VAPT Report

Client : [redacted]

Engagement Period : 15 March 2024 – 28 March 2024

Prepared by: Shoumik Chandra – Cybersecurity Consultant

Table of Contents :

1. Assessment Overview

The assessment was conducted to evaluate the security posture of [redacted] network and web assets. This included external-facing infrastructure and critical web applications that handle customer data.

2. Finding Severity Ratings

Severity	Definition
Critical	Immediate exploitation possible
High	Easily exploitable with significant impact
Moderate	Requires user interaction or specific context
Low	Limited impact or hard to exploit
Informational	No direct risk but useful for recon

3. Risk Factor

A. Likelihood

Likelihood is determined by the ease of exploitation, availability of tools, and attacker motivation.

B. Impact

Impact assesses data exposure, service downtime, privilege escalation, or financial loss.

4. Scope

- 2 Web Applications (main portal + admin dashboard)
- 5 Subdomains
- External Network (13 IPs)

5. Scope Exclusion

- Internal network
- Mobile applications
- Third-party integrations (e.g., payment gateways)

6. Client Allowances

- Permission for intrusive testing
- Temporary admin access for login-based tests
- Testing window: 12 AM – 6 AM GMT

7. Executive Summary

A. Testing Summary

The engagement identified a total of 6 vulnerabilities:

- 1 Critical
- 1 High
- 1 Moderate
- 2 Low
- 1 Informational

No unauthorized access was achieved, but serious misconfigurations and outdated software were found.

8. Security Strength

- ✅ SIEM triggered alerts on vulnerability scans
- ✅ MFA enabled for all admin access
- ✅ Password policy enforces 12+ characters with complexity

9. Security Weakness

- ❌ Session fixation vulnerability in login endpoint
- ❌ Potential for Denial of Service via improperly limited API calls
- ❌ Insecure direct object references (IDOR) in ticketing module

10. Vulnerability Summary and Report Card

A. Network Penetration Test

Severity	Count
Critical	1
High	1
Moderate	0
Low	0
Informational	0

Grade: C

B. Web Application Penetration Test

Severity	Count
Critical	0
High	0
Moderate	1
Low	2
Informational	1

Grade: A

11. Technical Findings

A. Network Penetration Test Findings

Finding #1: Outdated OpenSSH Version (Critical)

- **Risk**: Known remote code execution vulnerability
- **System**: [redacted]
- **Tools Used**: Nmap, Nessus
- **References**: CVE-2023-25136
- **Evidence**:

```
[redacted]
```

Remediation: Upgrade OpenSSH to the latest stable version

Finding #2: Default Credentials on Web Admin Panel (High)

- **Risk**: Allows unauthorized access
- **System**: [redacted]
- **Tools Used**: Hydra, manual login
- **Evidence**:

  [redacted]

Remediation: Change all default credentials and restrict admin access

B. Web Application Penetration Test Findings

Finding #1: Reflected Cross-Site Scripting (XSS) (Moderate)

- **Risk**: Can be used to steal cookies or redirect users
- **System**: [redacted]
- **Tools Used**: Burp Suite, manual testing
- **References**: OWASP XSS Guide
- **Evidence**:

  [redacted]

Remediation: Use context-aware output encoding and input validation

Finding #2: Clickjacking Vulnerability (Low)

- **Risk**: Tricking users into clicking hidden UI elements
- **System**: [redacted]
- **Tools Used**: Burp Suite, Clickjacking PoC
- **References**: OWASP Clickjacking Guide
- **Evidence**:

```
[redacted]
```

Remediation: Set `X-Frame-Options: DENY` or use Content-Security-Policy

Finding #3: Server Version Disclosure (Informational)

- **Risk**: Exposes software versions, aiding recon
- **System**: [redacted]
- **Tools Used**: Nikto, curl
- **References**: General Reconnaissance Best Practices
- **Evidence**:

```
[redacted]
```

Remediation: Hide or obfuscate server version in headers

Finding #4: Sensitive Data in URL (Low)

- **Risk**: Can be stored in browser history or logs
- **System**: [redacted]
- **Tools Used**: Manual inspection
- **References**: OWASP A01 – Broken Access Control
- **Evidence**:

  ```
  [redacted]
  ```

Remediation: Use POST method for sensitive actions

12. Conclusion

The Vulnerability Assessment and Penetration Testing (VAPT) conducted for the target organization revealed a mix of strengths and areas that require immediate attention.

Remediation of the vulnerabilities found should be prioritized based on the severity ratings provided in this report. Additionally, implementing regular security testing, secure development practices, and security awareness training will help reduce the overall risk posture in the long term.

It is recommended that the organization adopt a proactive security strategy involving continuous monitoring, regular audits, and security compliance reviews to ensure resilience against evolving cyber threats.