**Ethical Hacking Report**

Prepared for: Martines Music Store Online

Prepared by: John Martine Gamilo

Keven Jahn C. Pajenago,

Keith Marianne Olaso

Date: April 26, 2024

---

**Executive Summary:**

This report presents the findings of an ethical hacking assessment conducted on Martines Music Store Online's e-commerce platform. The objective of the assessment was to identify potential vulnerabilities that could compromise the security and integrity of the online store. A total of 15 vulnerabilities were discovered, ranging from web application flaws to network misconfigurations. Recommendations are provided to mitigate these vulnerabilities and enhance the overall security posture of Martines Music Store Online.

---

**Vulnerability Assessment Results:**

**1. SQL Injection (Web Application)**

- Vulnerability: The web application is vulnerable to SQL injection attacks, allowing attackers to execute arbitrary SQL queries and access sensitive information from the database.

- Recommendation: Implement parameterized queries and input validation to prevent SQL injection attacks. Regularly sanitize user inputs and conduct security audits to detect and remediate vulnerabilities.

**2. Cross-Site Scripting (XSS) (Web Application)**

- Vulnerability: Cross-site scripting vulnerabilities exist in the web application, enabling attackers to inject malicious scripts into web pages viewed by other users.

- Recommendation: Implement output encoding and content security policies (CSP) to mitigate XSS vulnerabilities. Conduct security training for developers to raise awareness of secure coding practices.

**3. Outdated Software Versions (Server Infrastructure)**

- Vulnerability: Some server components are running outdated software versions, exposing the system to known security vulnerabilities.

- Recommendation: Establish a patch management process to ensure timely updates of software and firmware. Regularly monitor vendor advisories and security bulletins for patch releases.

**4. Weak Authentication Mechanisms (User Accounts)**

- Vulnerability: Weak authentication mechanisms are in place, allowing for brute-force attacks against user accounts.

- Recommendation: Enforce strong password policies, including requirements for length, complexity, and expiration. Implement multi-factor authentication (MFA) to enhance user authentication security.

**5. Insecure Direct Object References (Web Application)**

- Vulnerability: The web application exposes direct references to internal objects, enabling attackers to manipulate URLs and access unauthorized resources.

- Recommendation: Implement proper access controls and authorization mechanisms to restrict user access to authorized resources. Utilize session tokens instead of direct object references.

**6. Sensitive Data Exposure (Payment Processing)**

- Vulnerability: The payment processing system lacks proper encryption, potentially exposing sensitive payment information to unauthorized access.

- Recommendation: Encrypt sensitive data both in transit and at rest using strong encryption algorithms. Comply with Payment Card Industry Data Security Standard (PCI DSS) requirements for handling payment card data.

**7. Missing Security Headers (Web Application)**

- Vulnerability: Essential security headers such as Content Security Policy (CSP) and Strict-Transport-Security (HSTS) are missing from HTTP responses.

- Recommendation: Configure web servers to include security headers that provide additional layers of protection against common web-based attacks. Regularly audit and update security headers based on best practices.

**8. Insufficient Input Validation (Web Forms)**

- Vulnerability: Web forms lack proper input validation, enabling attackers to submit malicious input and potentially execute code on the server.

- Recommendation: Implement server-side input validation to sanitize user inputs and prevent injection attacks. Utilize frameworks and libraries that offer built-in protection against common vulnerabilities.

**9. Insecure File Uploads (User Content)**

- Vulnerability: The file upload feature allows users to upload files without proper validation, opening avenues for malicious file uploads and execution.

- Recommendation: Implement file upload restrictions based on file type, size, and content. Utilize server-side validation and file type verification to prevent the upload of malicious files.

**10. Exposed Admin Interfaces (Server Configuration)**

- Vulnerability: Admin interfaces are exposed to the public internet, increasing the risk of unauthorized access and administrative control.

- Recommendation: Restrict access to admin interfaces through IP whitelisting or VPNs. Implement strong authentication mechanisms and role-based access controls for administrative accounts.

**11. Lack of Intrusion Detection/Prevention Systems (Network Infrastructure)**

- Vulnerability: The network lacks intrusion detection/prevention systems (IDS/IPS), making it challenging to detect and respond to suspicious activities.

- Recommendation: Deploy IDS/IPS solutions to monitor network traffic for signs of unauthorized access and malicious activity. Configure alerts and automated response mechanisms for timely incident response.

**12. Improper Session Management (Web Application)**

- Vulnerability: Session tokens are not properly managed, potentially enabling session hijacking and unauthorized access to user accounts.

- Recommendation: Implement secure session management mechanisms such as session expiration, token regeneration, and secure cookie attributes. Enforce HTTPS for all session-related communications.

**13. Inadequate Backup and Recovery Procedures (Server Infrastructure)**

- Vulnerability: Backup and recovery procedures are inadequate, increasing the risk of data loss in the event of system failures or cyberattacks.

- Recommendation: Establish regular backup schedules for critical data and systems. Ensure off-site storage and encryption of backup files. Test backup and recovery procedures periodically to validate effectiveness.

**14. Unencrypted Network Traffic (Data Transmission)**

- Vulnerability: Network traffic is transmitted in plaintext, exposing sensitive data to interception and eavesdropping.

- Recommendation: Implement encryption protocols such as SSL/TLS to secure network communications. Use secure cipher suites and key exchange mechanisms to protect data confidentiality.

**15. Insecure Third-Party Integrations (Payment Gateways)**

- Vulnerability: Third-party payment gateways are integrated without proper security assessments, potentially introducing vulnerabilities into the system.

- Recommendation: Conduct thorough security assessments of third-party integrations to ensure compliance with security standards and best practices. Monitor for security updates and patches provided by third-party vendors.

---

**Conclusion:**

The vulnerabilities identified in this ethical hacking assessment pose significant risks to the security and integrity of Martines Music Store Online's e-commerce platform. It is essential that immediate action is taken to remediate these vulnerabilities and strengthen the overall security posture of the online store. By implementing the recommended security measures and adhering to best practices, Martines Music Store Online can mitigate potential threats and protect its customers' data and transactions from exploitation and compromise.

---

**Disclaimer**

This report is based on the findings of an ethical hacking assessment conducted by John Martine Gamilo and is intended solely for the use of Martines Music Store Online. The recommendations provided herein are advisory in nature and should be implemented at the discretion of Martines Music Store Online in accordance with its business requirements, risk tolerance, and regulatory obligations. John Martine Gamilo, Keven Jahn C. Pajenago, Keith Marianne Olaso

assumes no liability for any damages or losses arising from the implementation or non-implementation of the recommendations outlined in this report.