**{{company\_name}}**

**Security Assessment Report**

Client: **{{client\_name}}**

Project Name: **{{[project\_name}}**

Date: **{{date}}**

**TABLE OF CONTENTS**

1. **EXECUTIVE SUMMARY**
   1. **ASSESSMENT OVERVIEW**
   2. **RISK SUMMARY**
   3. **CONCLUSIONS & RECOMMENDATIONS**
2. **TESTING METHODOLOGY**
   1. **SUMMARY**
3. **TECHNICAL SUMMARY**
   1. **RESULTS SUMMARY**
   2. **RESULTS ASSESSMENT**
4. **ASSESSMENT RESULTS**
5. **CONCLUSION**

**FURTHER DETAILS AND EXAMPLES**

**1. Executive Summary**

**1.1 Assessment Overview**

{{company\_name}} begun a discovery process on {{audit\_start\_date}}. On the {{contract\_start\_date}}, {{client\_name}} authorised {{company\_name}} to conduct a {{brief\_scope\_details}}.

The assessment involved both a technical assessment and documentary addition. The report was requested by {{client\_name}} in its entirety, identifying security concerns and define a scope for purposes of the executed contract.

This report covers {{report\_cover\_detials}}, it does not include any information pertaining to unattached entities (third party) and otherwise, whom handle or may handle the {{client\_name}}s information unless already authorised to do so.

The disclosure made available to {{client\_name}} may contain information released **in-confidence** for the purpose of identifying and securing {{client\_nam}}’s systems.

{{company\_name}} identifies the scope as {{scope}}.

{{client\_name}} engaged the services of {{company\_name}} to:

* Conduct a penetration test on {{client\_name}} systems.
* Identify and mitigate any risks associated with {{client\_name}}
* Provide a detailed write up provided in the consultant’s report for the scopes identified.

The report provided is an output of the assessment performed and should be used as input in investigating and auditing a larger risk mitigation process.

The results provided are a point in time assessment of the systems and environment as they were present at the time of initial discovery. Any changes made since could impact this report.

**The purpose of the audit is to assist in securing services, systems and intellectual property owned, stored and processed by {{client\_name}}, and its subsidiaries.**

**1.2 About {{company\_name}}**

{{about\_company}}

**1.3 Risk Summary**

The overall security risk rating was calculated as: **{{highest\_risk}}.**

This rating was attributed to the result of the highest critical finding discovered during the assessment. Details regarding this are presented in this report.

More statistics based on findings:

|  |  |  |
| --- | --- | --- |
| **{{Critical}}**  Critical | **{{High}}**  High | **{{Medium}}**  Medium |
| **{{Low}}**  Low | **{{Informational}}**  Informational | **{{Total}}**  Total |

**1.4 Conclusions and Recommendations**

{{conclusion\_and\_recommendations}}

**2. Testing Methodology**

**2.1 Summary**

{{methodogy\_summary}

**3. Technical Summary**

**3.1 Results Summary**

{{result\_summary}}

The highest risk rating was classified as **{{highest\_risk}}**.

**3.2 Results Assessment**

|  |  |  |  |
| --- | --- | --- | --- |
| **Category** | **Risk** | **Summary** | **Recommendations** |
| {{category}} | **{{risk}}** | {{summary}} |  |
|  | **{{risk}}** |  |  |
| {{category}} | **{{risk}}** |  |  |

**4. Assessment Results**

**4.1 {{title}}**

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **Title** | **{{title}}** |  |
| **Risk Rating**   |  | | --- | | **{{RISK}}** | | **CVSS3**   |  | | --- | | **{{CVSS3}}** | | **CVE**   |  | | --- | | {{CVE}} | |

|  |  |  |
| --- | --- | --- |
| **Technical Overview**   |  | | --- | | {{technical\_overview}} | |  |
| **Attack Conditions**   |  | | --- | | {{attack\_conditions}} | |  |
| **Business Impact**   |  | | --- | | {{business\_impact}} | |  |
| **Recommendations**   |  | | --- | | {{recommendations}} | |  |
| **Attack Example**   |  | | --- | | {{attack\_example}} | |  |

**5. Conclusion**

{{report\_conclusion}}

**Further Details and Examples**

**Descriptive**

**Risk Rating System - CVSS3**

The Common Vulnerability Scoring System (version 3.1);

During an assessment only the base metric group is calculated for each vulnerability.

For further information on the CVSS3, see the following reference:

* https://www.first.org/cvss/user-guide

**Our Qualitative Rating Scale**

The Qualitative Rating Scale used by {{company\_name}} follows {{guidelines}}