Mithra

Vulnerability Assessment and Penetration Testing Report

Client Name

Conducted by:
Mithra Consulting Team

Executive Summary

Mithra Consulting vulnerability assessment and penetration testing team conducted a vulnerability assessment of the **Client Name**, Application, and environment. The objective was to assess and test the security vulnerabilities that may exist within the applications and environment used by Client name customers. We were provided with user-level as well as admin level credentials to conduct testing. This penetration test is a manual and automated exploitation of the web application.

A vulnerability assessment of the system was conducted to assess the security of the system. The vulnerability assessment was conducted from **Pentest Date**, according to OWASP guidelines. This assessment was a manual and automated exploitation of the web application and underlying API framework. The researchers leveraged tools to facilitate their work. During the penetration testing, security risks and vulnerabilities were identified. These vulnerabilities are described in this report below. We found risk vulnerabilities that require attention and a plan. Based on our testing found for the **Application Name** Web application, there were **Two (2) "High", Two (2) " Medium", and Three (3) "Low" vulnerabilities.**

Scope

Web Application URL: test.com
Web API : test.com

Testing Methodology

Mithra Consulting utilizes a combination of automated testing using standard VAPT tools and services along with manual testing. Mithra Consulting conducts security testing using a methodical and standardized approach. The objective of the assessment was to measure security posture of the in scope assets and identify any deviating vulnerabilities by measuring them against industry adopted controls.

Mithra Consulting team attempts to gain unauthorized access to the applications and systems within scope, and systems connected to networks within scope using non-invasive "white hat" techniques. There are two approaches to penetration testing. The first, black-box testing, is where the tester will perform the evaluation given an IP address. With no knowledge of the system behind the IP addresses, various procedures are used to gain access to the machine. The second, white box testing, is typically focused on an application, and a set of test credentials are known at the time of conducting the test. The latter method is employed when vulnerabilities that attackers will exploit to compromise application data are to be discovered.

Once a list of targets has been compiled, and approved by the customer's stakeholders, the process of attempting to compromise the asset is performed. If an asset is compromised, the Mithra Consulting team will document the process by which the compromise took place and include screenshots, undeniable proof of compromise, and how the compromise was carried out.

ithra

Testing Process

The tests were performed according to penetration testing best practices under OWASP standards and the testing process including the following:

Pre-Testing

- Scoping
- Customer Q&A
- Documentation
- Information gathering
- Discovery

Penetration Testing

- Tool Assisted assessment.
- Manual assessment of OWASP top 10 & business logic
- Exploitation
- Risk Analysis
- Reporting

Post Testing

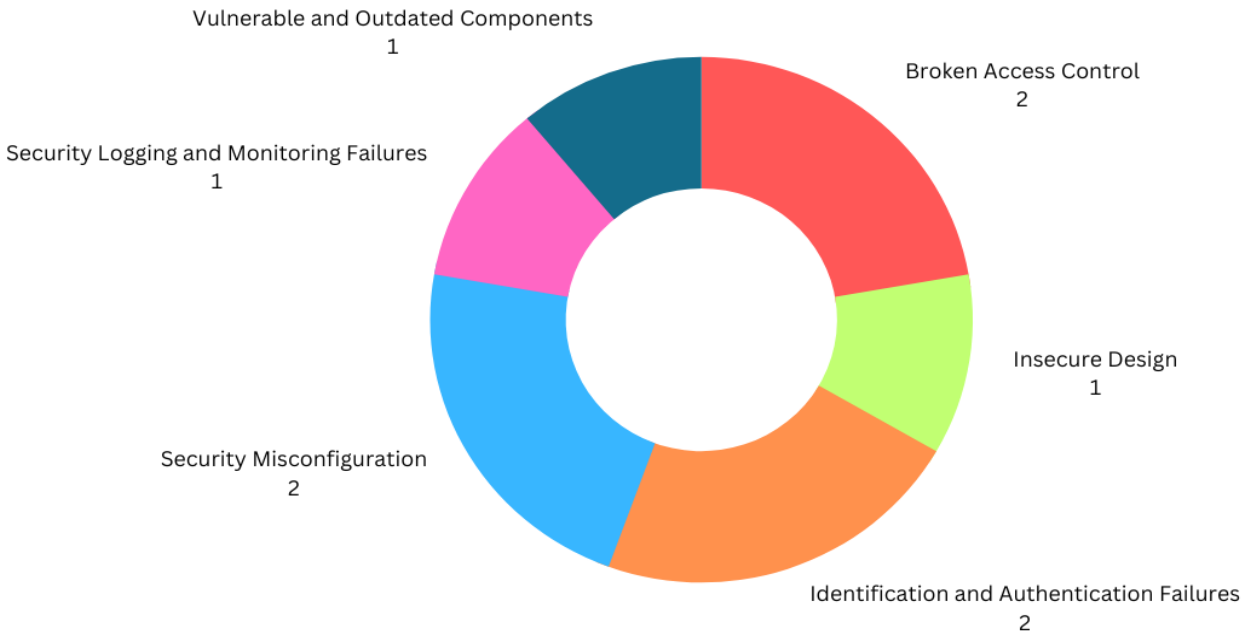
- Prioritized Remediation
- Best Practice Support
- Re-testing

ithra

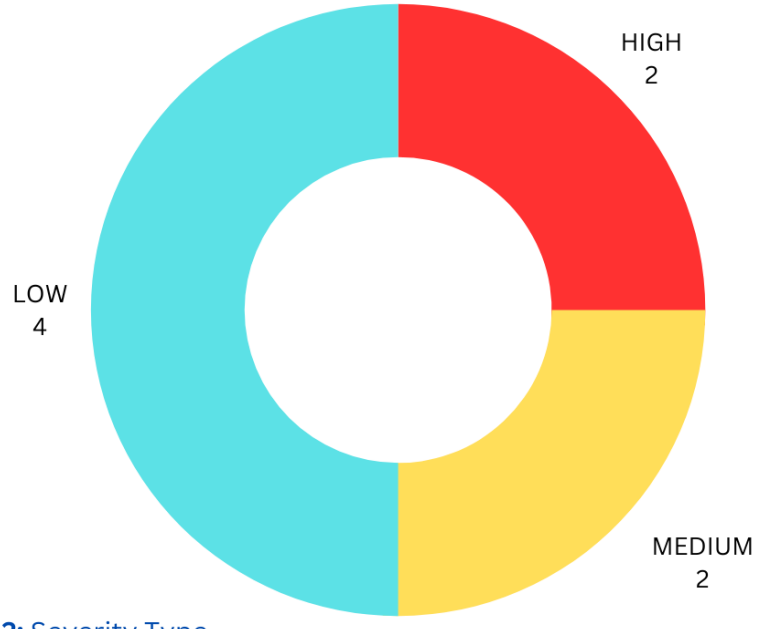
Summary

OWASP Top 10 (Web Application)	Vulnerability ID
A01:2021-Broken Access Control	1
A02:2021-Cryptographic Failures	NONE
A03:2021-Injection	1
A04:2021-Insecure Design	NONE
A05:2022-Security Misconfiguration	1
A06:2022-Vulnerable and Outdated Components	2
A07:2022-Identification and Authentication Failures	2
A08:2022-Software and Data Integrity Failures	NONE
A09:2022-Security Logging and Monitoring Failures	1
A10:2022-Server-Side Request Forgery	NONE

Graphical Summary



Graph 1: Issues Type



Graph 2: Severity Type

ithra

Vulnerability Descriptions

1. Vulnerability Name

Vulnerability Category:

Severity:

CVSS v3 Score:

OWASP Reference: A01:2021 - Broken Access Control

Proof of Concept Link: Click Here

Description: Provides a detailed description of the vulnerability, including how it works, the conditions required for exploitation, and the potential impact on the system. Include technical details but keep the language accessible to both technical and non-technical stakeholders.

Recommendation: Provides clear and actionable recommendations for mitigating or remedying the vulnerability. This may include software patches, configuration changes, or other security measures.

---

2. Vulnerability Name

Vulnerability Category:

Severity:

CVSS v3 Score:

OWASP Reference: A01:2021 - Broken Access Control

Proof of Concept Link: Click Here

Description: Provides a detailed description of the vulnerability, including how it works, the conditions required for exploitation, and the potential impact on the system. Include technical details but keep the language accessible to both technical and non-technical stakeholders.

Recommendation: Provides clear and actionable recommendations for mitigating or remedying the vulnerability. This may include software patches, configuration changes, or other security measures.
