Background pattern

Description automatically generated**{{project.name}} for**

**{{project.companyname.name}}**

## 

## 

|  |  |
| --- | --- |
| **Presented By:**  **M2P Fintech**  Plot No C1 & C56, Olympia Quest,  SIDCO, Thiru Vi Ka Industrial Estate,  Guindy, Chennai- 600032,  Tamil Nadu, India. | **Presented to:**  **{{project.companyname.name}}**  **{{project.companyname.address}}** |

**Disclaimer:**

This document contains confidential and proprietary information. Unauthorized use or reproduction of this document is prohibited.

**{{project.projecttype}} for {{project.companyname.name}}**

**Warning:** **THIS DOCUMENT, ALONG WITH ALL ACCOMPANYING MATERIALS, MAY CONTAIN INFORMATION THAT COULD SEVERELY DAMAGE OR IMPACT THE INTEGRITY AND SECURITY OF THE ORGANIZATION IF DISCLOSED PUBLICLY. THIS DOCUMENT, ALONG WITH ALL ACCOMPANYING MATERIALS, SHOULD BE SAFEGUARDED AT ALL TIMES AND MAINTAINED IN A SECURE LOCATION WHEN NOT IN USE. {{MYCOMPANY}} ASSUMES NO RESPONSIBILITY OR LIABILITY FOR THE SECURITY OF THIS DOCUMENT OR ANY ACCOMPANYING MATERIALS AFTER DELIVERY TO THE PRESENTED ORGANIZATION. IT IS THE PRESENTED ORGANIZATION’S RESPONSIBILITY TO SAFEGUARD THIS MATERIAL AFTER DELIVERY.**

**This report contains proprietary information that must not be shared, copied, disclosed, or otherwise divulged without the express written consent of {{MYCOMPANY}} or their designated representative. Use of this reporting format by anyone other than {{MYCOMPANY}} or its subsidiaries is strictly prohibited.**

**Disclaimer: The recommendations contained in this report are based on industry standard best practices. Best practices are, by necessity, generic in nature and may not consider specific exacerbating or mitigating circumstances. These recommendations, even if correctly applied, may cause conflicts in the operating system or installed applications. Any recommended changes to the operating system or installed applications should first be evaluated in a non-production environment before being deployed in your production network.**

**Table of Contents**

[2](#__RefHeading___Toc1653_1338118478)

[Project Detail 3](#__RefHeading___Toc1655_1338118478)

[Document Version 3](#__RefHeading___Toc1657_1338118478)

[Project Scope 4](#__RefHeading___Toc1659_1338118478)

[5](#__RefHeading___Toc1661_1338118478)

[{{mycomany}} Team 5](#__RefHeading___Toc1663_1338118478)

[{{project.companyname.name}} Team 5](#__RefHeading___Toc1665_1338118478)

[Project Exception 7](#__RefHeading___Toc1667_1338118478)

The penetration test conducted by {{mycompany}} on {{project.name}} employed the {{standard|join(', ')}} standards to identify vulnerabilities exploitable by attackers. The testing methodology encompassed both manual and automated techniques to evaluate the application's security posture. During the assessment, a total of {{totalvulnerability}} vulnerabilities were identified, with severities ranging from Critical to Informational.

Based on the penetration test results, it is strongly advised that these identified vulnerabilities be addressed promptly to enhance the service's overall security posture. The test revealed several vulnerabilities that could be exploited by attackers, thereby posing risks to the confidentiality, integrity, or availability of the application and underlying systems. Immediate action is recommended to mitigate these vulnerabilities and reduce the risk of successful attacks.

**Project Objectives:**

**{{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 != 'Audit' %} | | | | | |
| {%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 %} | | | | | |

**Scope:**

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

**{{mycompany}} 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 %} | | | |

{% if project.projectexception %}

**Project Exception:**

{{p project\_exception}}

{% endif %}

**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 }}  {% else %}  Informational  {% 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}}**

|  |  |
| --- | --- |
| **CVSS Score{{r new\_line}}{% if vulnerability.vulnerabilityseverity == 'Critical' %}{{ vulnerability. cvssscore}}{% elif vulnerability.vulnerabilityseverity == 'High' %}{{ vulnerability. cvssscore}}{% elif vulnerability.vulnerabilityseverity == 'Medium' %}{{ vulnerability. cvssscore}}{% elif vulnerability.vulnerabilityseverity == 'Low' %}{{ vulnerability. cvssscore}}{% else %}{{ vulnerability. cvssscore}}{% endif %}** | **Status{{r new\_line}}{% if vulnerability.status == 'Vulnerable' %}{{ vulnerability.status }}{% elif vulnerability.status == 'Confirm Fixed' %}{{ vulnerability.status }}{% elif vulnerability.status == 'Accepted Risk' %}{{ vulnerability.status }}{% endif %}** |
| **Severity{{r new\_line}}{% if vulnerability.vulnerabilityseverity == 'Critical' %}{{ vulnerability. vulnerabilityseverity }}{% elif vulnerability.vulnerabilityseverity == 'High' %}{{ vulnerability. vulnerabilityseverity }}{% elif vulnerability.vulnerabilityseverity == 'Medium' %}{{ vulnerability. vulnerabilityseverity }}{% elif vulnerability.vulnerabilityseverity == 'Low' %}{{ vulnerability. vulnerabilityseverity }}{% else %}{{ vulnerability. vulnerabilityseverity }}{% endif %}** | **CVSS Vector{{r new\_line}}{{vulnerability.cvssvector}}** |

{% if vulnerability.cwe %}

**CWE**

{% for cwe\_item in vulnerability.cwe %}

* {{ cwe\_item }}

{%- endfor %}

{% endif %}

**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 }} | {% if instance.Status == 'Vulnerable' %}{{ instance.Status }}{% elif instance.Status == 'Confirm Fixed' %}{{ instance.Status }}{% elif instance.Status == 'Accepted Risk' %}{{ instance.Status }}{% endif %} |
| {%tr endfor %} | | |

**References**

{{p vulnerability.vulnerabilityreferlnk}}

{% if not loop.last %}

{{r page\_break}}

{% endif %}

{% endfor %}