Threat Track – Pretesting Report

{{name}}

{{client.name}}

Report Issued: {{end\_date}}

{{client.logo}}

# Confidentiality Notice

*This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage to {{client.name}} or facilitate attacks against {{client.name}}. Threat Track shall not be held liable for special, incidental, collateral or consequential damages arising out of the use of this information.*

# Disclaimer

*Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a “point-in-time” assessment made on {{client.name}}’s environment. Any changes made to the environment during the period of testing may affect the results of the assessment.*

**TABLE OF CONTENTS**

[Confidentiality Notice 2](#_Toc142682758)

[Disclaimer 2](#_Toc142682759)

[EXECUTIVE SUMMARY 4](#_Toc142682760)

[SCOPE 5](#_Toc142682761)

[Provided Credentials 5](#_Toc142682762)

[TESTING METHODOLOGY 6](#_Toc142682763)

[CLASSIFICATION DEFINITIONS 7](#_Toc142682764)

[Risk Classifications 7](#_Toc142682765)

[APPENDIX B - ENGAGEMENT INFORMATION 9](#_Toc142682766)

[Client Information 9](#_Toc142682767)

[Version Information 9](#_Toc142682768)

# EXECUTIVE SUMMARY

{{ s\_fields.Summary }}

|  |  |  |  |
| --- | --- | --- | --- |
| **CRITICAL** | **HIGH** | **MEDIUM** | **LOW** |
| **{{vulnerabilities|count\_risk\_rating('Critical')}}** | **{{vulnerabilities|count\_risk\_rating('High')}}** | **{{vulnerabilities|count\_risk\_rating('medium')}}** | **{{vulnerabilities|count\_risk\_rating('low')}}** |

Extra notes:

In order to ensure data confidentiality, integrity, and availability, security remediations should be implemented as described in the security assessment findings.

{{ s\_fields.Notes }}

# SCOPE

{{ s\_fields.Scope }}

## Provided Credentials

{{client.name}} provided our team with the following credentials and access to facilitate the security assessment listed below.

# ASSESSMENT FINDINGS

|  |  |  |  |
| --- | --- | --- | --- |
| **Number** | **Finding** | **Risk Score** | **Risk** |
| **{%tr for vuln in vulnerabilities|sort\_cvss() %}** | | | |
| {{vuln.number}} | {{vuln.name}} | {% cellbg '93c47d' if vuln.risk\_rating == 'Low' else  'ffd966' if vuln.risk\_rating == 'Medium' else  'e06666' if vuln.risk\_rating == 'High' else  'ffffff' %}**{{vuln.cvss}}** | {% cellbg '93c47d' if vuln.risk\_rating == 'Low' else  'ffd966' if vuln.risk\_rating == 'Medium' else  'e06666' if vuln.risk\_rating == 'High' else  'ffffff' %}{{vuln.risk\_rating }} |
| **{%tr endfor %}** | | | |

{% for vuln in vulnerabilities|sort\_cvss() %}

### {{vuln.number}} – {{vuln.name}}

|  |
| --- |
| **{% cellbg '93c47d' if vuln.risk\_rating == 'Low' else**  **'ffd966' if vuln.risk\_rating == 'Medium' else**  **'e06666' if vuln.risk\_rating == 'High' else**  **'ffffff' %}{{vuln.risk\_rating }}({{vuln.cvss}}/10)** |

**{% if vuln.target %}System Vulnerable: {{vuln.target}}{% endif %}**

**Security Implications**

{{vuln.description}}

**Impact**

{{vuln.impact}}

**Recommendations**

{{vuln.remediation}}

**Proof of Concept**

{{vuln.poc\_text}}

**Reference**

{{ vuln.fields.Reference }}

{% if not loop.last %}{{'\f'}}{% endif %}{% endfor %}

# TESTING METHODOLOGY

Our testing methodology was split into three phases: *Reconnaissance*, *Target Assessment*, and *Execution of Vulnerabilities*. During reconnaissance, we gathered information about network systems. We used port scanning and other enumeration methods to refine target information and assess target values. Next, we conducted our targeted assessment. we simulated an attacker exploiting vulnerabilities in the {{client.name}} network. We gathered evidence of vulnerabilities during this phase of the engagement while conducting the simulation in a manner that would not disrupt normal business operations.

The following image is a graphical representation of this methodology.

# CLASSIFICATION DEFINITIONS

## Risk Classifications

|  |  |  |
| --- | --- | --- |
| **Level** | **Score** | **Description** |
| **Critical** | **10** | The vulnerability poses an immediate threat to the organization. Successful exploitation may permanently affect the organization. Remediation should be immediately performed. |
| **High** | **7-9** | The vulnerability poses an urgent threat to the organization, and remediation should be prioritized. |
| **Medium** | **4-6** | Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible. |
| **Low** | **1-3** | The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible. |
| **Informational** | **0** | These findings have no clear threat to the organization, but may cause business processes to function differently than desired or reveal sensitive information about the company. |

APPENDIX A - TOOLS USED

|  |  |
| --- | --- |
| **TOOL** | **DESCRIPTION** |
| **BurpSuite Community Edition** | Used for testing of web applications. |
| **Metasploit** | Used for exploitation of vulnerable services and vulnerability scanning. |
| **Nmap** | Used for scanning ports on hosts. |
| **OpenVAS** | Used to scan the networks for vulnerabilities. |
| **PostgreSQL Client Tools** | Used to connect to the PostgreSQL server. |

# APPENDIX B - ENGAGEMENT INFORMATION

## Client Information

|  |  |
| --- | --- |
| **Client** | {{client.name}} |
| **Primary Contact** |  |
| **Approvers** | The following people are authorized to change the scope of engagement and modify the terms of the engagement |

## Version Information

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Description** |
| 1.0 | {{expected\_end\_date}} | Initial report to client |