Vulnerability Assessment & Penetration Testing (VAPT) Report

Client Info

Client Type: Startup Web Application (NDA-protected)

Analyst: Kaushal Kumar

Date: April 2024

Tools Used: Burp Suite, Nmap, OWASP ZAP, Nikto, WhatWeb, Dirb

Standards Followed: OWASP Top 10, CVSS v3.1

1. Reconnaissance

- Identified subdomains, robots.txt, sitemap.xml using tools like whatweb, gobuster, nmap.

- Collected HTTP headers and performed server fingerprinting.

2. Vulnerabilities Found

1. Reflected XSS - Medium - CWE-79

2. SQL Injection (Login) - High - CWE-89

3. IDOR - High - CWE-639

4. Clickjacking - Low - CWE-1021

3. Technical Details & Evidence

3.1 Reflected XSS

Endpoint: /search?q=

Payload: <script>alert('Kaushal')</script>

Screenshot: (Not Included)

4. Recommendations

- XSS: Use output encoding and input sanitization

- SQLi: Use parameterized queries

- IDOR: Add access controls

- Clickjacking: Add X-Frame-Options: DENY header

Vulnerability Assessment & Penetration Testing (VAPT) Report

5. Summary

Total Vulnerabilities: 4

High Severity: 2

Medium: 1

Low: 1

6. Scope & Limitations

Scope:

- Web application hosted at https://example.com
- Login, search, and profile modules
- No brute-force, DDoS, or social engineering tests were conducted

Limitations:

- Black-box testing only (no source code access)
- No permission for production database interaction
- Testing was time-boxed to 7 days

7. Risk Rating Matrix

Severity	Risk Score	Description
High	7.0-10	Critical impact and high likelihood
Medium	4.0-6.9	Moderate impact or likelihood
Low	0.1-3.9	Low impact and low likelihood

8. Methodology Followed

1. Reconnaissance

2. Vulnerability Scanning

3. Manual Validation

4. Exploitation (Ethical & Safe)

5. Reporting & Remediation Suggestion

6. Final Review

9. Tools & Versions

- Burp Suite Community v2024.3

- OWASP ZAP v2.14

- Nmap v7.94

- Nikto v2.5.0

- WhatWeb v0.5.5

- Linux (Kali Rolling 2024.1)

About the Analyst

Kaushal Kumar

Freelance Web Security Analyst | VAPT | TryHackMe | OWASP

Email: kaushalkumar9578@gmail.com

LinkedIn | GitHub