

Created By: {{settings.ORG}}

Prepared By: {{project.owner.full\_name}}

Generated on: {{ currentdate.strftime('%B %d, %Y') }}

**{{project.testingtype}} {{project.projecttype}} {{Report\_type}} Report Of {{project.name}} For {{project.companyname.name}}**

**Table Of Content**

[Executive Summary 3](#_Toc24486)

[Vulnerabilities Summary 3](#_Toc11973)

Executive Summary

The pentest was conducted by {{ settings.ORG }} on {{ project.name }} using the {{ standard|join(', ') }} standards to identify vulnerabilities exploitable by attackers. The testing methodology encompassed both manual and automated techniques, evaluating the application's security posture. During the assessment, a total of {{ totalvulnerability }} vulnerabilities were identified, varying in severity from Critical to Informational. Based on the pentest results, it is strongly advised to address these identified vulnerabilities promptly, enhancing the service's overall security posture. Overall, the pentest revealed several vulnerabilities exploitable by attackers, posing risks to the confidentiality, integrity, or availability of the application and underlying systems. Immediate action is recommended by the organization to mitigate these vulnerabilities and diminish the risk of successful attacks.

## Project Detail

{{project.description}}

## Document Version

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Start Date | End Date | Prepared By |
| 1.0 | {{ project.startdate.strftime("%d/%m/%Y") }} | {{ project.enddate.strftime("%d/%m/%Y") }} | {{ project.owner.full\_name }} |
| {% if Report\_type == 'Re-Audit' %}  {% if totalretest %}  {%tr for retest in totalretest %} | | | |
| 1.{{loop.index}} | {{ retest .startdate.strftime("%d/%m/%Y") }} | {{ retest .enddate.strftime("%d/%m/%Y") }} | {{ retest.owner.full\_name}} |
| {%tr endfor %}  {% endif %}  {% endif %} | | | |

## Project Scope

|  |  |  |
| --- | --- | --- |
| SR | Scope | Description |
| {%tr for scope in projectscope %} | | |
| {{loop.index}} | {{ scope.scope }} | {{ scope.description }} |
| {%tr endfor %} | | |

## {{settings.ORG}} Team

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SR | Name | Email | Number | Position |
| {%tr for user in internalusers %} | | |  |  |
| {{loop.index}} | {{user.full\_name }} | {{ user.email }} | {{ user.number }} | {{ user.position }} |
| {%tr endfor %} | | |  |  |

Vulnerabilities Summary

## Severity Classification

|  |  |  |  |
| --- | --- | --- | --- |
| SR | Vulnerability Name | Severity | Status |
| {%tr for vulnerability in vulnerabilities %} | | |  |
| {{loop.index}} | {{ vulnerability.vulnerabilityname }} | {% if vulnerability.vulnerabilityseverity == ‘Critical’ %}  {{ vulnerability.vulnerabilityseverity  }}  {% elif  vulnerability.vulnerabilityseverity  == ‘High' %}  {{ vulnerability.vulnerabilityseverity  }}  {% elif  vulnerability.vulnerabilityseverity  == ‘Medium' %}  {{ vulnerability.vulnerabilityseverity  }}  {% elif  vulnerability.vulnerabilityseverity  == ‘Low' %}  {{ vulnerability.vulnerabilityseverity  }}  {% elif  vulnerability.vulnerabilityseverity  == 'None' %}  {{ vulnerability.vulnerabilityseverity }}  {% endif %} | {% if vulnerability.status== 'Vulnerable' %}{{ vulnerability.status }}{% elif vulnerability.status == 'Confirm Fixed' %}{{ vulnerability.status }}{% elif vulnerability.status == 'Accepted Risk' %}{{ vulnerability.status }}{% endif %} |
| {%tr endfor %} | | |  |

Vulnerability Details

{% for vulnerability in vulnerabilities %}

**{{vulnerability.vulnerabilityname}}**

|  |  |
| --- | --- |
| **Severity** | {% if vulnerability.vulnerabilityseverity == ‘Critical’ %}{{ vulnerability.vulnerabilityseverity  }}{% elif  vulnerability.vulnerabilityseverity  == ‘High' %}{{ vulnerability.vulnerabilityseverity  }}{% elif  vulnerability.vulnerabilityseverity  == ‘Medium' %}  {{ vulnerability.vulnerabilityseverity  }}  {% elif  vulnerability.vulnerabilityseverity  == ‘Low' %}  {{ vulnerability.vulnerabilityseverity  }}  {% elif  vulnerability.vulnerabilityseverity  == 'None' %}  {{ vulnerability.vulnerabilityseverity }}  {% endif %} |
| **Status** | {% if vulnerability.status== 'Vulnerable' %}{{ vulnerability.status }}{% elif vulnerability.status == 'Confirm Fixed' %}{{ vulnerability.status }}{% elif vulnerability.status == 'Accepted Risk' %}{{ vulnerability.status }}{% endif %} |
| **CVSS Score** | {% if vulnerability.vulnerabilityseverity == ‘Critical’ %}{{ vulnerability.cvssscore}}{% elif  vulnerability.vulnerabilityseverity  == ‘High' %}{{ vulnerability.cvssscore}}{% elif  vulnerability.vulnerabilityseverity  == ‘Medium' %}{{ vulnerability.cvssscore}}{% elif  vulnerability.vulnerabilityseverity  == ‘Low' %}{{ vulnerability.cvssscore}}{% elif  vulnerability.vulnerabilityseverity  == 'None' %}{{ vulnerability.cvssscore}}  {% endif %} |
| **CVSS Vector** | {{vulnerability.cvssvector}} |

## Description

{{p vulnerability .vulnerabilitydescription }}

## POC

{{p vulnerability .POC}}

{% endfor %}