**XXX Company**

Report on the Provision of Penetration Test Service for {{task\_name}} {{component}}

{{today}}

# Executive Summary

## Introduction

We, Information security management (hereinafter known as “ISM”), have completed the Penetration Test Services (“the Assessment”) for {**{task\_name}}** in accordance with our statement of work. Our assessment was performed in {{start\_month}} {{start\_year}} and follow-up verification was not completed at the time of report issuance.

The objective of the Assessment was to identify technical security weaknesses on the applications and systems in the XXX’s networks. Practical recommendations were subsequently provided to assist XXX in addressing the identified gaps.

During the course of the work, we have discussed our findings and recommendations with the XXX IT team.

## Key Findings

From the assessment, we have identified a total of **{{total\_vulnerabilities}}** Issues. Our findings are summarized below and the detailed findings can be found in **Appendix A**. We have discussed our findings with the relevant XXX staff and their comments are incorporated into this report.

## Summary of Findings

The total number of findings and their associated risk ratings are summarised below.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Area of Work** | **Risk Rating** | | | | | **Total** |
| Critical | High | Medium | Low | Recommend |
| **{{task\_name}}** {{component}} Penetration Testing | **{{count\_critical}}** | **{{count\_high}}** | **{{count\_medium}}** | **{{count\_low}}** | **{{count\_recommend}}** | **{{total\_vulnerabilities}}** |
| **Total** | **{{count\_critical}}** | **{{count\_high}}** | **{{count\_medium}}** | **{{count\_low}}** | **{{count\_recommend}}** | **{{total\_vulnerabilities}}** |

The descriptions of the risk ratings are as follows:

|  |  |
| --- | --- |
| **Risk Rating** | **Description** |
|
| **Critical** | The item mentioned is a requirement to be followed as it has a significant impact to controls, finance or operations. We highly recommend that it be complied with and addressed immediately. |
| **High** | The item mentioned is a requirement to be followed as it has a significant impact to controls, finance or operations. We highly recommend that it be complied with and addressed immediately. |
| **Medium** | The item mentioned may be a requirement based on regulatory requirements and / or industry good practices, and has a moderate impact on controls, finance or operations. Compensating controls should be put in place if they are not implemented. |
| **Low** | The item mentioned has a low impact to controls, finance or operations if left uncorrected, but should be followed-up and evaluated as an opportunity for improvement. |
| **Recommend** | The item mentioned will ensure the application more safety and secure |

|  |  |
| --- | --- |
| **Area of Work** | **Work Performed** |
|
| {{task\_name}} {{component}} Penetration Test | We have tested the application in UAT environment using both automated and manual approach. The scope of the assessment was limited to the following URLs:  {{ environment\_test }} |

|  |  |  |  |
| --- | --- | --- | --- |
| **Ref.** | **Issue Description** | **Risk Rating** | **Status** |
| Application Penetration Testing on {{task\_name}}{% for vuln in vulnerabilities %} | | | |
| {{vuln.ref}} | {{vuln.name\_vuln}} | **{{vuln.risk\_rating}}** | {{vuln.status}}{% endfor %} |

{% if scope %}

Scope List:

{% for row in scope %}

- {{ row.No }}. {{ row.API }}

{% endfor %}

{% else %}

Scope is not provided.

{% endif %}

{% if scope %}

|  |  |
| --- | --- |
| **No** | **API**{% for row in scope %} |
| {{row.No}} | {{row.API}} {% endfor %} |

{% else %}

Scope is not provided.

{% endif %}

{%if vulnerabilities %}

{% for vuln in vulnerabilities %}

1. {{vuln.name\_vuln}}

|  |  |
| --- | --- |
| **Title: {{vuln.name\_vuln}}**  **Component: {{component}}** | **Ref:**  **{{vuln.ref}}** |
| **Risk assessment score (CVSS v3.1)**  SCORE:  **{{vuln.risk\_score}}**  VECTOR: {{vuln.risk\_vector}} | **Risk Rating:**  **{{vuln.risk\_rating}}** |
| **Description**  {{vuln.description}}  **Likelihood:** **{{vuln.likelihood\_rate}}**  Attack Vector (AV): {{vuln.risk\_av}}  Attack Complexity (AC): {{vuln.risk\_ac}}  Privileges Required (PR): {{vuln.risk\_pr}}  User Interaction (UI): {{vuln.risk\_ui}}  **Impact: {{vuln.impact\_rate}}**  {{vuln.impact}} | |
| **Evidence**  {% for item in vuln.evidence\_parts %}{% if item.type == 'text' %}{{ item.content }}{% elif item.type == 'image' %}  {{ item.content }}  {% endif %}{% endfor %} | |
| **Affected URL**{%if vuln.affected\_url\_list %}{% for url in vuln.affected\_url\_list %}  - {{ url }}{% endfor %} {% else %}No VULN API{% endif %} | |
| **Recommendations**  {{vuln.recommendation}} | |
| **References**  {{vuln.reference}} | |
| **ISM Follow-up**  Status: {{vuln.status}} | |

{% endfor%}

{% else %}

NO VULN

{% endif %}