TITTLE

Security Assessment Findings Report

Business Confidential

Date: Nov 1st, 2021

Contents

[Confidentiality Statement 4](#_Toc88045583)

[Disclaimer 4](#_Toc88045584)

[Contact Information 4](#_Toc88045585)

[Assessment Overview 5](#_Toc88045586)

[Assessment Components 5](#_Toc88045587)

[External Penetration Test 5](#_Toc88045588)

[Scope 6](#_Toc88045589)

[Scope Exclusions 6](#_Toc88045590)

[Client Allowances 6](#_Toc88045591)

[Penetration diagram 6](#_Toc88045592)

[Finding Severity Ratings 6](#_Toc88045593)

[Executive Summary 8](#_Toc88045594)

[Attack Summary 8](#_Toc88045595)

[Vulnerabilities CVSS score 8](#_Toc88045596)

[VULNERABILITY 8](#_Toc88045597)

[Vulnerabilities by Impact 8](#_Toc88045598)

[Vulnerabilities finding by Host 9](#_Toc88045599)

[Host: 9](#_Toc88045600)

[Summary 9](#_Toc88045601)

[Reconnaissance details 9](#_Toc88045602)

[Exploitation Phase 9](#_Toc88045603)

[Exploitation details 9](#_Toc88045604)

[Exploitation Phase 10](#_Toc88045605)

[Exploitation details 10](#_Toc88045606)

[Post exploitation 10](#_Toc88045607)

[Remediation for THE VULNERABILITY 10](#_Toc88045608)

[Analysis and exploitation of application 10](#_Toc88045609)

[Buffer Overflow details 10](#_Toc88045610)

[Remediation for Buffer overflows 10](#_Toc88045611)

Table of Figures

[Figure 1 - Assessment overview 5](#_Toc88045612)

# Confidentiality Statement

TEXT

# Disclaimer

TEXT

# Contact Information

|  |  |
| --- | --- |
|  |  |

|  |  |  |
| --- | --- | --- |
| Name | Title | Contact Information |
| **eLearn Security** | | |
| NAME | Lead Penetration Tester | Office: (555) 555-5555  Email: [EMAIL](mailto:patriciotaraya@gmail.com) |
| Support | Business Support | Office: (555) 555-5555  Email: [EMAIL](mailto:support@elearnsecurity.com) |

# Assessment Overview

From Nov 1st, 2021, to Nov 8th, 2021, COMPANY engaged COMPANY to evaluate the security posture of its infrastructure compared to current industry best practices that included an external penetration test. All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), 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

Figure 1 - Assessment overview

# Assessment Components

## External Penetration Test

TEXT

# Scope

|  |  |
| --- | --- |
| Assessment | Details |
| External Penetration Test | TEXT |
| COMPANY NAME | TEXT |

## Scope Exclusions

TEXT

## Client Allowances

TEXT

## Penetration diagram

IMAGE

## 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 V3.1 Score Range | Definition |
| --- | --- | --- |
| Critical | 9.0-10.0 | Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately. |
| High | 7.0-8.9 | Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible. |
| Medium | 4.0-6.9 | Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved. |
| Low | 0.1-3.9 | Vulnerabilities are non-exploitable but would reduce an organization’s attack surface. It is advised to form a plan of action and patch during the next maintenance window. |
| Informational | N/A | No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation. |

# Executive Summary

MEGA TEXT

## Attack Summary

The following table describes how eLS gained DMZ access, step by step:

|  |  |  |
| --- | --- | --- |
| Step | Action | Recommendation |
| 1 | ACTION | TEXT |
| 2 | ACTION | TEXT |

# Vulnerabilities CVSS score

The scoring system provides a simple and straightforward numeric system for establishing the potential threat individual components pose to a system, the lower the score, the less risky the vulnerability poses to the entire system, whereas a 10.0 score needs to be addressed immediately.

## VULNERABILITY

Base score: NUMBER

CODE

# Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:

# Vulnerabilities finding by Host

## Host:

|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
| Port | Service | Details of the Service | Vulnerability |
|  |  |  |  |

Summary

TEXT

Reconnaissance details

DETAILS

Exploitation Phase

SUMMARY

Exploitation details

DETAILS

Exploitation Phase

SUMMARY

Exploitation details

SUMMARY

Post exploitation

SUMMARY

Remediation for THE VULNERABILITY

REMEDIATION

Analysis and exploitation of application

SUMMARY

**Explanation of the python code by file**

|  |  |
| --- | --- |
| File Name | Details |
| NAME | EXPLANATION |
|  |  |
|  |  |
|  |  |

Buffer Overflow details

DETAILS

Remediation for Buffer overflows

REMEDIATION