**<ORGANIZATION Name>**

**Security Assessment Report**

January 11, 2021

Prepared by: <NAME>

Email: <EMAIL>

Version: 1.0

Table of Contents

[Confidentiality Statement 2](#_Toc94433242)

[Disclaimer 2](#_Toc94433243)

[Assessment Overview 3](#_Toc94433244)

[Scope 4](#_Toc94433245)

[Findings Severity Ratings 5](#_Toc94433246)

[Executive Summary 6](#_Toc94433247)

[Assessment Summary 6](#_Toc94433248)

[Vulnerabilities by Impact 7](#_Toc94433249)

[Technical Findings 8](#_Toc94433250)

[SQL Injection (High) 8](#_Toc94433251)

[Attack Narrative 8](#_Toc94433252)

[Remediation 8](#_Toc94433253)

[Unrestricted File Upload (Critical) 9](#_Toc94433254)

[Attack Narrative 9](#_Toc94433255)

[Remediation 9](#_Toc94433256)

# Confidentiality Statement

This document is the exclusive property of <ORGANIZATION NAME> and <NAME>. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of property owners.

<NAME> may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

# Disclaimer

A penetration test is a point-in-time assessment of the target environment. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. The weakest security controls an attacker would exploit were prioritized during this assessment. It is recommended that similar assessments are conducted on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

# Assessment Overview

From January 3, 2022, to January 11,2022, <ORGANIZATION NAME> engaged <NAME> to evaluate the security posture of its web application compared to current industry best

practices by performing a Black Box Penetration Test. The goals of the assessment are to report any vulnerabilities and working exploits against the application with the objective of logging in to the administrator area of the application as the administrator user. All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment and customized testing frameworks*.

Phases of penetration testing activities include the following:

* Planning – Customer goals are gathered, and rules of engagement obtained.
* Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
* Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
* Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.

Diagram

Description automatically generated

## Scope

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

## Findings Severity Ratings

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

|  |  |  |
| --- | --- | --- |
| **Risk Rating** | **CVSSv3 Score** | **Description** |
| **Critical** | 9.0 - 10.0 | The vulnerability discovered is rated critical. It can be easily exploited resulting in system level compromise. This requires immediate plan of action and patching. |
| **High** | 7.0 - 8.9 | The vulnerability discovered is rated high. It is difficult to exploit but could cause elevated privileges, loss of data, or downtime if exploited. A plan of action should be formed, and patching should be conducted as soon as possible. |
| **Medium** | 4.0 - 6.9 | The vulnerability discovered is rated medium. It may not be exploitable or requires extra steps such as social engineering. A plan of action and should be formed, and patching should be conducted after high-priority issues are resolved. |
| **Low** | 0.1 - 3.9 | The vulnerability discovered is rated low. It may not be exploitable but increases the organization’s attack surface. This should be addressed as part of routine maintenance tasks. |
| **Informational** | N/A | No vulnerability was discovered. Instead, information is given about the items discovered during testing, strong controls, and additional documentation. |

# Executive Summary

From January 3, 2022, to January 11, 2022, an evaluation of <ORGANIZATION NAME>’s web application was conducted through a Black Box Penetration Test. Several vulnerabilities were discovered within <ORGANIZATION NAME>’s web application and a critical vulnerability was used to gain access to the web server hosting the application which led to access to the administrator area of the application as the administrator user. It is advised that <ORGANIZATION NAME> address these vulnerabilities as soon as possible as it can be exploited with minimal effort.

## Assessment Summary

The table below describes the steps taken to meet the assessment objective.

|  |  |  |
| --- | --- | --- |
| Step | Action | Recommendation |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |

## Vulnerabilities by Impact

The graph below represents a summary of the total number of vulnerabilities found within the assessment’s scope.

# Technical Findings

## SQL Injection (High)

|  |  |
| --- | --- |
| Description | SQL Injection or SQLI are the result of attackers inserting SQL queries into a data input in an application. SQLI is performed by injecting SQL commands into data-plane input in which alters the execution of the application’s predefined SQL commands. This attack enables attackers to read and modify data from databases as well as issue commands to the operating system. |
| Impact | High |
| Affected Hosts/URLs |  |
| References |  |

### Attack Narrative

### Remediation

## Unrestricted File Upload (Critical)

|  |  |
| --- | --- |
| Description | Unrestricted File Upload is a vulnerability that allows users to arbitrarily upload files. This attack is performed by uploading files that allows attackers to gain code execution of the server. The consequences of unrestricted file upload include system takeover and defacement of the website. |
| Impact | Critical |
| Affected Hosts/URLs |  |
| References |  |

### Attack Narrative

### Remediation