BS3944: Penetration Testing

Written Report

Figure 1: Illustration of penetration testing concepts (Evalian®, 2024).

Table of Contents

Platform Overview

The company’s new jewellery website caters to affluent customers seeking exclusivity and elegance. With high-value transactions at its core, robust security is vital. Any breach could compromise sensitive financial data and harm the brand's premium reputation. To maintain customer trust, protect the brand, and ensure secure interactions, it is crucial to address risks like unauthorized access and data breaches.

Threat Analysis

Potential Hazards and Limitation

Unauthorised access to administrative controls or customer accounts may be made possible via weak authentication. Data breaches could harm the jewellery brand's reputation by disclosing financial details, particularly during high-value purchases. Web vulnerabilities like CSRF, XSS, and SQL Injection may allow for the theft or modification of customisation data and compromise client data (Sharma, 2022). Attacks using lateral movement may take advantage of hacked devices or incorrectly configured servers. Over-reliance on outside services leads to risks, such as payment gateway abuse and supply chain breaches. Operations could be disrupted by ransomware or malware. Addressing these issues is essential to protecting the platform's security and preserving the confidence of its valuable customers.

Risk Evaluation and Impacts

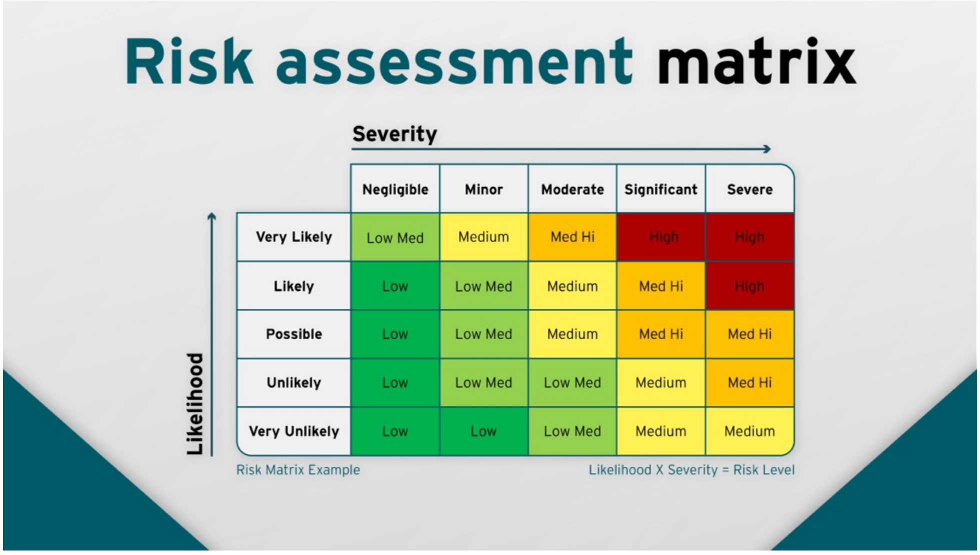
To facilitate risk assessment, a structured risk matrix takes impact and likelihood into account.

1. High-Probability Risks: With insufficient input validation, web vulnerabilities such as XSS present a moderate to high risk of exposing client data.

2. Moderate-Probability Risks: Unauthorised access to the Linux server could be made possible by inadequate network segmentation.

3. Low-Probability, High-Impact Risks: Windows or Linux zero-day vulnerabilities have the potential to result in serious security breaches or system failures

These risks could lead to financial losses, reputational harm undermining customer trust, and operations being disrupted by ransomware or DDoS attacks.



Risk assessment matrix

Severity

Likelihood

	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

Risk Matrix Example

Likelihood X Severity = Risk Level

Figure 2: Risk Assessment Matrix from RiskPal (2023), demonstrating the categorization of risk likelihood and severity.

Cyber Attack Scenarios

These vulnerabilities are brought to light by particular attack scenarios. A hacker might be able to obtain confidential client information, such as payment information and tailored orders, through SQL Injection. The Linux server may be vulnerable to additional intrusions due to a network reconnaissance assault (Kinger et al., 2023). DDoS assaults could overload the server, resulting in outages and damaging the reputation of the brand. The platform should use multi-factor authentication for access control, network segmentation to stop lateral movement, AES-256 encryption for data, TLS for secure transit, and real-time monitoring using IDS/SIEM tools to swiftly identify and address possible threats to reduce risks (*SentinelOne,* 2024).

Penetration Testing Report

Overview of Testing Phases

The jewellery company's e-commerce platform underwent a thorough penetration test to guarantee the site's security for wealthy customers. Reconnaissance, vulnerability analysis, password evaluation, and exploitation were the four main stages of the test. To evaluate the site's defences and recommend security enhancements, each step identified serious vulnerabilities that might compromise the platform's integrity and private user information.

Reconnaissance

Securing the company's new jewellery website, which serves affluent customers making high-value transactions, was the goal of the reconnaissance phase. Tools were used to detect possible risks, like illegal access, in order to protect private financial data and preserve the brand's high-end reputation. To find active hosts, open ports, and services within the IP range 192.168.64.0/24, Nmap used TCP SYN scans and service fingerprinting. Dmitry used IP and Whois lookups to obtain network ownership information. In order to identify active hosts and MAC addresses and identify vulnerabilities that needed to be fixed, Netdiscover used ARP-based discovery. In order to resolve hostnames and further evaluate hazards, Recon-ng also carried out reverse DNS lookups (Sankar, 2017).

Vulnerability Analysis

The vulnerability scanning phase's main focus was the jewellery website, which handles expensive transactions. Nikto found serious vulnerabilities that seriously jeopardised sensitive data, such as an out-of-date Apache server, exposed phpMyAdmin, and enabled TRACE techniques. Data breaches are far more likely now that OpenVAS has identified high-severity vulnerabilities including default credentials, RCE exploits, and backdoors across many services (Vaishnavi, 2024). The platform was further compromised when OWASP ZAP discovered security flaws like route traversal, MD5 hash leaking, missing CSRF tokens, and unencrypted headers. These results demonstrate how urgently configuration hardening, software updates, and policy enforcement are needed to provide strong security and maintain client confidence.

Vulnerability Risk Matrix

Table 1: Shows Vulnerabilities Risk Assessment Matrix

Vulnerability	Likelihood	Severity	Risk Level
Outdated Apache Server	High	Severe	High
ExposedPhpMyAdmin	High	Severe	High
Directory Traversal	Medium	Moderate	Medium
Missing CSRF Tokens	Medium	Moderate	Medium
Unencrypted Headers	Medium	Minor	Low

Password Analysis

Significant weaknesses in password management, which are essential for protecting high-value transactions, were found by the password analysis of the jewellery website. To enable exact brute-forcing, CeWL was used to extract selected keywords from the website and create a custom wordlist. The site's FTP service had weak default credentials (user:user), which Hydra found made it vulnerable to brute-force assaults. By using concurrent brute-forcing, Ncrack also revealed weak SSH credentials (user:user and msfadmin:msfadmin), highlighting vulnerabilities to data breaches, lateral movement, and unauthorised access. John the Ripper used wordlists like rockyou.txt to leverage dictionary and brute-force assaults to crack other weak passwords, like sys:batman and postgres:postgres. These results highlight the necessity of robust hashing techniques, frequent credential audits, account lockouts, and strong password restrictions in order to safeguard sensitive information and maintain consumer confidence (Biswas, 2022).

Exploitation

The jewellery website needs strong security to secure sensitive financial data and preserve its premium brand because it caters to wealthy clients who make high-value transactions. Using tools like the Metasploit Framework and SMTP Enumeration modules, exploit testing found important vulnerabilities. By using a reverse TCP payload to exploit a backdoor vulnerability, Metasploit was able to validate root control and grant remote shell access using commands like whoami and uname -a, exposing the possibility of system compromise and unauthorised access. Furthermore, by using Metasploit's auxiliary modules, SMTP Enumeration was able to find legitimate identities through VRFY/EXPN queries that could be used for additional exploitation. These weaknesses underline the necessity of taking preventative action to safeguard consumer interactions, stop security breaches, and maintain the exclusivity and credibility of the brand (*GeeksforGeeks*, 2022).

Key Findings

The jewellery platform's confidentiality, integrity, and availability were seriously jeopardised by the serious vulnerabilities found throughout the penetration testing procedure in several different areas. The main conclusions, arranged according to testing phases, are as follows:

1) Reconnaissance Phase:

   - Discovery of Hosts and Services: Nmap scans found several open ports on the target network, such as ports 21, 22, 80, and 443. These services (such as HTTP, SSH, and FTP) offer possible avenues for additional exploitation.

   - Exposure of Network Information: Programs like as Dmitry and Netdiscover made MAC addresses and other network information public, which may be used to move laterally within the network.

   - DNS Gaps: Unresolved DNS records were identified by recon-ng, indicating the possibility of configuration errors that might be used in focused assaults.

2) Vulnerability Analysis Phase:

   - Outdated Software: The Apache web server was vulnerable to known flaws including clickjacking and TRACE exploitation because it was running an outdated version (2.2.8).

   - Key Configurations: The attack surface was greatly expanded by Nikto and OWASP ZAP, which discovered directory traversal flaws, exposed phpMyAdmin, and missing security headers (such as CSP and X-Frame-Options).

   - High-Risk Vulnerabilities: Backdoors, remote code execution (RCE) exploits, and default credentials were among the serious vulnerabilities found by OpenVAS.

3) Password Analysis Phase:

   - Weak Default Credentials: Hydra discovered weak default credentials for SSH and FTP (such as msfadmin:msfadmin and user:user), exposing insufficient password management procedures.

- Exploitable Hashes: John the Ripper highlighted the necessity of safe password storage methods by successfully cracking weak hashes, such as MD5.

- Inadequate implementation of strong password policies has been exposed by the usage of easily guessed credentials (such as sys:batman and postgres:postgres), endangering account security and raising the possibility of unwanted access.

4) Exploitation Phase:

    - Root Access via Backdoor: The Metasploit Framework was able to gain root-level access of the target system by effectively exploiting a backdoor vulnerability. Commands like whoami and uname are examples of a confirmed full system penetration.

    - SMTP Enumeration: By exposing legitimate usernames on the server, the auxiliary SMTP module made it possible for other attacks such as privilege escalation, brute-forcing, and phishing.

Mitigation Plan

Based on the vulnerabilities discovered during penetration testing, the following solutions are proposed to strengthen the security of the jewellery e-commerce platform:

1) Unpatched System: The platform is vulnerable to known flaws due to the antiquated Apache server and associated software. Establish a patch management procedure that guarantees all systems are updated on a regular basis to lessen this. (Jackins, 2024) Reduce downtime by using automated methods to check for updates and apply fixes on time.

2) Weak Passwords: It was discovered that several default credentials, including user:user and msfadmin:msfadmin, were weak, and that some passwords, like postgres:postgres, were simple to figure out. Implement a robust password policy that consists of:

    - 12 characters is the minimum length.

    - A mix of special characters, digits, capitals, and lowercase letters.

    - Mandatory password changes and regular expiration.

    - Account lockouts following several unsuccessful attempts (Nidecki, 2022).

3) Open Ports: The attack surface is increased by having too many open ports, such as Telnet and FTP (port 21). Firewalls can be used to limit unused ports and services in order to solve this (Schrader, 2024). Establish a default deny-all policy that only permits necessary services, such as SSH (port 22) and HTTPS (port 443).

4) Unsecured Protocols: Data communications across protocols like HTTP and FTP are susceptible to interception since they are not encrypted. Make the switch to encrypted protocols like SFTP or SSH for file transfers and HTTPS (with TLS) for web traffic. Disable outdated protocols like Telnet and set up servers to reroute HTTP to HTTPS (Hakia, 2022).

The jewellery platform will greatly improve its defences, protect sensitive data, and uphold customer trust by taking aggressive steps to fix these vulnerabilities. The platform's security resilience will be further guaranteed by ongoing monitoring, frequent audits, and incident response preparation.

Security Enhancement

Adopting thorough long-term safeguards is essential to guaranteeing the jewellery platform's ongoing security and resilience. To find and fix new vulnerabilities while maintaining adherence to industry standards, regular penetration tests and audits should be carried out (Gilzene, 2023). To increase knowledge of prevalent cyberthreats like phishing and social engineering, employee training programs must be put in place. The possibility of human error resulting in breaches will be greatly decreased by training employees on safe password usage and data security. Deploying endpoint security capabilities, including as antivirus, anti-malware, and endpoint detection and response (EDR) solutions, will also protect all network-connected devices by enabling real-time monitoring and quick reactions to threats(Nasir, 2023).

The platform shall place a high priority on the development of safe and sustainable infrastructure in line with UN SDG 9 (Industry, Innovation, and Infrastructure). Reducing the environmental impact while preserving operational efficiency can be achieved by optimising server configurations and using energy-efficient hardware(Küfeoğlu, 2022). Scalability and resilience can be guaranteed without sacrificing security by implementing cutting-edge technology like secure cloud-based systems and AI-driven threat detection. Maintaining operational integrity, protecting sensitive client data, and establishing the platform as a pioneer in sustainable, progressive e-commerce may all be achieved by striking a balance between innovation and strong security procedures(Wing, 2021). These suggestions will promote long-term development and trust while guaranteeing the platform's resilience against changing threats.

Conclusion

Maintaining the jewellery e-commerce platform's premium brand and safeguarding sensitive financial data depend on its security. Unauthorised access, data breaches, and vulnerabilities like SQL Injection, XSS, and CSRF are examples of potential dangers that can lead to monetary loss, harm to one's reputation, and mistrust from customers. The requirement for strong security is increased when high-value transactions make the platform more appealing to attackers.

Protecting the jewellery platform, which serves wealthy clients conducting expensive transactions, requires penetration testing. By mimicking actual attacks, it finds weaknesses like out-of-date software, weak passwords, and unprotected protocols that might reveal private financial information or jeopardise consumer accounts. Critical defects including open ports, SQL Injection hazards, and inadequate authentication procedures are found throughout the testing phases of reconnaissance, vulnerability analysis, and exploitation. Resolving these issues guarantees that the platform will continue to withstand possible intrusions, safeguard consumer confidence, and maintain the high-end reputation of the brand.

For long-term success, a proactive security approach is necessary. Strong password policies, frequent system updates, encrypted communications, and ongoing monitoring with tools like SIEM and IDS are all part of this. Resilience is further increased by sustainable infrastructure development and employee training. By putting security first, the platform can protect user confidence, guarantee smooth operations, and position itself as a safe and creative leader in the luxury e-commerce space.

References

Biswas, D., 2022. Identifying and Mitigating Secure Socket Shell (SSH) Key Security Vulnerabilities*. [online] AppViewX. Available at: https://www.appviewx.com/blogs/identifying-and-mitigating-secure-socket-shell-ssh-key-security-vulnerabilities/ [Accessed 18 January 2025].*

Evalian®, 2024. *What is a penetration test and when should you get one?*, [Image], Evalian®. Available at: https://evalian.co.uk/what-is-a-penetration-test/ (Accessed 1 January 2025).

GeeksforGeeks, 2022. *SMTP Enumeration*. [online] Available at: https://www.geeksforgeeks.org/smtp-enumeration/[Accessed 19 Jan. 2025].

Gilzene, L., 2023. Implementing Cybersecurity Frameworks: Strengthening Defenses and Mitigating Risks. [online] CyberForum. Available at: https://medium.com/cyberforum/implementing-cybersecurity-frameworks-strengthening-defenses-and-mitigating-risks-d667be627b20 [Accessed 19 Jan. 2025].

Hakia, 2022. Secure Communication Protocols: SSL/TLS and HTTPS Encryption. [online] *Hakia.com.* Available at: https://hakia.com/secure-communication-protocols-ssl-tls-and-https-encryption/ [Accessed 19 Jan. 2025].

Jackins, T., 2024. Risks & Vulnerabilities of Unpatched Software. [online] Splashtop Blog. Available at: https://www.splashtop.com/blog/risks-and-vulnerabilities-of-unpatched-software [Accessed 19 Jan. 2025].

Kinger, P. Bharti, S. Oliveira, M.(2023) THE LINUX THREAT LANDSCAPE REPORT. *TrendMicro.* Available at: the-linux-threat-landscape-report (Accessed 4 December 2024).

Küfeoğlu, S., 2022. SDG-9: Industry, Innovation and Infrastructure. In: Emerging Technologies: Value Creation for Sustainable Development. Springer, pp.349–369. DOI:10.1007/978-3-031-07127-0_11. Available at: https://link.springer.com/chapter/10.1007/978-3-031-07127-0_11 [Accessed 19 Jan. 2025].

Nasir, S., 2023. Exploring the Effectiveness of Cybersecurity Training Programs: Factors, Best Practices, and Future Directions. Advances in Multidisciplinary & Scientific Research Journal Publication, 2(1), pp.151–160. DOI:10.22624/AIMS/CSEAN-SMART2023P18. Available at: https://www.researchgate.net/publication/373252980_Exploring_the_Effectiveness_of_Cy bersecurity_Training_Programs_Factors_Best_Practices_and_Future_Directions[Accessed 19 Jan. 2025].

Nidecki, T.A., 2022. Common Password Vulnerabilities. [online] *Acunetix Blog*. Available at: https://www.acunetix.com/blog/web-security-zone/common-password-vulnerabilities/ [Accessed 19 Jan. 2025].

RiskPal (2023) 'Risk Assessment Matrix', Risk Assessment Matrices - Tools to Visualise Risk*. Published on January 16, 2023. Available at: https://www.riskpal.com/risk-assessment-matrices/* Accessed: 18 December 2024).

Sankar, R., 2017. Netdiscover – Live Host Identification*. [online] Kali Linux Tutorials. Available at: https://kalilinuxtutorials.com/netdiscover-scan-live-hosts-network/#google_vignette [Accessed 18 January 2025].*

Schrader, D., 2024. Identifying Common Open Port Vulnerabilities in Your Network. [online] Netwrix Blog. Available at: https://blog.netwrix.com/open-ports-vulnerability-list [Accessed 19 Jan. 2025].

SentinelOne (2024) SIEM vs. IDS: Understanding the Core Differences. Available at: https://www.sentinelone.com/cybersecurity-101/data-and-ai/siem-vs-ids/#:~:text=IDS%20systems%20are%20network%2Dbased,anomalies%20in%20traffic%20are%20detected. (Accessed: 18 December 2024).

Sharma, K. (2022) SQL injection and cross-site scripting: The differences and attack anatomy. *ManageEngine.* Available at: https://www.manageengine.com/log-management/cyber-security/sql-injection-web-application-attack-and-cross-site-scripting-the-differences-and-attack-anatomy.html (Accessed 5 December 2024)

Soni, R. (2021) 'What is Broken Authentication Vulnerability and How to Prevent It?', *LoginRadius Blog*, 17 February. Available at: https://www.loginradius.com/blog/identity/what-is-broken-authentication/ (Accessed: 2 January 2025).

Vaishnavi, 2024. *Best Practices for Using OpenVAS in Vulnerability Assessment* | *Overview, Features, and Why Ethical Hackers Should Use It*. [online] WebAsha. Available at: https://www.webasha.com/blog/best-practices-for-using-openvas-in-vulnerability-assessment-overview-features-and-why-ethical-hackers-should-use-it [Accessed 18 January 2025].

Wing, S., 2021. Scalability, security, and performance in the cloud*. IBM Blog. Available at: https://www.ibm.com/blog/scalability-security-and-performance-in-the-cloud/ [Accessed 19 January 2025].*