Security Testing Report for DGKart Application

By: Nischal Subedi

Date: September 2024

Executive Summary

This report outlines the security vulnerabilities identified in the DGKart shopping cart application during security testing. The scope of testing included critical workflows such as user login, adding items to the cart, payment checkout, password changes, and feedback submission.

Key vulnerabilities discovered during testing include SQL Injection, Broken Authentication, and Sensitive Data Exposure. The potential impact of these vulnerabilities includes data breaches, financial fraud, and unauthorized access to user accounts. The report provides recommendations for mitigating these risks, with a focus on remediation of high-severity vulnerabilities first.

By securing DGKart against these vulnerabilities, the application will offer better protection for users, enhance customer trust, and reduce the likelihood of cyberattacks.

Detailed Findings: Vulnerability 1 - SQL Injection

Severity: High

CVSS Score: 9.0 (Critical)

Proof of Concept (PoC):

An attacker can manipulate the login form using SQL Injection by inputting malicious SQL code into the username field, such as: ' OR 1=1; -- This allows the attacker to bypass the login authentication process entirely.

Steps to Reproduce:

1. Navigate to the login page of DGKart.
2. Enter malicious input (' OR 1=1; --) into the username field.
3. Click the 'Login' button and observe that authentication is bypassed.

Description:

SQL Injection vulnerabilities occur when untrusted data is concatenated directly into SQL queries. This allows attackers to execute arbitrary commands on the database, leading to unauthorized access or data manipulation.

Remediation:

1. Use parameterized queries or prepared statements to handle user input safely.
2. Sanitize and validate all user inputs.

Detailed Findings: Vulnerability 2 - Broken Authentication

Severity: High

CVSS Score: 8.5 (High)

Proof of Concept (PoC):

The application lacks mechanisms to enforce strong password policies or implement multi-factor authentication (MFA). Attackers can attempt brute force or credential stuffing to gain access to user accounts.

Steps to Reproduce:

1. Attempt to log in with a weak password (e.g., 'password123').
2. Observe that no MFA is required, allowing easy access.

Remediation:

1. Enforce strong password policies (minimum length, complexity).
2. Implement MFA to provide an additional layer of security.

Detailed Findings: Vulnerability 3 - Sensitive Data Exposure

Severity: Medium

CVSS Score: 7.0 (Medium)

Proof of Concept (PoC):

Sensitive data such as user payment information is not properly encrypted, potentially exposing it to attackers during data transmission.

Steps to Reproduce:

1. Perform a man-in-the-middle attack during the checkout process to intercept unencrypted payment data.

Remediation:

1. Implement encryption for sensitive data both at rest and in transit (e.g., HTTPS).
2. Store passwords securely using hashing algorithms such as bcrypt.

Conclusion

In conclusion, the security testing of DGKart revealed several high-risk vulnerabilities that must be addressed immediately. SQL Injection and Broken Authentication are critical risks that could lead to major data breaches if left unmitigated. Sensitive Data Exposure also poses a significant threat to user privacy and financial information.

To maintain the security and trustworthiness of DGKart, it is essential to implement the recommended remediation steps, including the use of parameterized queries, enforcing stronger password policies, and implementing encryption. Continuous monitoring and regular security audits will ensure the platform remains secure against future threats.