

Table of Contents

[1 Executive Summary 5](#_Toc179913815)

[1.1. Project Objective 5](#_Toc179913816)

[1.2. Scope & Timeframe 5](#_Toc179913817)

[1.3. User Accounts provided by Ephanti 6](#_Toc179913818)

[1.4. Summary of Business Risks 6](#_Toc179913819)

[1.5. Standards Followed 7](#_Toc179913820)

[2 Technical Details 8](#_Toc179913821)

[2.1 Methodology 8](#_Toc179913822)

[2.2 Terminology and score 8](#_Toc179913823)

[2.3 Security tools used 9](#_Toc179913824)

[3 Finding Details 10](#_Toc179913825)

[3.1 Summary of Findings 10](#_Toc179913826)

[3.2 Critical Severity Findings 10](#_Toc179913827)

[3.2.1 Vulnerability: Privilege Escalation 10](#_Toc179913828)

[3.2.2 Vulnerability: Session Hijacking 17](#_Toc179913829)

[3.3 High Severity Findings 20](#_Toc179913830)

[3.3.1 Vulnerability: Stored XSS 20](#_Toc179913831)

[3.3.2 Vulnerability: Server-Side Request Forgery (SSRF) 23](#_Toc179913832)

[3.3.3 Vulnerability: HTML Injection 27](#_Toc179913833)

[3.3.4 Vulnerability: Client-side URL Redirect 31](#_Toc179913834)

[3.3.5 Vulnerability: DOM XSS 33](#_Toc179913835)

[3.4 Medium Severity Findings 38](#_Toc179913836)

[3.4.1 Vulnerability: File Upload Vulnerability 38](#_Toc179913837)

[3.4.2 Vulnerability: Session Time-out 41](#_Toc179913838)

[3.4.3 Vulnerability: CSS Injection 44](#_Toc179913839)

[3.4.4 Vulnerability: Clickjacking 45](#_Toc179913840)

[3.4.5 Vulnerability: URL Redirection using XML Injection 48](#_Toc179913841)

[3.5 Low Severity Findings 51](#_Toc179913842)

[3.5.1 Vulnerability: Missing Security Headers 51](#_Toc179913843)

[3.5.2 Vulnerability: Protocol Downgrade Attack 53](#_Toc179913844)

[3.5.3 Vulnerability: Improper Error Handling 55](#_Toc179913845)

[3.5.4 Vulnerability: Leakage of Local Storage 57](#_Toc179913846)

[3.6 Security status according to OWASP Top 10 60](#_Toc179913847)

[4 Tests Performed 63](#_Toc179913848)

[5 Chatbot-MEVA testing details 68](#_Toc179913849)

[7 Conclusion 72](#_Toc179913850)

Document Name: Web application PEN Test Report –{{companyName}} Classification: Confidential

Reference: Web application PEN Test Report Version: {{ version }}

Date:

#### Document Confidentiality

This document contains sensitive information which needs to be shared with appropriate personnel of {{ companyName }} on a purely need to know basis. The following recommendations are issued with respect to distributing this document

* Distribute to authorized personnel only
* Comply with the appropriate security measures according to the classification level of the document

#### Version History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Author | Comment | Date |
| {{ version }} | {{ Author}} | {{ Comment }} | {{ Date}} |

# Executive Summary

## Project Objective

Our primary goal within this project was to provide the {{ companyName }} with an understanding of the current level of security in the web application and its infrastructure components. We completed the following objectives to accomplish this goal:

* + - Identifying application-based threats to and vulnerabilities in the application
    - Comparing {{ companyName }} current security measures with industry best practices
    - Providing recommendations that {{ companyName }} can implement to mitigate threats and vulnerabilities and meet industry best practices

## Scope & Timeframe

The section defines the scope and boundaries of the project.

#### Constraints and Limitations

The assessment was performed with the knowledge shared by the Company Onboarding team about the target. Pragya Cyber conducted the assessments, and the result(s) / finding(s) made are highly subjective to target system(s) and service(s) visibility and availability at that given point of time.

#### Target Scope

Identify weaknesses that might be exploited by adversaries who have authorized or unauthorized access to Company Technical Skill Test and underlying infrastructure:

* + Test access credentials were provided. It was a Grey-Box Testing.
  + The objective is to mimic an adversary and identify the threats and vulnerabilities.

Following application was in the scope of the penetration test. Automated as well as manual security testing was conducted

|  |  |  |
| --- | --- | --- |
| **Sr.no** | **Application Type** | **URL/IP/Domain** |
| {%tr for item in targetScopeTable %} | | |
| 1 | {{ item.applicationType }} | {{ item.address }} |
| {%tr endfor %} | | |

## User Accounts provided by {{companyName}}

|  |  |
| --- | --- |
| **URL/IP/API** | **Username** |
| {%tr for user in userDeatialTable%} | |
| {{ user.url }} | {{ user.username }} |
| {%tr endfor %} | |

## Summary of Business Risks

|  |  |
| --- | --- |
| **Vulnerability** | **Business Risk** |
| {%tr for item in summary %} | |
| {{item.vulnerability}} | {{item.risk}} |
| {%tr endfor %} | |

## Standards Followed

* OWASP
* OSSTMM
* PTES
* WASC-TC

# Technical Details

## Methodology

* + - [Penetration Testing Execution Standard (PTES)](http://www.pentest-standard.org/index.php/Main_Page)
    - [OWASP Top 10 Application Security Risks](https://owasp.org/www-project-top-ten/)
    - [OWASP Web Security Testing Guide](https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/)
    - [Open-Source Security Testing Methodology Manual (OSSTMM)](https://www.isecom.org/OSSTMM.3.pdf)
    - [Web Application Security Consortium Threat Classification (WASC-TC)](http://projects.webappsec.org/w/page/13246978/Threat%20Classification)

## Terminology and score

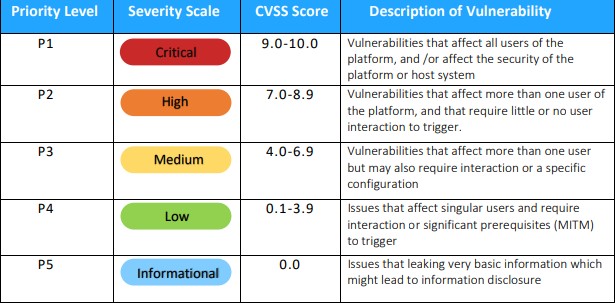
**CVE -** is a dictionary of publicly known information security vulnerabilities and exposures. CVE’s common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services. An information security "vulnerability" is a mistake in software application, configuration or operating system that can be directly used by a hacker to gain access to a system or network.

**Vulnerability -** A weakness which allows a hacker to break into / compromise a system's security.

**Exploit -** Code which allows an attacker to take advantage of a vulnerable system.

**Payload -** Actual code which runs on the system after exploitation.

**CWE -** Common Weakness Enumeration is a tangible set of software weaknesses that



## Security tools used

{% for item in securityTool %}

* {{ item.name }} : {{ item.desc }}

{% endfor %}

# Finding Details

## Summary of Findings

{{ pieChart.image }}

## Critical Severity Findings

{% for item in criticals %}

# 3.2.{{ loop.index }} Vulnerability: {{item.name}}

##### **Description**

{{item.desc}}

##### **Impact**

{% for impact in item.impacts %}

* **{{impact.name}}**: {{impact.desc}}

{% endfor %}

##### **CVSS Score**

* {{ item.cvssScore }}

##### **Severity**

* critical

##### **Mitigation**

{% for mitigation in item.mitigations %}

* **{{ mitigation.name }}**: {%for point in mitigation.desc %}
* {{point}}

{% endfor %}

{% endfor %}

{% if item.poc %}

##### **Proof Of Concept**

{% for poc in item.poc %}

{{ poc.image }}

{{ poc.name }}

{% for desc in poc.desc %}

* {{ desc }}

{% endfor %}

{%endfor %}

{% endif %}

##### **Evidence**

{% for evidence in item.evidences %}

{{ evidence.image }}

{{ evidence.name }}

{% for point in evidence.desc %}

* {{ point }}

{% endfor %}

**{{ evidence.extra }}**

{% endfor %}

{% endfor %}

## High Severity Findings

{% for item in highs %}

# 3.3.{{ loop.index }} Vulnerability: {{item.name}}

##### **Description**

{{item.desc}}

##### **Impact**

{% for impact in item.impacts %}

* **{{impact.name}}**: {{impact.desc}}

{% endfor %}

##### **CVSS Score**

* {{ item.cvssScore }}

##### **Severity**

* high

##### **Mitigation**

{% for mitigation in item.mitigations %}

* **{{ mitigation.name }}**: {%for point in mitigation.desc %}
* {{point}}

{% endfor %}

{% endfor %}

{% if item.poc %}

##### **Proof Of Concept**

{% for poc in item.poc %}

{{ poc.image }}

{{ poc.name }}

{% for desc in poc.desc %}

* {{ desc }}

{% endfor %}

{%endfor %}

{% endif %}

##### **Evidence**

{% for evidence in item.evidences %}

{{ evidence.image }}

{{ evidence.name }}

{% for point in evidence.desc %}

* {{ point }}

{% endfor %}

**{{ evidence.extra }}**

{% endfor %}

{% endfor %}

## Medium Severity Findings

{% for item in mediums %}

# 3.4.{{ loop.index }} Vulnerability: {{item.name}}

##### **Description**

{{item.desc}}

##### **Impact**

{% for impact in item.impacts %}

* **{{impact.name}}**: {{impact.desc}}

{% endfor %}

##### **CVSS Score**

* {{ item.cvssScore }}

##### **Severity**

* Medium

##### **Mitigation**

{% for mitigation in item.mitigations %}

* **{{ mitigation.name }}**: {%for point in mitigation.desc %}
* {{point}}

{% endfor %}

{% endfor %}

{% if item.poc %}

##### **Proof Of Concept**

{% for poc in item.poc %}

{{ poc.image }}

{{ poc.name }}

{% for desc in poc.desc %}

* {{ desc }}

{% endfor %}

{%endfor %}

{% endif %}

##### **Evidence**

{% for evidence in item.evidences %}

{{ evidence.image }}

{{ evidence.name }}

{% for point in evidence.desc %}

* {{ point }}

{% endfor %}

**{{ evidence.extra }}**

{% endfor %}

{% endfor %}

## Low Severity Findings

{% for item in lows %}

# 3.5.{{ loop.index }} Vulnerability: {{item.name}}

##### **Description**

{{item.desc}}

##### **Impact**

{% for impact in item.impacts %}

* **{{impact.name}}**: {{impact.desc}}

{% endfor %}

##### **CVSS Score**

* {{ item.cvssScore }}

##### **Severity**

* low

##### **Mitigation**

{% for mitigation in item.mitigations %}

* **{{ mitigation.name }}**: {%for point in mitigation.desc %}
* {{point}}

{% endfor %}

{% endfor %}

{% if item.poc %}

##### **Proof Of Concept**

{% for poc in item.poc %}

{{ poc.image }}

{{ poc.name }}

{% for desc in poc.desc %}

* {{ desc }}

{% endfor %}

{%endfor %}

{% endif %}

##### **Evidence**

{% for evidence in item.evidences %}

{{ evidence.image }}

{{ evidence.name }}

{% for point in evidence.desc %}

* {{ point }}

{% endfor %}

**{{ evidence.extra }}**

{% endfor %}

{% endfor %}

{% if web %}

## Security status according to OWASP Top 10

|  |  |  |  |
| --- | --- | --- | --- |
| **#** | **Vulnerability** | **Description** | **Status** |
| {%tr for item in vulnerabilities %} | | | |
| {{item.id}} | {{item.name}} | {{item.desc}} | {%if item.pass%}  **Pass**  {% if item.fail%}  **Fail**  {%else%}  **N/A**  {%endif%}  {%endif%} |
| {%tr endfor %} | | | |

{% endif %}

# Tests Performed

|  |  |  |  |
| --- | --- | --- | --- |
| **Test name** | **Pass** | **Fail** | **N/A** |
| {%tr for test in testPerfom %} | | | |
| **{{test.name}}** | | | |
| {%tr for item in test.step %} | | | |
| {{item.name}} | {% if item.pass %}  Yes  {%endif%} | {% if item.fail %}  Yes  {%endif%} | {% if item.noAns %}  Yes  {%endif%} |
| {%tr endfor %} | | | |
| {%tr endfor %} | | | |

{% if chatbot %}

# Chatbot-MEVA testing details

|  |  |
| --- | --- |
| Test Category | Status |
| {%tr for item in chatbotTest %} | |
| {{ item.name }} |  |
| {{ item.category }} | {{ item.status }} |
| {%tr endfor %} |  |

{% endif %}

{% if apiTest %}

API testing details  
**Sensitive Information Disclosure:**

{{ api.sensitiveInfo }}

**Proof of Concept for Sensitive Information Disclosure:**

**{% for item in api.poc %}**

* 1. {{item}}

{%endfor%}

**Screenshots:**

**{% for item in api.screenshot %}**

* 1. API explorer exposed on **{{item.url}}**

{{item.image}}

{% endfor %}

**Mitigations:**

**{%for item in metigations%}**

* + **{{item.name}}:** {{item.desc}}.

{% endfor %}

{% endif %}

# Conclusion

The vulnerability assessment and penetration testing (VAPT) revealed the following critical issues: {% for item in conclusion %}

* **{{item.name}}:** {{item.desc}}

{% endfor %}