Vulnerability Assessment and Penetration Testing (VAPT) Report

Organization: TechSecure Corp
Assessed by: [Your Name]
Date: June 2025

---

1. Executive Summary

This report outlines the findings from a comprehensive VAPT of TechSecure Corp's internal network and OWASP Juice Shop application. Key vulnerabilities and recommended mitigations are provided.

---

2. Network Assessment Summary

Tools Used: Nmap, Recon-ng, Amass

IP Address	OS Guess	Open Ports & Services
192.168.1.10	Linux (Ubuntu)	22 (SSH), 80 (HTTP)
192.168.1.15	Windows Server	139, 445 (SMB), 3389 (RDP)

---

3. Web Application Assessment Summary

Target: OWASP Juice Shop
Tools Used: OWASP ZAP

Vulnerability	Risk Level	Description	PoC
SQL Injection	High	Found in `/rest/user/login`	`' OR '1'='1`
Stored XSS	High	Found in `/#/contact` feedback form	`<script>alert(1)</script>`
Insecure Direct Object Reference	Medium	Orders API allows ID enumeration	`/api/Orders/3`

---

4. Recommendations

- Sanitize inputs and use parameterized queries (SQLi)
- Encode all user-generated outputs (XSS)
- Implement access control checks (IDOR)
- Patch outdated services (SSH, SMB)

---

5. Conclusion

Immediate remediation of high-risk vulnerabilities is advised. Ongoing monitoring and regular testing

should be incorporated into the organization’s DevSecOps cycle.

[End of Report]