{COMPANY/ ASSET}

Security Assessment Findings Report

<LOGO OR IMAGE >

Date: March 11th to 19th , 2024 **By: Ashique Thaha**

Table of Contents

Confidentiality Statement

This document is a confidential property of {ASSET NAME}.This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent.

Disclaimer

This report is the result of a comprehensive security assessment conducted on [Website Name/URL] as of [Date]. The scope of this assessment was limited to the web application and its immediate supporting infrastructure as agreed upon. The assessment was conducted based on the methodologies and practices that are current as of [Date]. Any changes to the web application or its environment after the date of the assessment are not covered under this report.

Contact Information

Name	Title	Contact Information
Ashique Thaha	*Pentester*	*ashiquethahaofficial@gmail.com*

Assessment Overview

From May 20th, 2019 to May 29th, 2019, I engaged TCMS to evaluate the security posture of its infrastructure compared to current industry best practices. All testing performed is based on the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks.

Phases of penetration testing activities include the following:

- **Planning** – Customer goals are gathered and rules of engagement are obtained.
- **Discovery** – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- **Attack** – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- **Reporting** – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

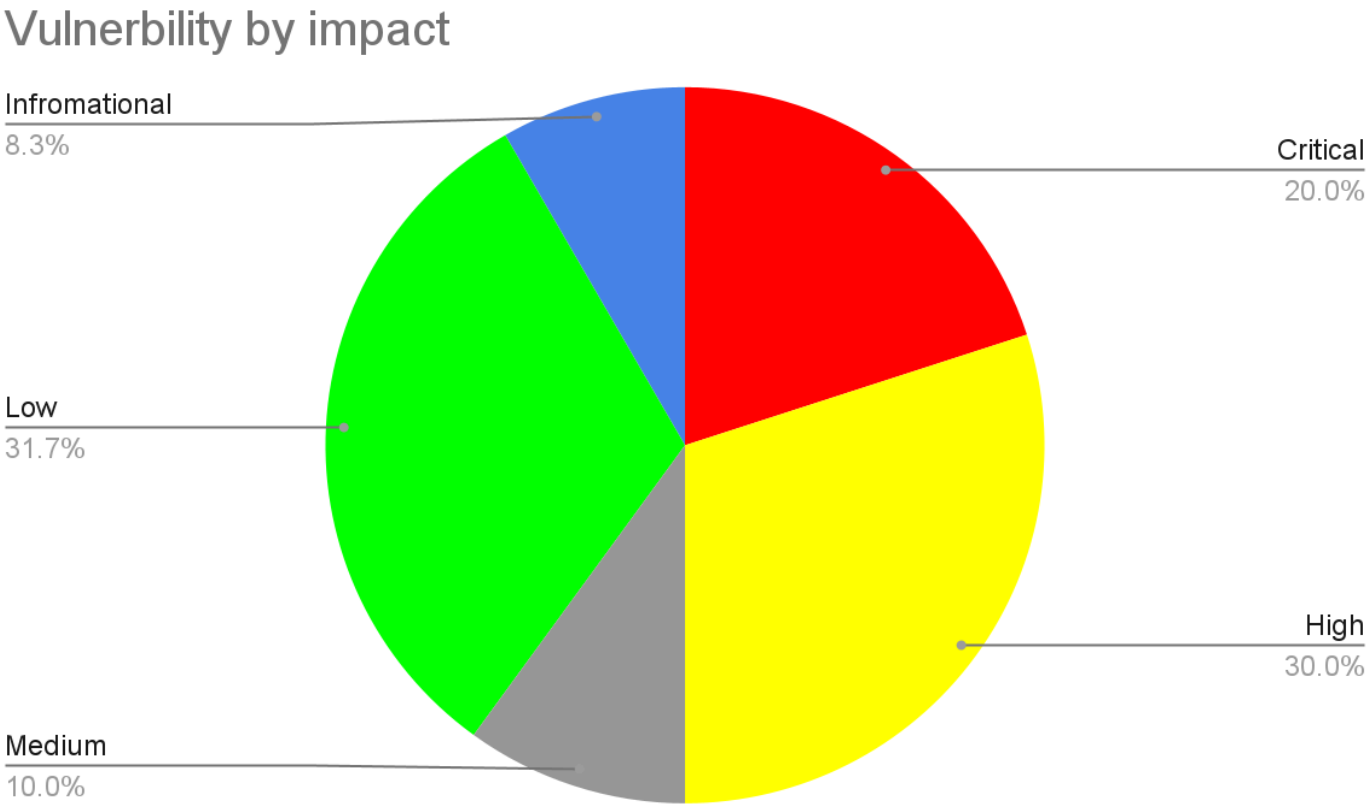
Scope

Scope	Scope type	Start date	End Date

Executive Summary

The Vulnerability Assessment and Penetration Testing (VAPT) conducted on [Website Name/URL] revealed key security insights as of [Date]. While the assessment identified vulnerabilities within the web application and its infrastructure, it's essential to note that not all potential weaknesses may have been uncovered. This report provides recommendations to enhance security, but implementation should be approached cautiously. Confidentiality and limitations apply.

Vulnerability by Impact



This chart shows the percentage of vulnerability based on risk level. Please go through it to get an insight on risk.

Penetration Test Findings

Index

SL.NO	Vulnerability	Affected Component
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		

16		
17		

Vulnerability no. _

Name of Vulnerability:

- **Affected Component:**
- **Affected URL:**

Description Of Vulnerability:

Steps to Reproduce the vulnerability:

Impact

Company's Perspective:

Customer's Perspective:

Legal Issues:

The vulnerability may result in many legal issues some of these are possible ones:

-

Steps for mitigation: