

Created By: {{mycomany}}

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

[3](#__RefHeading___Toc4368_675183759)

[Executive Summary 4](#__RefHeading___Toc4400_675183759)

[Project Detail 4](#__RefHeading___Toc4370_675183759)

[Project Detail 4](#__RefHeading___Toc4370_675183759)

[Document Version 5](#__RefHeading___Toc4372_675183759)

[Document Version 5](#__RefHeading___Toc4372_675183759)

[5](#__RefHeading___Toc4374_675183759)

[5](#__RefHeading___Toc4374_675183759)

[5](#__RefHeading___Toc4376_675183759)

[5](#__RefHeading___Toc4376_675183759)

[Project Scope 5](#__RefHeading___Toc4378_675183759)

[Project Scope 5](#__RefHeading___Toc4378_675183759)

[{{mycomany}} Team 6](#__RefHeading___Toc4380_675183759)

[{{mycomany}} Team 6](#__RefHeading___Toc4380_675183759)

[8](#__RefHeading___Toc4382_675183759)

[8](#__RefHeading___Toc4382_675183759)

[Severity Classification 10](#__RefHeading___Toc4384_675183759)

[Severity Classification 10](#__RefHeading___Toc4384_675183759)

[Vulnerability Details 11](#__RefHeading___Toc4398_675183759)

[11](#__RefHeading___Toc4396_675183759)

[Description 11](#__RefHeading___Toc4386_675183759)

[Description 11](#__RefHeading___Toc4386_675183759)

[POC 11](#__RefHeading___Toc4388_675183759)

[POC 11](#__RefHeading___Toc4388_675183759)

[Recommendations 12](#__RefHeading___Toc4390_675183759)

[Recommendations 12](#__RefHeading___Toc4390_675183759)

[Instances 12](#__RefHeading___Toc4392_675183759)

[Instances 12](#__RefHeading___Toc4392_675183759)

[References 12](#__RefHeading___Toc4394_675183759)

[References 12](#__RefHeading___Toc4394_675183759)

The pentest was conducted by {{mycomany}} 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

{{ p 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") }} | {% for owner in owners -%}  {{ owner.full\_name + '\n' }}  {%- endfor %} |
| {% 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") }} | {% for owner in retest.owners -%}  {{ owner + '\n' }}  {%- endfor %} |
| {%tr endfor %}  {% endif %}  {% endif %} | | | |

## 

## 

## Project Scope

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

## {{mycomany}} Team

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name | Email | Number | | Role | |
| {%tr for user in projectmanagers %} | | | | | |
| {{ user.full\_name }} | {{ user.email }} | {{ user.number }} | | {{ user.position }} | |
| {%tr endfor %} | | | | | |
| {%tr for owner in owners %} | | | | | |
| {{ owner.full\_name }} | {{ owner.email }} | | {{ owner.number }} | | {{ owner.position }} |
| {%tr endfor %} | | | | | |

## {{project.companyname.name}} Team

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Email | Number | Role |
| {%tr for user in customeruser %} | | | |
| {{ user.full\_name }} | {{ user.email }} | {{ user.number }} | {{ user.position }} |
| {%tr endfor %} | | | |

## 

## 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 %} | | | |

{% for vulnerability in vulnerabilities %}**{{vulnerability.vulnerabilityname}}**

|  |  |
| --- | --- |
| **Severity** | **{% cellbg 'FF491C' if vulnerability.vulnerabilityseverity== 'Critical' else 'F66E09' if vulnerability.vulnerabilityseverity== 'High' else 'FBBC02' if vulnerability.vulnerabilityseverity== 'Medium' else '20B803' if vulnerability.vulnerabilityseverity== 'Low' else '3399FF' %}{{ vulnerability.vulnerabilityseverity}}** |
| **Status** | **{% cellbg 'FF0000' if vulnerability.status== 'Vulnerable' else '20B803' if vulnerability.status== 'Confirm Fixed' else 'FFA500' %}{{ vulnerability.status}}** |
| **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}}

## Recommendations

{{p vulnerability.vulnerabilitysolution}}

## Instances

|  |  |  |
| --- | --- | --- |
| **URL** | **Parameter** | **Status** |
| {%tr for instance in vulnerability.instances\_data %} | | |
| **{{ instance.URL }}** | **{{ instance.Parameter }}** | **{% cellbg 'FF0000' if instance.Status== 'Vulnerable' else '20B803' if instance.Status== 'Confirm Fixed' else 'FFA500' %}{{ instance.Status}}** |
| {%tr endfor %} | | |

## References

{{p vulnerability.vulnerabilityreferlnk}}

{% if not loop.last %}{{r page\_break}}{% endif %}

{% endfor %}