|  |
| --- |
| {name} |
| Pentest Report  Executed by <YOUR COMPANY HERE> |
| {date | convertDateLocale: 'us': 'full'} |

{%company.logo}

modifications history

| **Version** | **Date** | **Author** | **Description** |
| --- | --- | --- | --- |
| 0.1 | {date | convertDateLocale: 'us':'short'} | {creator.firstname} {creator.lastname} | Initial Version |
|  |  |  |  |
|  |  |  | Quality Assurance |
| 1.0 |  |  | Finalization |

distribution circle

|  |  |  |
| --- | --- | --- |
| **Organization** | **Team** | **Members** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Table of Contents

1. General Information 4

1.1 Scope 4

1.2 Organization 4

2. Executive Summary 5

3. Technical Details 6

3.1 title 6

4. Vulnerabilities summary 8

# General Information

## Scope

{company.name} has mandated us to perform security tests on the following scope:

* {-w:p scope}{name}{/scope}

## Organization

The testing activities were performed between {date\_start | convertDateLocale: 'us':'short'} and {date\_end | convertDateLocale: 'us':'short'}.

# Executive Summary

This penetration test was conducted to assess the security posture of {company.name}’s [network/infrastructure/application].

The objective was to identify vulnerabilities that could be exploited by malicious actors and provide recommendations to mitigate these risks.

Starting from {date\_start | convertDateLocale: 'us':'short'}, a pentest of the environment has been conducted.

The overall risk based on the identified vulnerabilities is [Low/Medium/High/Critical]. This assessment takes into account the ease of exploitation and the potential impact on the organization.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Critical**  {#findings}{#cvss.baseSeverity == 'Critical'}  {@cvss.cellColor}  {/cvss.baseSeverity == 'Critical'}{/findings} | **High**  {#findings}{#cvss.baseSeverity == 'High'}  {@cvss.cellColor}  {/cvss.baseSeverity == 'High'}{/findings} | **Medium**  {#findings}{#cvss.baseSeverity == 'Medium'}  {@cvss.cellColor}  {/cvss.baseSeverity == 'Medium'}{/findings} | **Low**  {#findings}{#cvss.baseSeverity == 'Low'}  {@cvss.cellColor}  {/cvss.baseSeverity == 'Low'}{/findings} | **Info**  {#findings}{#cvss.baseSeverity == 'None'}  {@cvss.cellColor}  {/cvss.baseSeverity == 'None'}{/findings} |
| {findings | count: 'Critical'} | {findings | count: 'High'} | {findings | count: 'Medium'} | {findings | count: 'Low'} | {findings | count: 'None'} |

The penetration test has highlighted several areas where the security posture can be improved. By addressing the identified vulnerabilities and implementing the recommended measures, the risks of exploitation can significantly be reduced.

FREE TEXT HERE

**DISCLAIMER**

A pentest is always a snapshot of the current situation with the time given to identify potential flaws. This situation changes over time when new threats and vulnerabilities occur. A pentest is not a guarantee to identify all technical vulnerabilities and fixing all findings must not be considered a completely implemented Security Concept. A pentest does not replace any organizational procedures to ensure IT Security or the proper operation of the service or application.

# Vulnerabilities summary

Following vulnerabilities have been discovered:

|  |  |  |
| --- | --- | --- |
| **Risk** | **Page** | **Vulnerability** |
| {@cvss.cellColor}  {#findings}{#cvss.baseSeverity == 'Critical'}  {cvss.baseSeverity} |  | {title}  {/cvss.baseSeverity == 'Critical'}{/findings} |
| {@cvss.cellColor}  {#findings}{#cvss.baseSeverity == 'High'}  {cvss.baseSeverity} |  | {title}  {/cvss.baseSeverity == 'High'}{/findings} |
| {@cvss.cellColor}  {#findings}{#cvss.baseSeverity == 'Medium'}  {cvss.baseSeverity} |  | {title}  {/cvss.baseSeverity == 'Medium'}{/findings} |
| {@cvss.cellColor}  {#findings}{#cvss.baseSeverity == 'Low'}  {cvss.baseSeverity} |  | {title}  {/cvss.baseSeverity == 'Low'}{/findings} |
| {@cvss.cellColor}  {#findings}{#cvss.baseSeverity == 'None'}  {cvss.baseSeverity} |  | {title}  {/cvss.baseSeverity == 'None'}{/findings} |

# Technical Details

{#findings}

## {title}

|  |  |
| --- | --- |
| Severity | {@cvss.cellColor}  {cvss.baseSeverity} |
| **Affected scope** | {@affected | convertHTML} |
| **Description** | {#description}  {@text | convertHTML}  {#images}  {%image}  Image 1 – {caption}  {/images}  {/description} |
| **Observation** | {#observation}  {@text | convertHTML}  {#images}  {%image}  Image 1 – {caption}  {/images}  {/observation} |
| **Remediation** | {#remediation}  {@text | convertHTML}  {#images}  {%image}  Image 1 – {caption}  {/images}  {/remediation} |
| **References** | {#references}  {.}  {/references} |

{/findings}