REPORT

VULNERABILITY ASSESSMENT REPORT

Title: Vulnerability Assessment of Web Application

Submitted By: P RENUGA

Course: Cyber Security Lab

EXECUTIVE SUMMARY

This report presents the results of a vulnerability assessment conducted on a publicly available test website. The objective of this assessment was to identify potential security vulnerabilities using ethical and non-intrusive testing techniques. Various security testing tools and manual inspection methods were used to analyze the target system. The assessment identified multiple security weaknesses that may expose the system to cyber threats. Recommendations have been provided to mitigate these risks and improve overall security.

SCOPE OF ASSESSMENT

The scope of this assessment includes the analysis of a publicly accessible web application. The testing was limited to passive and non-intrusive methods.
Target Website:http:testphp.vulnweb.com
Assessment Type: Vulnerability Assessment
Testing Method: Ethical and non-intrusive

T

METHODOLOGY

The vulnerability assessment was conducted using the following approach:
Network reconnaissance was performed to identify open ports and services running on the target system.
Automated vulnerability scanning was conducted to detect security misconfigurations and common web vulnerabilities.
Manual inspection was performed using browser developer tools to analyze cookies, HTTPS configuration, and network requests

Tools Used

Network scanning tool for port and service detection
Automated vulnerability scanner for identifying security risks
Browser developer tools for manual security analysis

FINDING 1: MISSING SECURE COOKIE FLAG

DESCRIPTION:

COOKIES WERE FOUND WITHOUT THE SECURE ATTRIBUTE.

RISK LEVEL: HIGH

IMPACT:

ATTACKERS MAY INTERCEPT SESSION COOKIES OVER UNSECURED NETWORKS, LEADING TO SESSION HIJACKING.

RECOMMENDATION:

ENABLE SECURE AND HTTPONLY FLAGS FOR ALL COOKIES.

FINDING 2: MIXED CONTENT VULNERABILITY

DESCRIPTION:

THE WEBSITE LOADS SOME RESOURCES USING HTTP INSTEAD OF HTTPS.

RISK LEVEL: MEDIUM

IMPACT:

DATA TRANSMITTED MAY BE INTERCEPTED OR MODIFIED BY ATTACKERS.

RECOMMENDATION:

ENSURE ALL WEBSITE RESOURCES ARE LOADED THROUGH HTTPS.

FINDING 3: MISSING SECURITY HEADERS

DESCRIPTION:

THE APPLICATION LACKS ESSENTIAL SECURITY HEADERS.

RISK LEVEL: MEDIUM

IMPACT:

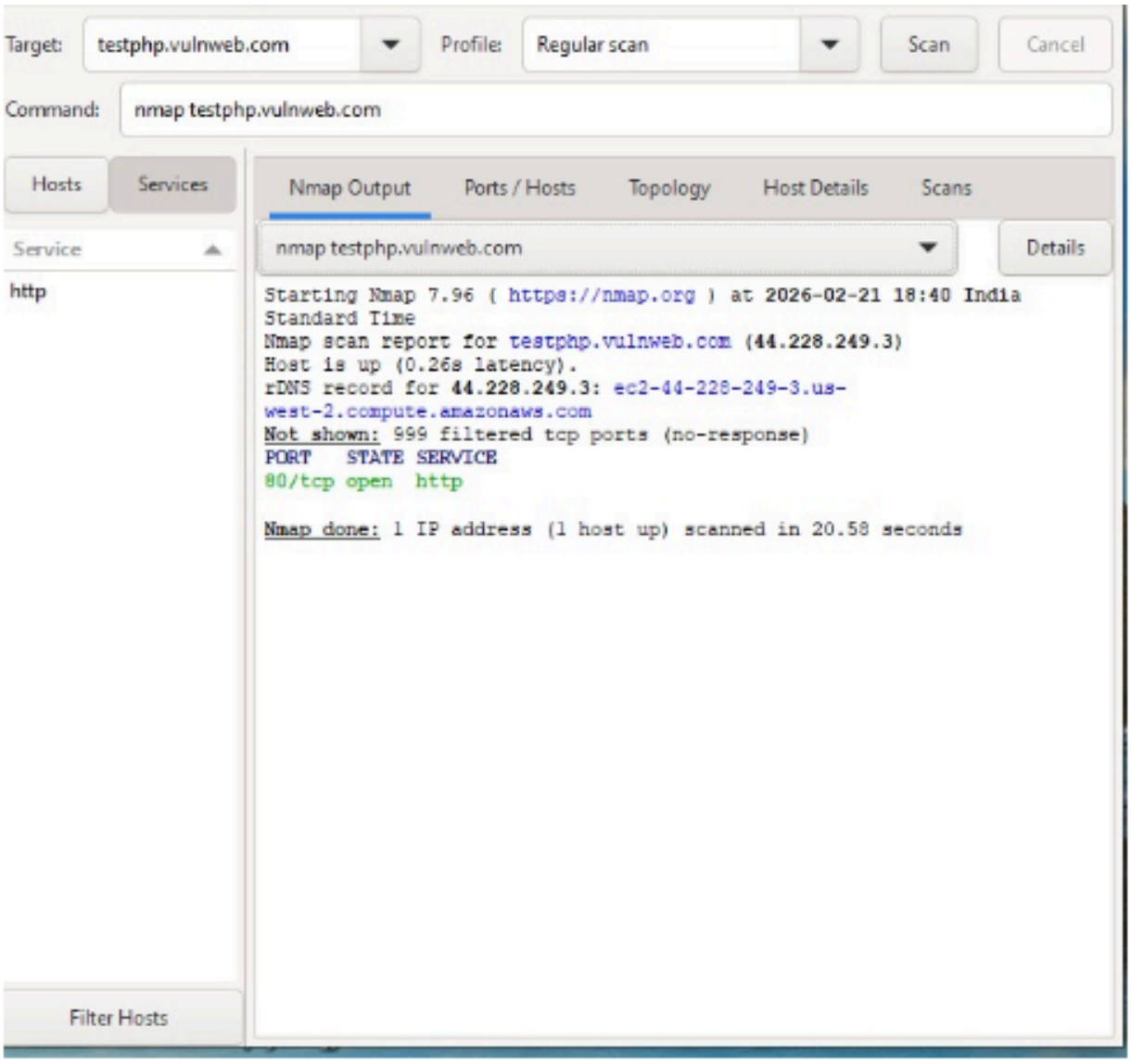
THIS MAY EXPOSE THE SYSTEM TO CLICKJACKING AND CROSS-SITE SCRIPTING ATTACKS.

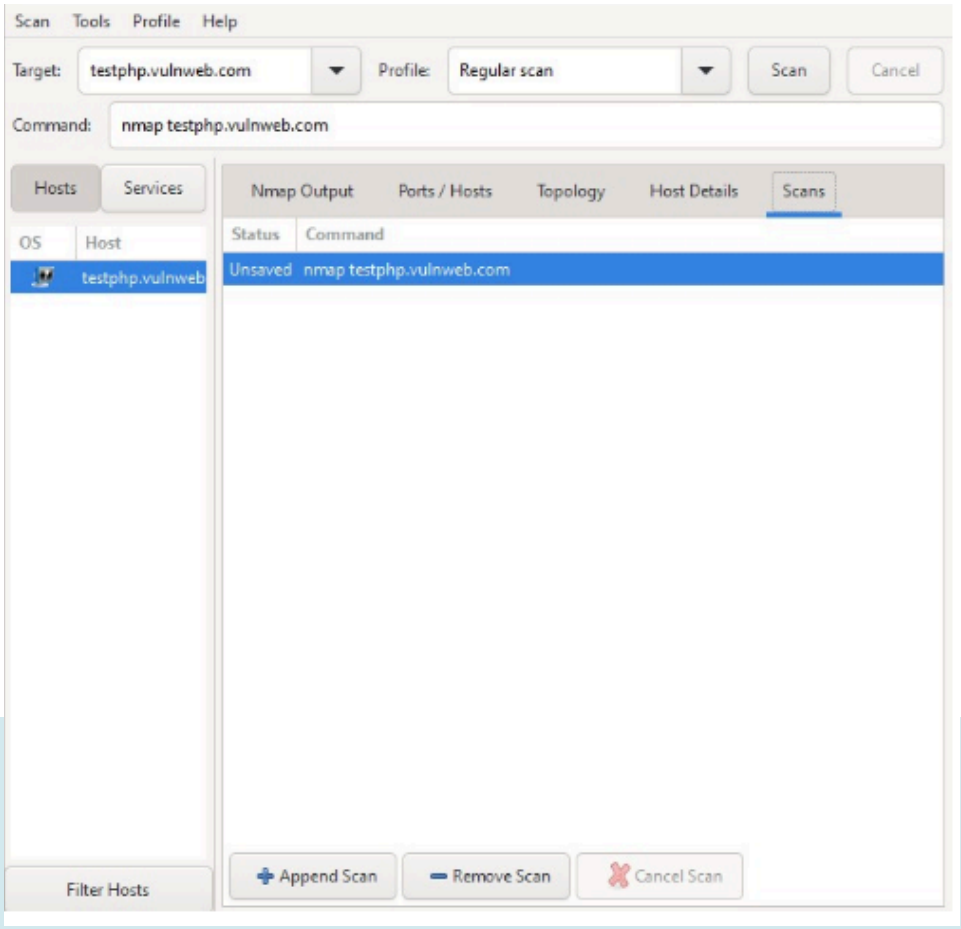
RECOMMENDATION:

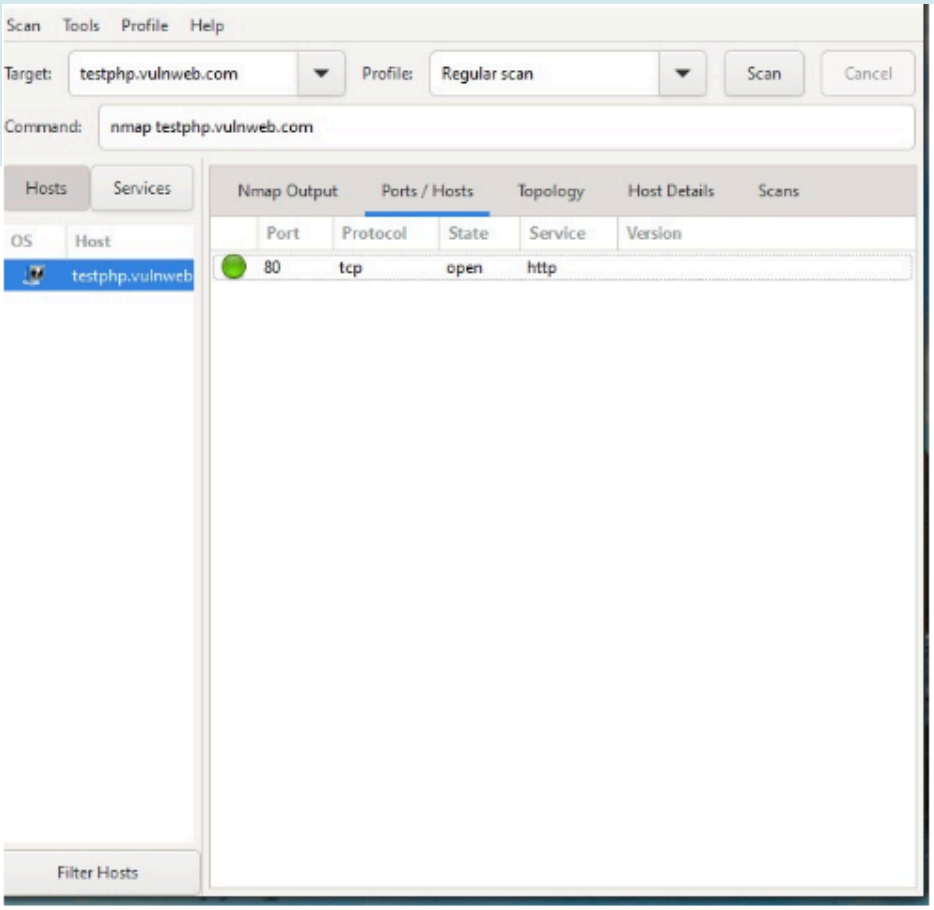
IMPLEMENT NECESSARY SECURITY HEADERS SUCH AS X-FRAME-OPTIONS AND CONTENT SECURITY POLICY.

TOOL: NMAP

OPEN PORT(80,ETC)
SERVICE VERSION
OUTDATED VERSION

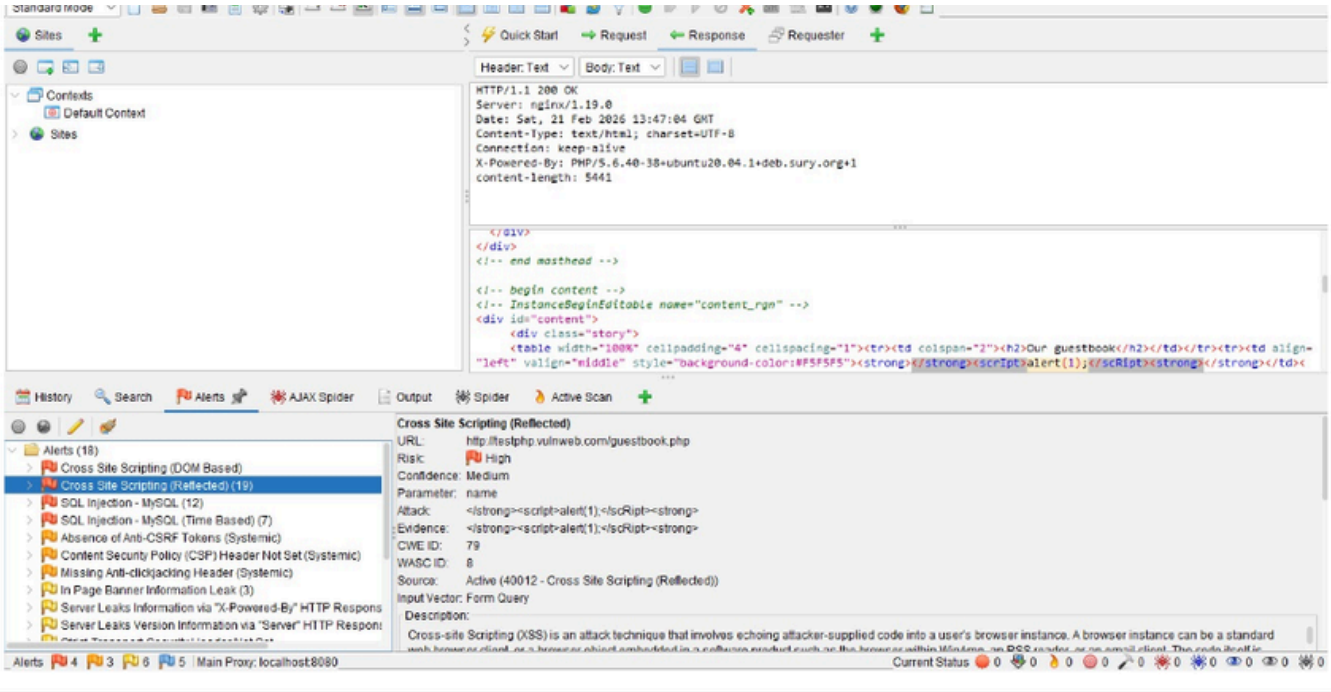


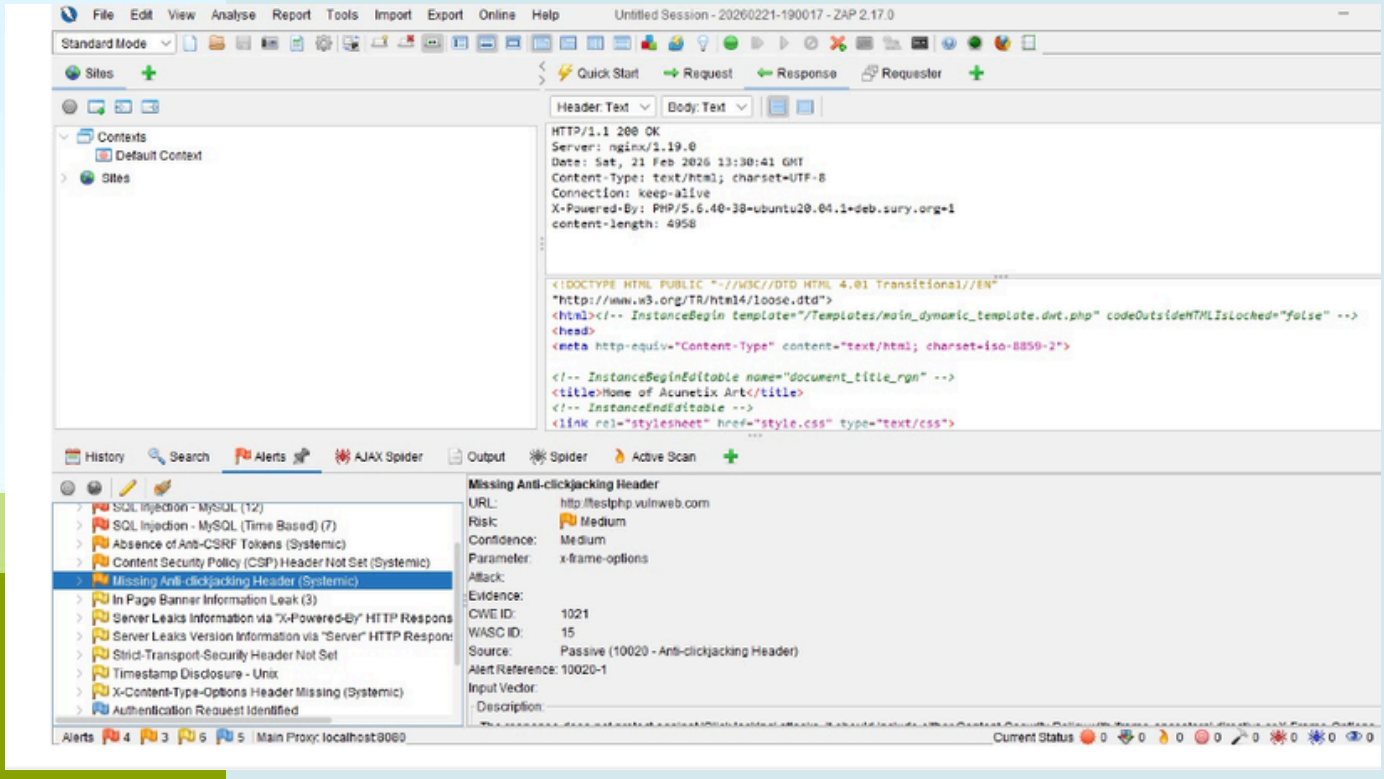

Scan Tools Profile Help
Target: testphp.vulnweb.com
Profile: Regular scan
Scan
Cancel
Command: nmap testphp.vulnweb.com
Hosts
Services
OS
Host
testphp.vulnweb
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Status
Command
Unsaved
nmap testphp.vulnweb.com
Append Scan
Remove Scan
Cancel Scan
Filter Hosts

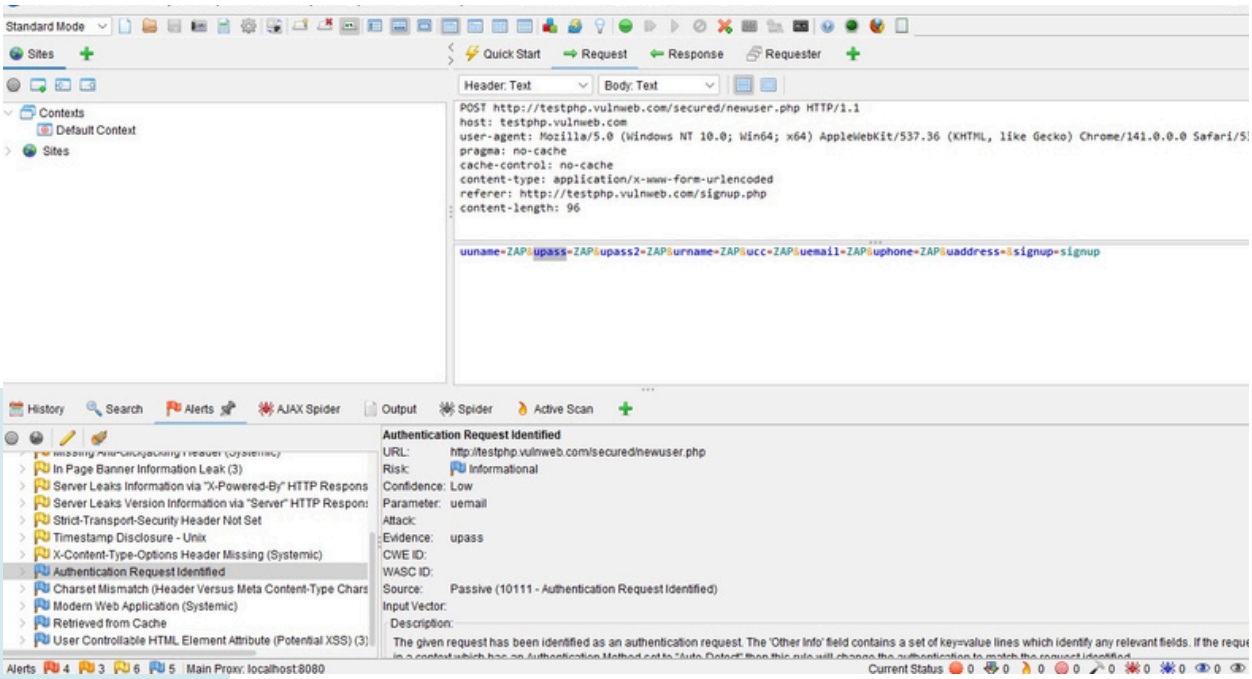

Scan Tools Profile Help
Target: testphp.vulnweb.com
Profile: Regular scan
Scan
Cancel
Command: nmap testphp.vulnweb.com
Hosts
Services
OS
Host
testphp.vulnweb
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Port
Protocol
State
Service
Version
80
tcp
open
http
Filter Hosts

TOOL:OWASP ZAP

DIRECTORY BROWER
MISSING HEADER
ZSS VULNARABILITY
COOKIES ISSUES
MIXED CONTENT

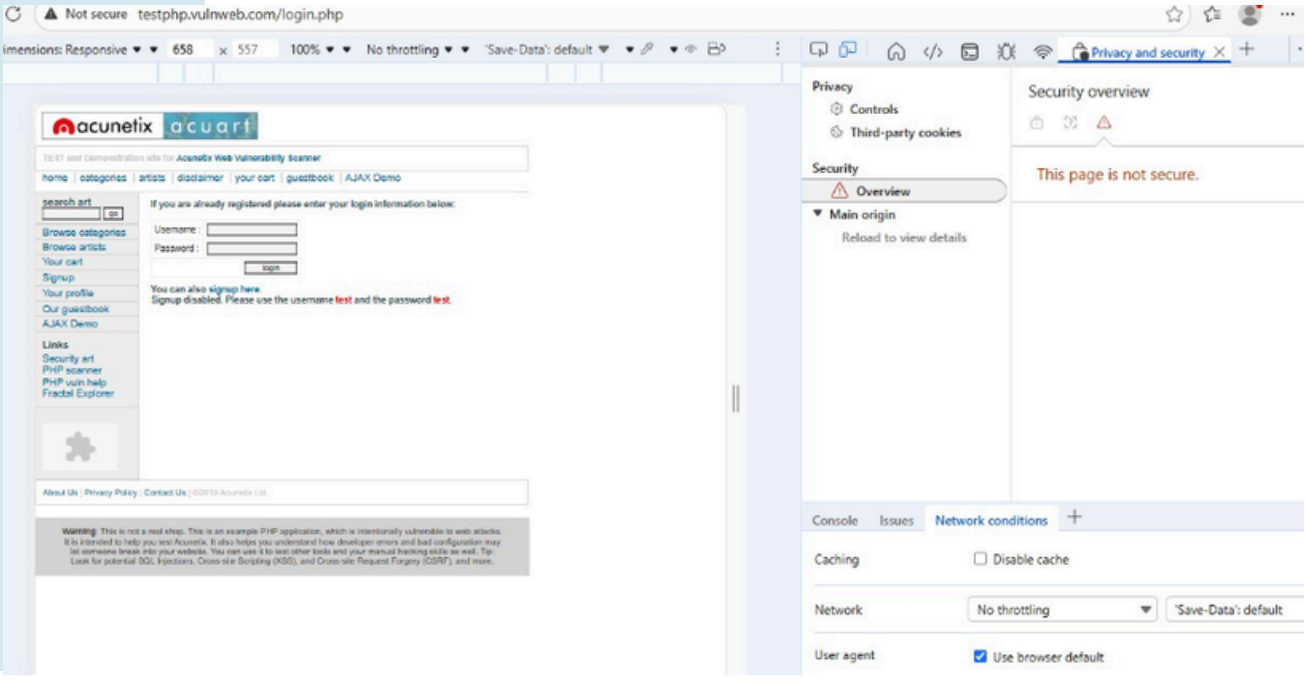


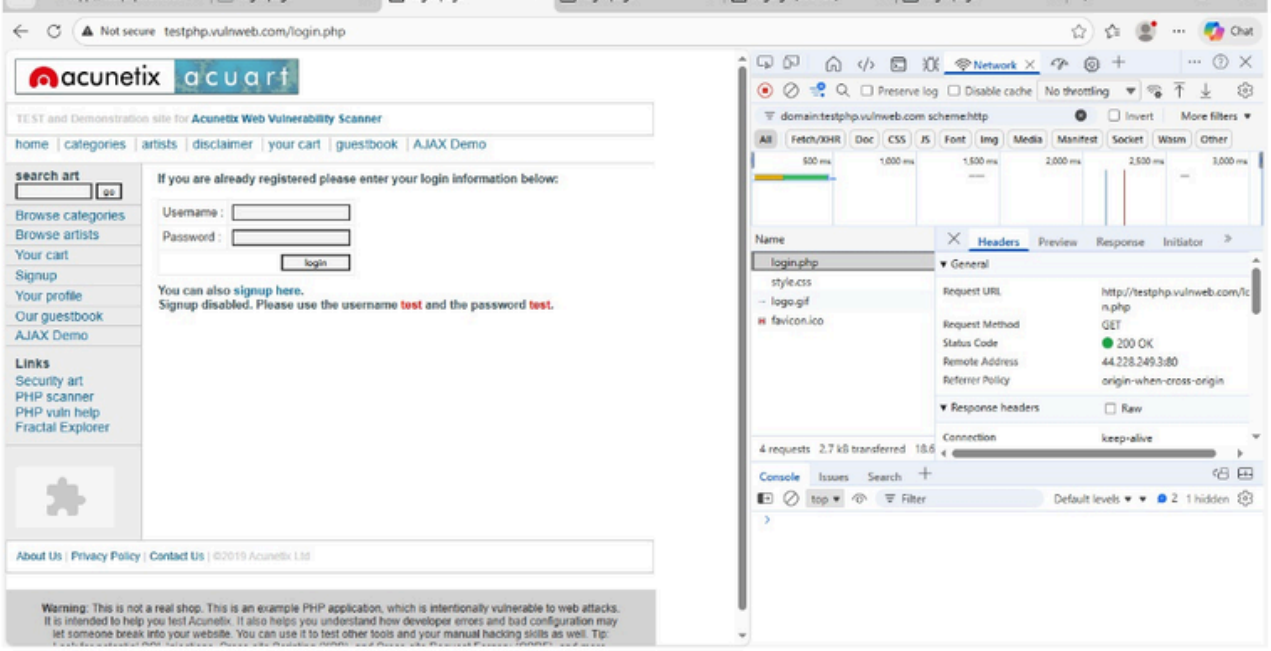


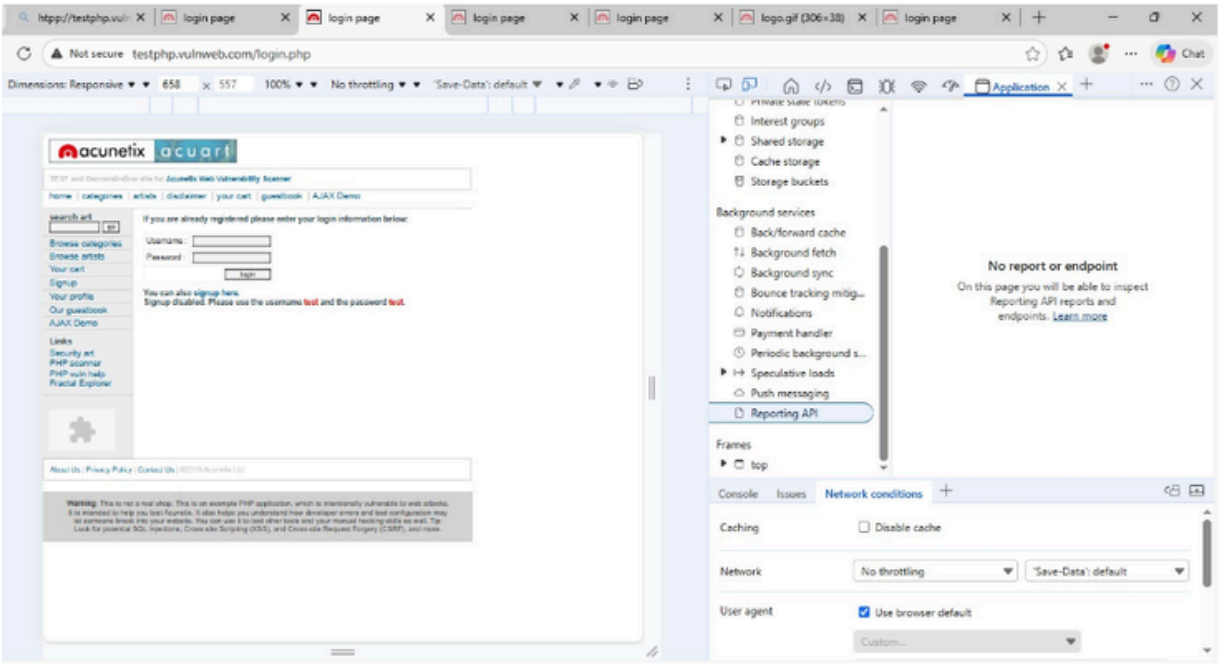


TOOL:BROWSER DEVTOOLS CHECK

- SECURITY TAB
  - SECURE OR NOT
- NETWORK TAB
  - REQUEST URL
  - HEADER
- APPLICATION
  - COOKIE
  - HTTP ONLY ENABLE







RISK CLASSIFICATION

Risk Level
Description
High
Can lead to major security breaches
Medium
May allow limited system exploitation
Low
Minor security weaknesses

Remediation Plan

To improve the overall security posture, the following measures are recommended:
Implement secure cookie configurations
Enforce HTTPS across all web resources
Enable essential security headers
Regularly update software and server component
Avoid storing sensitive data in client-side storage

Conclusion

The vulnerability assessment identified several security weaknesses in the target web application. Although no critical system compromise was observed, the presence of misconfigurations increases the risk of cyber attacks. Implementing the recommended mitigation strategies will significantly enhance the security of the system.

References

Security testing best practices

Web application security guidelines

Vulnerability assessment methodologies