FUTURE INTERNS CYBER SECURITY

API Security Risk Analysis Report

Comprehensive security evaluation of API endpoints, authentication, and data exposure vulnerabilities.

INTERN NAME
Shubhrat Chaursiya

ORGANIZATION
Future Interns

DOMAIN & TASK
Cyber Security - Task 3

CIN
FIT/JAN26/CS5559

PREPARED AS PART OF THE CYBER SECURITY INTERNSHIP PROGRAM

02. OBJECTIVE

◎ Goal

The objective of this task is to analyze the security risks associated with API endpoints, identify authentication and authorization issues, detect insecure configurations, and recommend suitable remediation measures using simple and professional language.

03. SCOPE

API TESTED

`https://jsonplaceholder.typicode.com`

Areas Covered

- ✓ Auth & Authorization
- ✓ Data Exposure
- ✓ Input Validation
- ✓ Rate Limiting

Constraint

⚠ No destructive testing or stress testing was performed on the live infrastructure.

04. TOOLS & TECHNOLOGIES

Postman
API request testing and environment management.

Browser DevTools
Inspection of network headers and response times.

GitHub / Canva
Documentation, version control, and submission.

05. METHODOLOGY

Endpoint Identification
Selected public test API and mapped all accessible endpoints.

Traffic Analysis
Sent GET/POST requests using Postman to observe response behaviors.

Control Review
Analyzed authentication requirements and authorization tokens.

Risk Assessment
Documented identified vulnerabilities and assigned risk levels.

06. CRITICAL RISK ANALYSIS

Missing Authentication

LEVEL: HIGH

Vulnerability ID: API-SEC-01

Description

The API allows access to sensitive endpoints without any authentication tokens, exposing data to the public internet.

Impact

Unauthorized data leakage and potential misuse of API resources by automated bots.

REMEDIATION

Implement OAuth2.0 or API Keys. Enforce strict access control policies for all GET/POST methods.

07. DATA EXPOSURE ANALYSIS

Excessive Data Exposure

LEVEL: MEDIUM

Vulnerability ID: API-SEC-02

Description

API responses return complete object models even when only specific fields are requested.

Impact

Potential privacy concerns and metadata leakage that aids reconnaissance.

REMEDIATION

Implement backend response filtering to return only the minimum data required for the UI.

08. AVAILABILITY ANALYSIS

Missing Rate Limiting

LEVEL: LOW

Vulnerability ID: API-SEC-03

Description

The API does not enforce limits on the number of requests sent within a specific timeframe.

Impact

Risk of Denial-of-Service (DoS) and resource exhaustion during brute-force attempts.

REMEDIATION

Implement throttling/rate-limiting based on IP or User-ID to prevent flooding.

09. RISK SUMMARY TABLE

Consolidated API Security Matrix

API Risk Found	Classification	Risk Level
Missing Authentication	Security Bypass	High
Excessive Data Exposure	Information Leakage	Medium
Missing Rate Limiting	Availability Risk	Low

10. CONCLUSION

Final Summary

The API security analysis identified multiple risks that could affect data confidentiality and service availability. Implementing authentication, limiting data exposure, and enforcing rate limiting can significantly improve API security.

11. LEARNING OUTCOMES

Technical Skills

Practical usage of Postman for intercepting and analyzing API calls.

Vulnerability ID

Understanding of OWASP API Top 10 security fundamentals.

Documentation

Developing professional security documentation and reporting skills.

Analysis

Learning to identify insecure configurations in live API environments.

12. DISCLAIMER

⚠ SECURITY DISCLAIMER

This API security analysis was conducted strictly for educational purposes using publicly available test APIs. No real user data was accessed or misused. This report does not constitute a full penetration test but serves as a risk analysis exercise for the Cyber Security Internship Program.