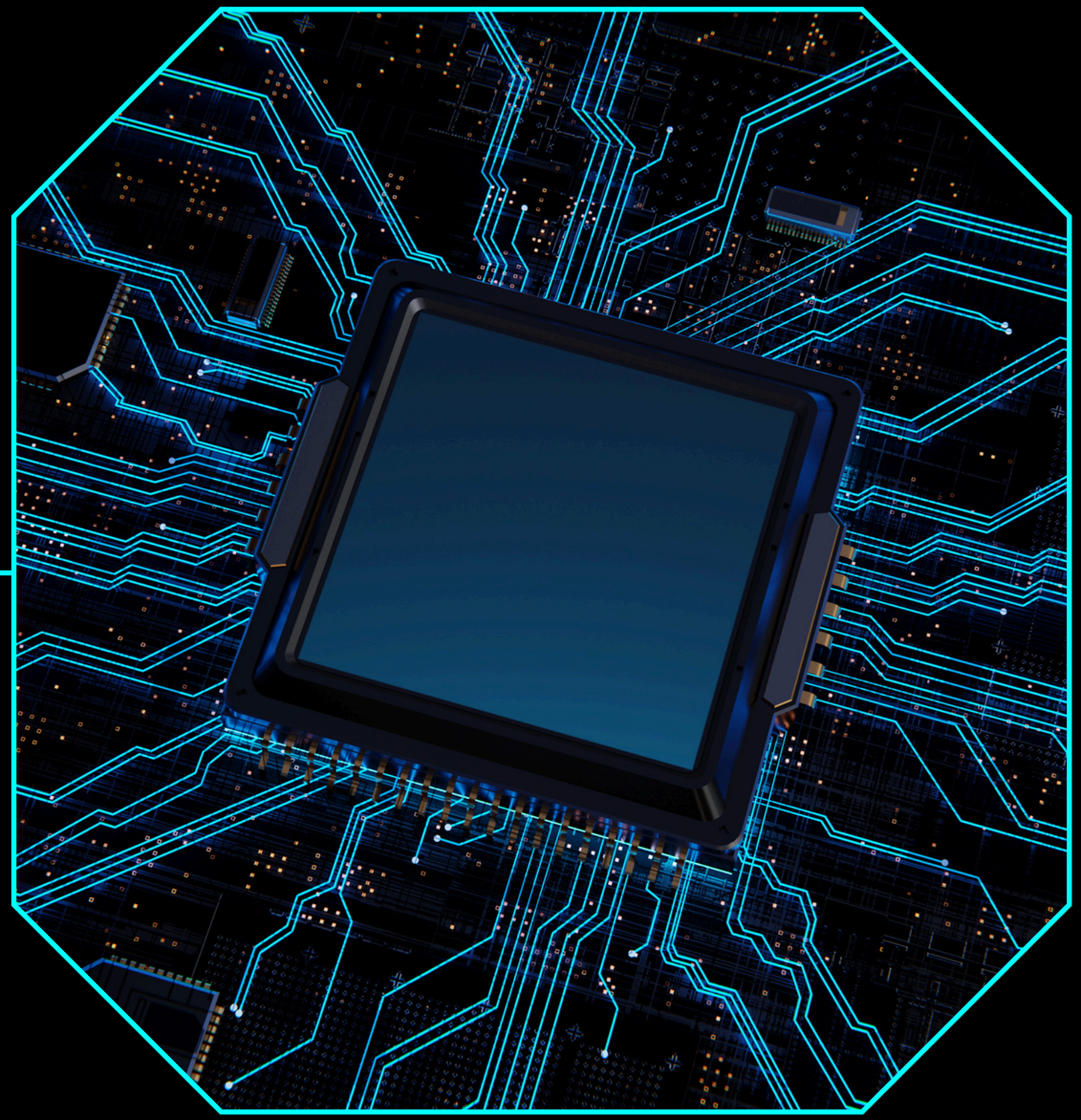
CYBER SECURITY

VULNERABILITY ASSESSMENT REPORT

LIVE WEBSITE SECURITY ANALYSIS

- Prepared by: Jatin Malik
- Internship: Cyber Security – Future Interns
- Target Website: testphp.vulnweb.com
- Tools: Nmap, OWASP ZAP, Browser DevTools
- Date: (8 feb 2026)



EXECUTIVE SUMMARY

This vulnerability assessment was conducted on an intentionally vulnerable live website to identify common web security weaknesses.

Passive scanning techniques were used to ensure no harm was caused to the target application. Multiple vulnerabilities related to insecure communication, missing security headers, and information disclosure were identified.

This report highlights the risks, business impact, and recommended remediation steps in simple and clear language

SCOPE & METHODOLOGY

- Target: http://testphp.vulnweb.com
- Testing type: Passive security assessment

Methodology

- Network reconnaissance using Nmap
- Passive vulnerability scanning using OWASP ZAP
- Client-side inspection using browser developer tools
- No exploitation or active attacks performed

TOOLS USED

- Nmap: Identified open ports and running services
- OWASP ZAP (Passive): Detected web vulnerabilities
- Browser DevTools: Analyzed cookies and requests
- Canva: Designed professional report

VULNERABILITY 1
NO HTTPS:

DESCRIPTION:

The website uses HTTP instead of HTTPS, causing data to be transmitted in plain text.

Impact:
Attackers can intercept sensitive information using Man-in-the-Middle attacks.

Remediation:

- Implement SSL/TLS certificate
- Force HTTPS redirection

RISK LEVEL: 🔴 HIGH

Vulnerability 2

Missing Security Headers

Description:

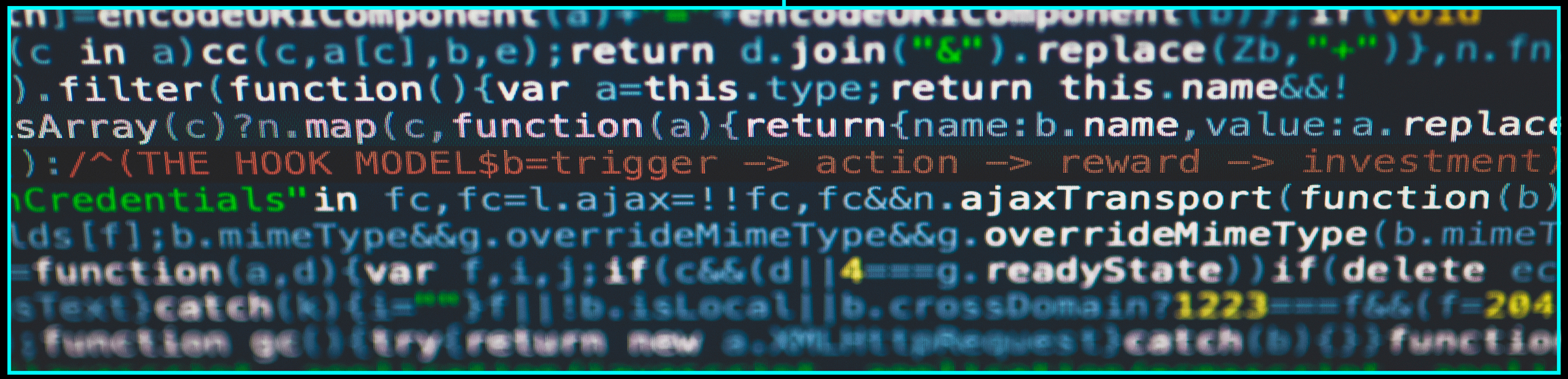
Important HTTP security headers are missing from server responses.

Impact:
Increases exposure to clickjacking and cross-site scripting attacks.

Remediation:
Add:
X-Frame-Options

- Content-Security-Policy
- X-Content-Type-Options

Risk Level: Medium



VULNERABILITY 3 COOKIES WITHOUT HTTPONLY FLAG

DESCRIPTION:

Cookies can be accessed via JavaScript due to missing HttpOnly flag.

Impact:
Session hijacking possible if XSS attack occurs.

Remediation:

- Enable HttpOnly and Secure flags on cookies

Risk Level: Medium

VULNERABILITY 4 INFORMATION DISCLOSURE

DESCRIPTION:

Server reveals Apache server details.

Impact:
Helps attackers identify known vulnerabilities.

Remediation:

- Disable server version disclosure

Risk Level: Low

Overall Risk Assessment

The application demonstrates weak security configurations. While suitable for testing purposes, similar issues in real-world applications could lead to serious security breaches.

Immediate security hardening is recommended

Conclusion & Recommendations

- Enforce HTTPS
- Implement security headers
- Harden server configurations
- Perform regular security assessments

Disclaimer

This assessment was performed on an intentionally vulnerable website for educational purposes only.

No real systems, organizations, or user data were targeted or harmed