API SECURITY RISK ANALYSIS REPORT

Dharani L

Cybersecurity Internship task 3

Future interns

API TESTED:

JSONPlaceholder (https://jsonplaceholder.typicode.com)

PURPOSE OF API:

JSONPlaceholder is a public REST API used for testing and prototyping applications.

TOOLS USED:

- Postman
- Browser Developer Tools
- OWASP API Security Top 10 (Reference)

SCOPE OF ANALYSIS:

This analysis was limited to read-only testing of public API endpoints using safe GET requests. No exploitation or intrusive testing was performed.

TESTED ENDPOINTS:

- GET /users
- GET /posts

IDENTIFIED SECURITY RISKS:

1. OPEN / UNAUTHENTICATED ENDPOINTS

All tested endpoints were accessible without authentication or API keys.

Severity: **High**

Business Impact: Unauthorized users can freely access and scrape data, leading to data exposure and abuse.

Remediation: Implement authentication mechanisms such as API keys, OAuth 2.0, or JWT.

2. EXCESSIVE DATA EXPOSURE

The /users endpoint exposes user details such as email and address information.

Severity: **Medium**

Business Impact: Increases privacy risks and potential misuse of personal data.

Remediation: Apply data minimization and return only necessary fields.

3. MISSING AUTHORIZATION CONTROLS

Resources can be accessed directly by ID without ownership validation.

Severity: **High**

Business Impact: Users may access data belonging to other users.

Remediation: Enforce object-level authorization checks.

4. MISSING RATE LIMITING

No visible request limits were observed on the API.

Severity: **Medium**

Business Impact: APIs are vulnerable to abuse and denial-of-service attacks.

Remediation: Implement rate limiting and request throttling.

RISK SUMMARY:

Unauthenticated Access – High

Excessive Data Exposure – Medium

Missing Authorization – High

No Rate Limiting – Medium

CONCLUSION:

This API demonstrates common security weaknesses found in real-world SaaS applications. If deployed in production, these risks could result in data leaks and service abuse. Implementing authentication, authorization, and rate limiting would significantly improve security.