# Ethical Hacking Technical Report

**Client: CLC Enterprises**

**Date: May 14, 2024**

**Prepared by: Ma. Teresa R. Papa and Dominic Bañaria**

**Executive Summary:**

This report presents the technical findings of the ethical hacking assessment conducted for CLC Enterprises. The assessment aimed to identify vulnerabilities within the organization's network. Through various testing methodologies, including penetration testing and vulnerability scanning, critical and high-risk issues were discovered. This report provides detailed descriptions of these findings, along with actionable recommendations for remediation.

**Vulnerability Summary:**

**1. SQL Injection Attack**

Critical: Allows attackers to execute arbitrary SQL queries, potentially leading to data leakage or loss.

High: Allowing unsanitized user inputs in SQL queries.

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

Critical: Enables attackers to inject malicious scripts into web pages viewed by other users.

High: Lack of input validation and output encoding in web applications.

**3. Remote Code Execution (RCE)**

Critical: Allows attackers to execute arbitrary code on the server, leading to complete compromise.

High: Unpatched software or vulnerable server configurations.

**4. Insecure Direct Object References (IDOR)**

Critical: Allows attackers to access unauthorized resources or manipulate sensitive data.

High: Lack of proper access controls and authorization checks.

**5. Sensitive Data Exposure**

Critical: Exposes sensitive information such as passwords or personal data.

High: Storing passwords in plaintext or inadequate encryption mechanisms.

**6. Insecure Deserialization**

Critical: Can lead to remote code execution or denial of service attacks.

High: Lack of integrity checks or validation on serialized data.

**7. Security Misconfiguration**

Critical: Incorrectly configured security settings or default credentials.

High: Open ports, unnecessary services running, or outdated software versions.

**8. Weak Password Policies**

Critical: Allows easy access to accounts through brute-force attacks or password guessing.

High: Lack of password complexity requirements, no multi-factor authentication.

**9. File Inclusion Vulnerabilities**

Critical: Enables attackers to include and execute arbitrary files on the server.

High: Inclusion of files from user-controlled inputs without proper validation.

**10. Broken Authentication**

Critical: Allows unauthorized users to gain access to privileged functionalities.

High: Session fixation, weak session management, or predictable session tokens.

**Recommendations**

- Implement input validation and output encoding to prevent SQL Injection and XSS attacks.
- Keep software and systems up-to-date to mitigate Remote Code Execution vulnerabilities.
- Enforce strict access controls and authorization checks to prevent Insecure Direct Object References.
- Encrypt sensitive data at rest and in transit to mitigate Sensitive Data Exposure risks.
- Implement integrity checks and validation on deserialized data to prevent Insecure Deserialization.

- Regularly audit and review security configurations to avoid Security Misconfigurations.
- Enforce strong password policies and implement multi-factor authentication to mitigate Weak Password Policies.
- Sanitize user-controlled file inclusions and limit file access to prevent File Inclusion Vulnerabilities.
- Implement secure authentication mechanisms and session management to address Broken Authentication issues.

**Conclusion**

The findings of this ethical hacking assessment reveal significant vulnerabilities within CLC Enterprises' network infrastructure and applications. Immediate action is required to remediate these issues to safeguard against potential exploitation by malicious actors.

**Signature:**

Ma. Teresa R. Papa

Dominic Bañaria