|  |
| --- |
| {company.name} |
| Vulnerability Report |
| {date | convertDateLocale: 'en': 'full'} |

{%company.logo}

modifications history

| **Version** | **Date** | **Author** | **Description** |
| --- | --- | --- | --- |
| 1.0 | {date | convertDateLocale} | {creator.firstname} {creator.lastname} | Initial Version |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[General Information 4](#_TOC000008)

[Scope 4](#_TOC000009)

[Organisation 4](#_TOC000010)

[Executive Summary 5](#_TOC000011)

[Vulnerabilities summary 6](#_TOC000012)

[Technical Details 7](#_TOC000013)

[title 7](#_Toc29853419)

# General Information

## Scope

{company.name} has mandated [YOUR Company] to perform security tests on the following scope:

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

## Organisation

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

# Executive Summary

In response to the request for a security assessment, a comprehensive penetration test was conducted on {company.name}'s network and systems. The primary objective of this test was to evaluate the organization's security posture and identify vulnerabilities that could potentially be exploited by malicious actors.

The assessment encompassed an in-depth analysis of both internal and external systems, aiming to simulate real-world attack scenarios. Throughout the testing process, the focus remained on uncovering vulnerabilities that could lead to unauthorized access, data breaches, or service disruptions. The engagement was conducted following industry best practices and ethical guidelines.

The results of the penetration test highlight critical findings that demand immediate attention. These vulnerabilities, if left unaddressed, could compromise the confidentiality, integrity, and availability of the organization's sensitive information and assets. It is recommended that {company.name} takes swift action to remediate these issues to mitigate the associated risks.

Additionally, the penetration test revealed a number of high and medium-severity vulnerabilities that should be addressed promptly to enhance the overall security posture. The report provides detailed descriptions of each vulnerability, along with risk assessments and potential impact scenarios. This information will facilitate informed decision-making for the allocation of resources to remediation efforts.

It's worth noting that the organization's existing security measures demonstrated resilience against a variety of simulated attacks. This indicates a foundation of good security practices and highlights areas where strengths lie. However, as the threat landscape continues to evolve, ongoing security assessments and improvements are crucial to maintaining a robust defense against emerging threats.

The comprehensive penetration test report provides an overview of the assessment process, key findings, and actionable recommendations for mitigating the identified vulnerabilities. The insights gained from this assessment will empower the organization to prioritize security enhancements, allocate resources efficiently, and ensure the protection of critical assets.

The success of this engagement lies not only in identifying vulnerabilities but in catalyzing proactive measures to strengthen the organization's security posture. By addressing the identified vulnerabilities and adopting a proactive security stance, {company.name} will be better equipped to safeguard its digital assets and maintain the trust of its stakeholders.

For a detailed breakdown of findings, risk assessments, and recommended remediation steps, please refer to the following section.

# Vulnerabilities summary

Following vulnerabilities have been discovered:

|  |  |  |
| --- | --- | --- |
| **Risk** | **ID** | **Vulnerability** |
| {#findings}{#cvss.baseSeverity == 'Critical'}{cvss.baseSeverity} | {identifier} | {title} {/cvss.baseSeverity == 'Critical'}{/findings} |
| {#findings}{#cvss.baseSeverity == 'High'}{cvss.baseSeverity} | {identifier} | {title} {/cvss.baseSeverity == 'High'}{/findings} |
| {#findings}{#cvss.baseSeverity == 'Medium'}{cvss.baseSeverity} | {identifier} | {title} {/cvss.baseSeverity == 'Medium'}{/findings} |
| {#findings}{#cvss.baseSeverity == 'Low'}{cvss.baseSeverity} | {identifier} | {title} {/cvss.baseSeverity == 'Low'}{/findings} |
| {#findings}{#cvss.baseSeverity == ''}{cvss.baseSeverity} | {identifier} | {title} {/cvss.baseSeverity == ''}{/findings} |

# Technical Details

{#findings}

## {title}

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CVSS Severity** | **{@cvss.cellColor}**  **{cvss.baseSeverity}** | | **CVSSv3 Score** | | **{@cvss.cellColor}**  **{cvss.baseMetricScore}** |
| **CVSSv3 criterias** | Attack Vector : | **{cvssObj.AV}** | Scope : | **{cvssObj.S}** | |
| Attack Complexity : | **{cvssObj.AC}** | Confidentiality : | **{cvssObj.C}** | |
| Required Privileges : | **{cvssObj.PR}** | Integrity : | **{cvssObj.I}** | |
| User Interaction : | **{cvssObj.UI}** | Availability : | **{cvssObj.A}** | |
| **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} | | | | |
| **Test details**  {#poc}  {@text | convertHTML}  {#images}  {%image}  Image 1 – {caption}  {/images}  {/poc} | | | | | |
| **Remediation** | {#remediation}  {@text | convertHTML}  {#images}  {%image}  Image 1 – {caption}  {/images}  {/remediation} | | | | |
| **References** | {#references | loopObject}  {@value | linkTo: value | p}  {/} | | | | |

{/findings}