

Penetration Test Report

{{customer}}  
{{product}}

Assessment Date: **{{assessment\_date}}**

# Table of Contents

{{toc|md}}

# 1. Executive Summary

{{executive\_summary|md}}

# 2. Introduction

## 2.1 Background

{{ background|md }}

## 2.2 Purpose

{{ purpose|md }}

## 2.3 Methodology

{{ methodology|md }}

## 2.4 Scope

{{ scope|md }}

# 3. Definitions

This matrix is used to evaluate and prioritize risks identified during the penetration test. It combines the **Likelihood** of a vulnerability being exploited with the **Consequence** of such an event to determine the overall risk level. The matrix provides a clear and structured way to categorize risks as Low, Medium, High, or Critical, enabling stakeholders to focus on mitigating the most significant vulnerabilities effectively and efficiently.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Consequence*** | |  |  |  |  |  | | --- | --- | --- | --- | --- | | Catastrophic | High | High | Critical | Critical | | Major | Medium | High | High | Critical | | Moderate | Low | Medium | High | High | | Minor | Low | Low | Medium | High | |  | Low | Medium | High | Very high | |
|  | ***Likelihood*** |

{{definition\_descriptions|md}}

# 4. Findings

This section summarizes the vulnerabilities identified during the penetration test.

Each vulnerability has been categorized by its risk level (Low, Medium, High, Critical) based on its likelihood of exploitation and potential impact.

Technical details, including detailed description, proof of concept, remediation recommendations and references, are provided in the **Findings Detail** section.

{%- set severities = ['Critical', 'High', 'Medium', 'Low'] -%}

{%- for severity in severities %}

{%- set severity\_findings = findings | selectattr('severity', 'equalto', severity) | list -%}

{%- if severity\_findings %}

#### {{r severity|color }}

{%- for finding in severity\_findings %}

5.{{ finding.finding\_number }} - {{ finding.finding\_title }}

{%- endfor %}  
{%- endif %}  
{%- endfor %}

# 5. Findings Detail

This section provides detailed technical information for each vulnerability identified during the penetration test. For each finding, the following details are included: a description of the issue, proof of concept, severity and recommendations for remediation. These details aim to help stakeholders understand the vulnerabilities and take appropriate actions to address them.

{% for finding in findings %}

## 5.{{finding.finding\_number}} {{finding.finding\_title}}

**Consequence:** {{r finding.consequence|color}} **| Likelihood:** {{r finding.likelihood|color}} **| Severity:** {{r finding.severity|color}}

“{{finding.general\_vulnerability\_description}}”

{{finding.finding\_text|md}}{% endfor %}

# 6. Conclusion

{{conclusion|md}}