**<EXAM NAME> Security Assessment and Penetration Test**

Prepared for



**By**

<NAME HERE>

Table of Contents

[Executive Summary 1](#_Toc1625301236)

[Introduction 1](#_Toc712332737)

[Services 1](#_Toc1652628488)

[Findings Summary 1](#_Toc1417777005)

[Web Application Security Assessment 1](#_Toc321998938)

[Discovery and Port Scanning 1](#_Toc360630664)

[Vulnerability Scanning 2](#_Toc55437759)

[Penetration Testing 2](#_Toc1575932757)

[Findings Details 3](#_Toc1950059389)

[Web Application Security Assessment 4](#_Toc1830530763)

[Overview  4](#_Toc295861040)

[Discovery and Port Scanning 4](#_Toc1889065175)

[Vulnerability Scanning  4](#_Toc680506653)

[Web Application Penetration Testing  4](#_Toc1633069877)

[Technical Web Application Findings 6](#_Toc103161085)

[Finding WAPT-001: Finding Example 1 6](#_Toc1864184928)

[Finding WAPT-001: Finding Example 2 7](#_Toc500377720)

[Finding WAPT-001: Finding Example 3 8](#_Toc1809970290)

[Finding WAPT-001: Finding Example 4 9](#_Toc145450777)

# 

# Executive Summary

## Introduction

This report is separated into this Executive Summary, which provides a “high-level” view of the findings, with limited technical information and a technical details section. The detailed section is an abbreviated compilation of the engineer’s observations, results of security scanning tools, and manual testing.

## Services

eLearnSecurity required a security and penetration test for a combination of regulatory compliance, customer requirements, and general security purposes. This report details the results of the annual security assessment and penetration test, conducted <DATES OF EXAM>.

Security testing and analysis was conducted as follows:

* Web Application (Internet-based) discovery, port, and vulnerability scans, and Penetration Testing of specified systems

Internet-based testing was conducted from the engineer’s home office. eLearnSecurity staff had no limitations in testing.

## Findings Summary

<USE THE FOLLOWING AS A GENERAL GUIDELINE FOR WRITING SUMMARY FINDINGS>

Based on the technical areas reviewed, <YOUR NAME> has determined that eLearnSecurity is at an overall *<HIGH/MEDIUM/LOW>-*risk level. There are multiple items that should be remediated for security purposes and that require remediation for most compliance purposes.

## Web Application Security Assessment

### Discovery and Port Scanning

All in scope domains provided by eLearnSecurity that were identifiable were tested for accessibility and connectivity. Hosts found to be accessible were tested for vulnerabilities and exploitation using industry best standards. Untested systems may contain vulnerabilities that are not represented in this report.

### Vulnerability Scanning

The next phase in a typical security assessment is to determine the vulnerabilities which exist on the systems identified in the port scanning phase. For this assessment, all live systems were specified for testing.

High, Medium, and low risk vulnerabilities were discovered. Most can be resolved with a configuration change, proper management of security certificates, or update to a new version.

### Penetration Testing

Many high, medium, and low vulnerabilities were confirmed and are shown in the Penetration testing details section.

# Findings Details

#### 

#### 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** | 9-10 | Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately. |
| **High** | 7-8 | 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. |
| **Moderate** | 4-6 | 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** | 1-3 | 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. |

## Web Application Security Assessment

### Overview

External attackers have the advantages of anonymity and flexibility of time and schedule. They can be aggressive in attacking an organization’s Internet-facing systems. Unnoticed misconfigurations or missing patches can allow an attacker access to sensitive systems and data.

This web application assessment focused on known vulnerabilities that could be exploited by an anonymous, Internet-based attacker.

During this phase, <YOUR NAME> performed detailed assessment tests and probing to identify the presence of vulnerabilities.  These tests were performed with multiple tools, including <LIST YOUR TOOLS USED HERE>, and more.

### Discovery and Port Scanning

eLearnSecurity provided the following URLs for testing, noting that any domain and subdomain found is in scope:

|  |  |
| --- | --- |
| **In Scope IP addresses** | **Corresponding Domain Name** |
|  |  |
|  |  |
|  |  |

### Vulnerability Scanning

The table below shows the vulnerabilities that were verified by the engineer during testing. <ADD THE APPROPRIATE INFORMATION BELOW, WHICH WILL CORRESPOND WITH THE TECHNICAL FINDINGS SECTION LATER IN THE REPORT>

| **IP Addresses/Domains** | **Reference Item** | **Vulnerability Title** | **Severity** | **Recommendation** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### Web Application Penetration Testing

A Web Application Penetration Test differs from a vulnerability assessment in that the engineer attempts to exploit the vulnerabilities to determine what information is exposed to the outside world. A Web Application Penetration Test mimics the actions of an actual attacker exploiting weaknesses in the network security without the usual dangers. This test examines external IT systems for any weakness that could be used by an external attacker to disrupt the confidentiality, availability, or integrity of the network, thereby allowing the organization to address each weakness.

This web application penetration test follows best practice in penetration testing methodologies which includes:

* Footprinting
* Public Information & Information Leakage
* DNS Analysis & DNS Bruteforcing
* Port Scanning
* System Fingerprinting
* Services Probing
* Exploit Research
* Manual Vulnerability Testing and Verification of Identified Vulnerabilities
* Password Service Strength Testing

## Technical Web Application Findings

### Finding WAPT-001: Finding Example 1

|  |  |
| --- | --- |
| **Description:** | Include a brief description of the issue found |
| **Systems:** | Include the URL(s) or IP(s) affected |
| **Severity:** | Match Severity with the Severity Table |
| **Tools Used:** | List the tool(s) used for the finding |
| **References:** | List appropriate research references for the issue |

**Evidence**

**A picture containing logo

Description automatically generated**

***Use this comment space for vulnerable commands, vulnerable links, or any other supporting information; Replace the image above with screenshot evidence of the issue***

**Remediation**

Use this space to offer suggestions for remediating the issue found.

### Finding WAPT-001: Finding Example 2

|  |  |
| --- | --- |
| **Description:** | Include a brief description of the issue found |
| **Systems:** | Include the URL(s) or IP(s) affected |
| **Severity:** | Match Severity with the Severity Table |
| **Tools Used:** | List the tool(s) used for the finding |
| **References:** | List appropriate research references for the issue |

**Evidence**

**A picture containing logo

Description automatically generated**

***Use this comment space for vulnerable commands, vulnerable links, or any other supporting information; Replace the image above with screenshot evidence of the issue***

**Remediation**

Use this space to offer suggestions for remediating the issue found.

### Finding WAPT-001: Finding Example 3

|  |  |
| --- | --- |
| **Description:** | Include a brief description of the issue found |
| **Systems:** | Include the URL(s) or IP(s) affected |
| **Severity:** | Match Severity with the Severity Table |
| **Tools Used:** | List the tool(s) used for the finding |
| **References:** | List appropriate research references for the issue |

**Evidence**

**A picture containing logo

Description automatically generated**

***Use this comment space for vulnerable commands, vulnerable links, or any other supporting information; Replace the image above with screenshot evidence of the issue***

**Remediation**

Use this space to offer suggestions for remediating the issue found.

### Finding WAPT-001: Finding Example 4

|  |  |
| --- | --- |
| **Description:** | Include a brief description of the issue found |
| **Systems:** | Include the URL(s) or IP(s) affected |
| **Severity:** | Match Severity with the Severity Table |
| **Tools Used:** | List the tool(s) used for the finding |
| **References:** | List appropriate research references for the issue |

**Evidence**

**A picture containing logo

Description automatically generated**

***Use this comment space for vulnerable commands, vulnerable links, or any other supporting information; Replace the image above with screenshot evidence of the issue***

**Remediation**

Use this space to offer suggestions for remediating the issue found.

**THIS PAGE LEFT INTENTIONALLY BLANK**