Ethical Hacking Technical Report

Client: Lazada Philippines

Date: 2024-05-10

Prepared by: Mark Glandestine L. Maniscan, and Marife Ranido

Executive Summary: The ethical hacking report conducted for Lazada Philippines, an online shopping platform in the Philippines highlights the technical findings. The assessment aimed to identify vulnerabilities within the organization's network infrastructure, web applications, and other critical systems. Multiple crucial and high-risk issues were found by employing a variety of testing approaches, including vulnerability scanning, load stress testing, social engineering testing, penetration testing, and source code review. The report details these findings and offers actionable recommendations for mitigation and remediation.

Vulnerability Summary

1. Network Configuration:

- Critical: Remote Code Execution vulnerability CVE-2024-5236 in the Apache Tomcat server version 9.0 on AppServer1 lets an attacker execute arbitrary code remotely and potentially gain control of the server.
- High: Inaccurate firewall rules that allow unauthorized access to the internal systems from external IP addresses, creating a path for attackers.
- Medium: Several internal systems have default credentials, which leaves them accessible to unauthorized access.

2. Web Applications:

- Critical: A flaw in the product search functionality lets attackers to extract sensitive information from the database, including customer private data.
- High: Cross-site scripting (XSS) vulnerability in user comments and reviews lets attackers put harmful scripts into users' browsers, which can lead to stolen data or taking over sessions.

3. Payment Systems:

- Critical: not secure payment gateway integration exposing credit card information to potential man-in-the-middle attacks. This vulnerability poses significant risks to customer financial information.
- High: Lack of encryption for sensitive payment data and information at rest, increasing the risk of unauthorized access and data breaches.
- High: Transaction manipulation or denial-of-service attacks could result from poor input validation in the payment processing system.

4. Customer Accounts:

- High: Allowing the user to create a weak password on their account, making them prone to brute-force attacks.
- Medium: There's no account lockout mechanism after multiple failed login attempts, making it vulnerable to brute-force attacks increasing the risk of credential-stuffing.

5. Social Engineering:

- High: Several employees are vulnerable to phishing attacks, potentially compromising internal systems through unauthorized access and data leakage.
- Medium: Lack of security awareness training for staff makes them vulnerable to social engineering attacks like phishing and pretexting.

Recommendations:

1. Network Infrastructure:

- Always Update Apache Tomcat to its newest version to fix the Remote Code Execution vulnerability.
- Review and update firewall rules to make sure they only let in allowed access and keep out unwanted entries.

2. Web Applications:

- Implement parameterized queries to mitigate the risk and lower the danger of SQL Injection attacks. Conduct deep code checks to find. Fix, and address risky coding habits.
- Add input validation and output encoding to prevent Cross-Site Scripting (XSS) vulnerabilities in user-generated content.

3. Payment Systems:

- Implement secure payment gateway integration with strong encryption and secured communication channels to protect sensitive payment data and information.
- Make sure to encrypt sensitive payment info when stored, using standard encryption ways.

4. Customer Accounts:

- Enforce strong password policies with minimum complexity requirements to reduce the risk of brute-force attacks.
- Implement account lockout mechanisms to prevent multiple unauthorized login attempts and mitigate credential-stuffing risks.

5. Social Engineering:

- Often conduct security training on staff or employees so they know about phishing attacks and their potential impact on security.
- Implement email filtering and anti-phishing measures to detect and block fishy emails.

Conclusion: Several critical security flaws and vulnerabilities in Lazada Philippines' network, web apps, payment processors, and user account control were found in the conducted ethical hacking report for this online shopping in the Philippines. Lazada Philippines can greatly strengthen its security against data theft and other cyber dangers by putting into practice practical suggestions for mitigation and restoration procedures.

Signature: