

Security Assessment Findings Report

**Fake Company**

**Fake Client**

Date: 10th of March, 2024

Version: 1.0

# Table of Contents

[Table of Contents 2](#_Toc169552077)

[Confidentiality Statement 3](#_Toc169552078)

[Disclaimer 3](#_Toc169552079)

[Contact Information 3](#_Toc169552080)

[Assessment Overview 4](#_Toc169552081)

[Finding Severity Ratings 5](#_Toc169552082)

[Scope 6](#_Toc169552083)

[Scope Exclusions 6](#_Toc169552084)

[Client Allowances 6](#_Toc169552085)

[Executive Summary 7](#_Toc169552086)

[Scoping and Time Limitations 7](#_Toc169552087)

[Testing Summary 8](#_Toc169552088)

[Vulnerability Summary & Report Card 9](#_Toc169552089)

[Technical Findings Details 10](#_Toc169552090)

[1. Remote Code Execution (RCE) - Critical 10](#_Toc169552091)

[2. SQL Injection - High 11](#_Toc169552092)

[3. Insecure Direct Object References (IDOR) - High 12](#_Toc169552093)

[4. Cross-Site Scripting (XSS) - Medium 13](#_Toc169552094)

[5. Insufficient Logging and Monitoring - Medium 14](#_Toc169552095)

[6. Outdated Software - Low 15](#_Toc169552096)

# Confidentiality Statement

This document is owned solely by Fake Company.It contains proprietary and confidential information. Any duplication, redistribution, or use, whether in whole or in part, requires the express consent of both Fake Company and Fake Client. Fake Client is permitted to share this document with auditors under non-disclosure agreements to fulfill penetration test compliance requirements.

# Disclaimer

A penetration test provides a snapshot of security at a specific moment. The findings and recommendations are based on the information collected during the assessment period and do not account for any changes or modifications made thereafter. Due to time constraints, a comprehensive evaluation of all security controls may not be feasible. Fake Company focused on identifying the most vulnerable security controls that could be exploited by attackers.We advise conducting similar assessments annually, either internally or through third-party assessors, to ensure the ongoing effectiveness of the security controls.

# Contact Information

|  |  |  |
| --- | --- | --- |
| Name | Title | Contact Information |
|  |  |  |
|  |  |  |

# Assessment Overview

Between 10th of March, 2024 and 15th of March, 2024, Fake Company conducted an evaluation of Fake Client's infrastructure security posture, benchmarking it against current industry best practices, including an internal network penetration test. The testing was conducted following the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, the OWASP Testing Guide (v4), and other customized testing frameworks.

The phases of the penetration testing activities are as follows:

* 1. Planning – Define customer goals and establish rules of engagement.
* 2. Discovery – Scan and enumerate to identify potential vulnerabilities, weak points, and exploits.
* 3. Attack – Validate potential vulnerabilities through exploitation and continue discovery upon gaining access.
* 4. Reporting – Document all identified vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.

# Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

|  |  |  |
| --- | --- | --- |
| Severity | CVSS V3 Score Range | Definition |
| Critical | 9.0-10.0 | Exploitation is direct and typically leads to system-level compromise. Immediate action and patching are recommended. |
| High | 7.0-8.9 | Exploitation is more challenging but could result in elevated privileges and potential data loss or downtime. Prompt action and patching are advised. |
| Moderate | 4.0-6.9 | Vulnerabilities exist but are not easily exploitable or may require additional steps like social engineering. Action and patching after resolving high-priority issues are recommended. |
| Low | 0.1-3.9 | Vulnerabilities are not exploitable but may reduce the organization’s attack surface. Action and patching during the next maintenance window are advised. |
| Informational | N/A | No vulnerabilities are present. Additional information is provided regarding observations during testing, strong controls, and further documentation. |

# Scope

|  |  |
| --- | --- |
| Assessment | Details |
|  |  |

## Scope Exclusions

At the request of the client, Fake Company refrained from performing the following types of attacks during the testing:

## Client Allowances

Fake Client provided Fake Company the following allowances:

# Executive Summary

Fake Company evaluated Fake Client's internal security posture through penetration testing from 10th of March, 2024 to 15th of March, 2024. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

## Scoping and Time Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components.  
Time limitations were in place for testing. Internal network penetration testing was permitted for ten business days.

# Testing Summary

# Vulnerability Summary & Report Card

A brief summary of the identified vulnerabilities, including their severity and status.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 6 | 1 | 2 | 2 | 1 |
| Total | Critical | High | Medium | Low |

|  |  |  |  |
| --- | --- | --- | --- |
| Finding # | Vulnerability | Severity | Status |
| 1 | Remote Code Execution (RCE) | Critical | Open |
| 2 | SQL Injection | High | Open |
| 3 | Insecure Direct Object References (IDOR) | High | Open |
| 4 | Cross-Site Scripting (XSS) | Medium | Open |
| 5 | Insufficient Logging and Monitoring | Medium | Open |
| 6 | Outdated Software | Low | Open |

# Technical Findings Details

## 1. Remote Code Execution (RCE) - Critical

|  |  |
| --- | --- |
| CWE |  |
| CVSS 3.1 Score | 9.9 |
| Description | This vulnerability allows attackers to execute arbitrary code on the server, potentially gaining full control over the system. |
| Security Impact |  |
| Affected Domain |  |
| Remediation |  |
| External References |  |

Finding Evidence:

## 2. SQL Injection - High

|  |  |
| --- | --- |
| CWE |  |
| CVSS 3.1 Score | 9.8 |
| Description | This vulnerability allows attackers to execute arbitrary SQL commands on the database, potentially leading to unauthorized access and data manipulation. |
| Security Impact |  |
| Affected Domain |  |
| Remediation |  |
| External References |  |

Finding Evidence:

## 3. Insecure Direct Object References (IDOR) - High

|  |  |
| --- | --- |
| CWE |  |
| CVSS 3.1 Score | 8.6 |
| Description | This issue allows attackers to access unauthorized data by manipulating references to objects, such as database entries or files, through a user input. |
| Security Impact |  |
| Affected Domain |  |
| Remediation |  |
| External References |  |

Finding Evidence:

## 4. Cross-Site Scripting (XSS) - Medium

|  |  |
| --- | --- |
| CWE |  |
| CVSS 3.1 Score | 6.5 |
| Description | This vulnerability enables attackers to inject malicious scripts into web pages viewed by other users, which can result in data theft and session hijacking. |
| Security Impact |  |
| Affected Domain |  |
| Remediation |  |
| External References |  |

Finding Evidence:

## 5. Insufficient Logging and Monitoring - Medium

|  |  |
| --- | --- |
| CWE |  |
| CVSS 3.1 Score | 6.4 |
| Description | Lack of comprehensive logging and monitoring can delay the detection and response to security incidents. |
| Security Impact |  |
| Affected Domain |  |
| Remediation |  |
| External References |  |

Finding Evidence:

## 6. Outdated Software - Low

|  |  |
| --- | --- |
| CWE |  |
| CVSS 3.1 Score | 4.3 |
| Description | Running outdated software versions exposes the system to known vulnerabilities that have been fixed in newer releases, increasing the risk of exploitation. |
| Security Impact |  |
| Affected Domain |  |
| Remediation |  |
| External References |  |

Finding Evidence: