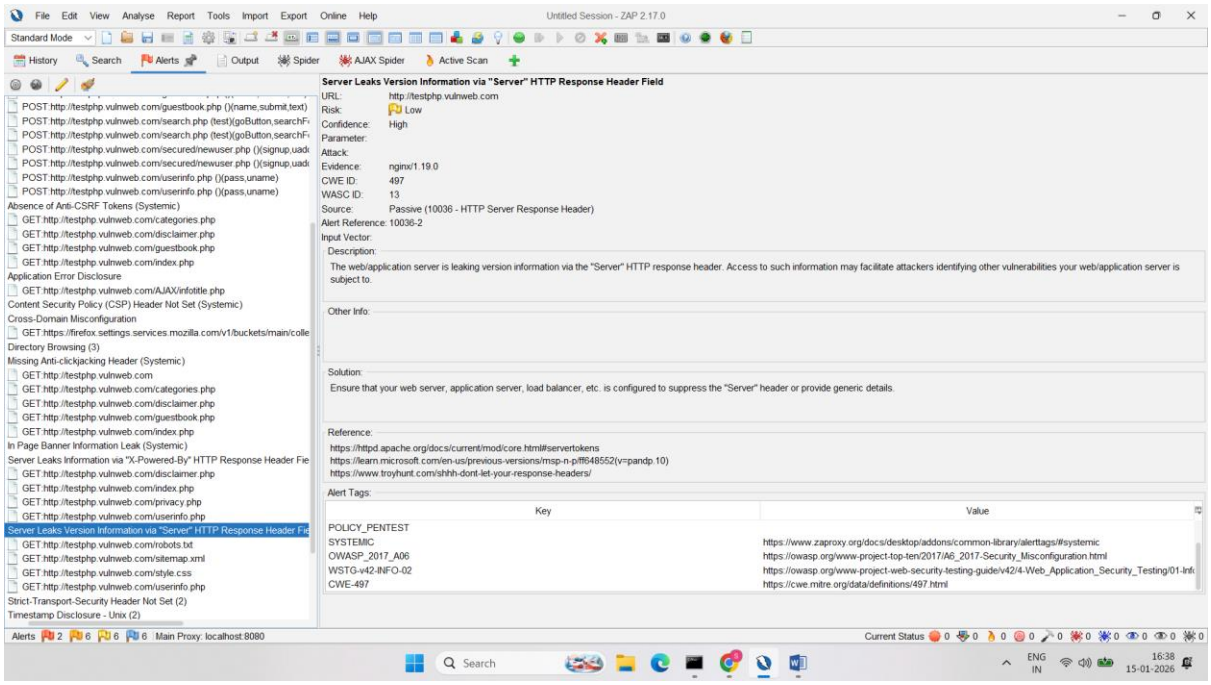
Alert Detail

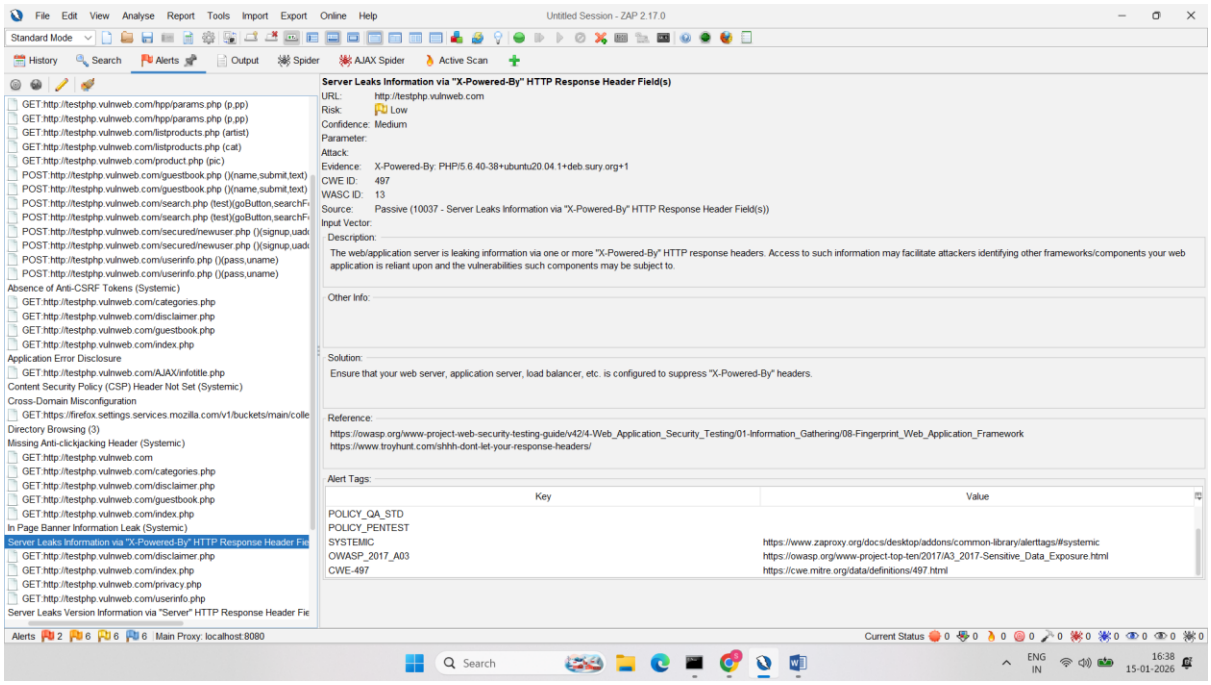
Sequence Details

With the associated active scan results.






File Edit View Analyse Report Tools Import Export Online Help
Untitled Session - ZAP 2.17.0
Standard Mode
History Search Alerts Output Spider AJAX Spider Active Scan
Server Leaks Version Information via "Server" HTTP Response Header Field
URL: http://testphp.vulnweb.com
Risk: Low
Confidence: High
Parameter:
Attack:
Evidence: nginx/1.19.0
CWE ID: 497
WASC ID: 13
Source: Passive (10036 - HTTP Server Response Header)
Alert Reference: 10036-2
Input Vector:
Description:
The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
Other Info:
Solution:
Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference:
https://httpd.apache.org/docs/current/mod/core.html#servertokens
https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)
https://www.troyhunt.com/shhh-dont-let-your-response-headers/
Alert Tags:
Key Value
POLICY_PENTEST
SYSTEMIC https://www.zaproxy.org/docs/desktop/addons/common-library/alerttags/#systemic
OWASP_2017_A06 https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html
WSTG-v42-INFO-02 https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Inf
CWE-497 https://cwe.mitre.org/data/definitions/497.html
Alerts 2 6 6 6 Main Proxy: localhost:8080
Current Status
Search
ENG IN
16:38 15-01-2026


File Edit View Analyse Report Tools Import Export Online Help
Untitled Session - ZAP 2.17.0
Standard Mode
History Search Alerts Output Spider AJAX Spider Active Scan
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
URL: http://testphp.vulnweb.com
Risk: Low
Confidence: Medium
Parameter:
Attack:
Evidence: X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
CWE ID: 497
WASC ID: 13
Source: Passive (10037 - Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))
Input Vector:
Description:
The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Other Info:
Solution:
Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference:
https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework
https://www.troyhunt.com/shhh-dont-let-your-response-headers/
Alert Tags:
Key Value
POLICY_QA_STD
POLICY_PENTEST
SYSTEMIC https://www.zaproxy.org/docs/desktop/addons/common-library/alerttags/#systemic
OWASP_2017_A03 https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html
CWE-497 https://cwe.mitre.org/data/definitions/497.html
Alerts 2 6 6 6 Main Proxy: localhost:8080
Current Status
Search
ENG IN
16:38 15-01-2026