COMPANY LOGO

Pathan Humam

[COMPANY NAME] [Company address]

Table of Contents

- Note this document is for Demonstration of our penetration report only actual may vary from this document base on client requirement and test type

1. Summary Test Result

Scope	Security level	Grade
Scope Name	Fair	C

Under Defence Grading Criteria:

Grade	Security	Criteria Description
A	Excellent	The security exceeds "Industry Best Practice" standards. The overall posture was found to be excellent with only a few low-risk findings identified.
B	Good	The security meets accepted standards for "Industry Best Practice." The overall posture was found to be strong with only a handful of medium- and low-risk shortcomings identified.
C	Fair	Current solutions protect some areas of the enterprise from security issues. Moderate changes are required to elevate the discussed areas to "Industry Best Practice" standards
D	Poor	Significant security deficiencies exist. Immediate attention should be given to the discussed issues to address the exposures identified. Major changes are required to elevate to "Industry Best Practice" standards.
E	Inadequate	Serious security deficiencies exist. Shortcomings were identified throughout most or even all of the security controls examined. Improving security will require a major allocation of resources.

2. Assumptions & Constraints

As the environment changes and new vulnerabilities and risks are discovered and made public, an organization's overall security posture will change. Such changes may affect the validity of this letter. Therefore, the conclusion reached from our analysis only represents a "snapshot" in time.

3. Objective & Scope

SCOPE	Name
Audit type	Penetration Testing
URL	URL Link
Duration	Testing Period

Consultants performed a discovery process initially to gather information about the target and searched for information disclosure vulnerabilities. With this data in hand, we conducted the bulk of the testing manually, which consisted of input validation tests, impersonation (authentication and authorization) tests, and session state management tests. The purpose of this penetration testing is to illuminate security risks by leveraging weak-nesses within the environment that lead to the obtainment of unauthorized access and/or the retrieval of sensitive information. The shortcomings identified during the assessment were used to formulate recommendationsand mitigation strategies for improving the overall security posture.

Result Overview

The test uncovered a few vulnerabilities that may cause impact to Flipp’s environment. if not addressed in an effective manner.
Below is the summary table of finding categorized by severity scoring.

Severity	Critical	High	Medium	Low	Informational
Number of issues	0	0	0	0	0

Severity scoring with descriptions:

Critical – Immediate threat to key business processes.
High – Direct threat to key business processes.
Medium – No direct threat exists. The vulnerability may be exploited using other vulnerabilities.
Low – No direct threat exists. The vulnerability may be exploited using other vulnerabilities.
Informational – This finding does not indicate vulnerability but states a comment that notifies about design flaws and improper implementation that might cause a problem in the long run.

4. Performed tests.

All sets of applicable OWASP Top 10 2023

Criteria Label	Status Validation
A1:2021 – Information Gathering	Fails Requirement
A2:2021 – Configuration and Deploy management	Fails Requirement
A3:2021 – Identity management	Meet Requirement
A4:2021 – Authentication & Authorization test	Fails Requirement
A5:2021 – Security Misconfiguration	Fails Requirement
A6:2021 – Session management test	Fails Requirement
A7:2021 – Data Validation test	Fails Requirement
A8:2021 – Error handling	Meet Requirement
A9:2021 – cryptography	Meet Requirement
A10:2021 – Business logic	Fails Requirement

Security tools used.

This are some of tools, procedures and scripts used during testing

- Burp Suite Pro
- Postman
- Nessus
- Nikto
- Curl
- ZAP
- And More

5. Methodology

Our Penetration Testing Methodology is based on the following standards and guidelines:

- OWASP Top 10 WEB Application Security Risks- 2021
- OWASP Testing Guide V-4.0

Open Security Project (OWASP) is an industry initiative for security testing. OWASP has identified the 10 most common attacks that has been successful worldwide.

Application penetration test includes all the items in the OWASP Top 10 and more. The penetration tester remotely tries to compromise the OWASP Top 10 flaws.

6. Finding Details

I. Information Gathering

Severity: HIGH- CWE-693: Protection Mechanism Failure (CVSs: 6.5)LOCATION: Link

ISSUE DESCRIPTION:

Our analyst ran a scan over the base URL and fount this vulnerability

PROOF OF VULNERABILITY:

- Image proof

Figure 1 :contain metafiles

Recommendation:

- Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

II. Configuration and Deploy Management (Application Admin interface)

Severity: Medium- CWE-639: Authorization Bypass Through User-Controlled Key (CVSs6.5)

LOCATION: link/admin

ISSUE DESCRIPTION:

Our analyst test admin privilage over the base URL and fount this vulnerability

PROOF OF VULNERABILITY:

- Image proof

Figure 2: Authentication access control

Recommendation:

- Conduct periodic reviews and updates of access control policies to align with any system changes.
- Foster an understanding of secure coding practices, the importance of data protection, and the risks associated with insecure direct object references.

III. Error Handling

Severity: LOW - CWE-754: Improper Check for Unusual or Exceptional Conditions. (CVSs :6.5)

LOCATION:

ISSUE DESCRIPTION:

Our analyst changed by removing certain fields over the base URL and fount this vulnerability.

PROOF OF VULNERABILITY:

- Image proof

Figure 3 : default field of the request

Recommendation:

- Provide generic error messages to users and avoid disclosing inaccurate information. Craft error messages that are helpful for developers but do not expose internal details.
- Implement an optional retry mechanism for authentication failures. This will give users a chance to correct their credentials and try again without having to restart the process from scratch.