API SECURITY RISK ANALYSIS

NAME: ADARSH SINGH RAWAT
INTERNSHIP: CYBER SECURITY – FUTURE INTERNS
TASK 3 – API SECURITY RISK ANALYSIS
CIN ID: FIT/FEB26/CS6144
DATE: FEBRUARY 2026

FUTURE
INTERNS

INTRODUCTION

This report presents a security assessment of a public API to identify potential vulnerabilities related to authentication, authorization, data exposure, and input validation. The objective was to analyze security risks and recommend mitigation strategies.

API OVERVIEW

Selected API: JSONPlaceholder

Base URL:

https://jsonplaceholder.typicode.com

Endpoints Tested:

- /users
- /users/{id}

The API provides sample user data for testing and development purposes.

METHODOLOGY

The evaluation was carried out utilizing:

- Postman for testing API requests
- Analyzing API answers by hand
- Testing for authorization and authentication
- Rate-limiting and input validation checks

To find security flaws, both GET and POST requests were examined.

HIGH RISK FINDINGS

.1. Inadequate Authentication
User data was accessible over the API without the need for authentication.
2. Object Level Authorization (BOLA) is broken.
By changing user IDs, individual user data could be accessed.
3. Illicit Data Generation
Fake users could be created without verification thanks to POST requests.

MEDIUM RISK FINDINGS

1. Exposure to sensitive data

Data about user addresses, phone numbers, and emails were available to the public.

2. Insufficient Validation of Input

Unvalidated data was accepted by the API.

3. Rate Limiting Missing

Several quick requests were granted without any limitations.

LOW RISK FINDINGS

Excessive Data Exposure

API returned additional fields such as geo-location and company details that may not be necessary for all use cases.

RECOMMENDATIONS

- Implement authentication and authorization mechanisms
- Apply input validation and data sanitization
- Use rate limiting to prevent abuse
- Restrict sensitive data exposure
- Follow OWASP API Security Top 10 guidelines

CONCLUSION

SEVERAL API SECURITY ISSUES WERE FOUND BY THE STUDY, SUCH AS INADEQUATE AUTHENTICATION, EXCESSIVE INFORMATION EXPOSURE, AND A LACK OF RATE LIMITATION. API SECURITY CAN BE GREATLY IMPROVED BY PUTTING IN PLACE PROPER AUTHORIZATION AND VALIDATION PROCEDURES.