API Security Risk Analysis Report

1. Executive Summary

APIs play a critical role in modern web and mobile applications by enabling data exchange between systems. This report presents a security risk analysis of a publicly accessible demo API to identify common API security weaknesses and recommend best practices.

The assessment focuses on authentication controls, data exposure, and general API security posture using non-intrusive methods.

2. Scope of Assessment

In Scope:

- Public API endpoint analysis
- Authentication and authorization review
- Data exposure observation
- Basic rate-limiting observation

Out of Scope:

- Exploitation or penetration testing
- Denial-of-service testing
- Authentication bypass attempts

3. API Overview

API Used: JSONPlaceholder
Base URL: https://jsonplaceholder.typicode.com
Purpose: Demo API providing fake user and post data for testing and learning.

4. Methodology

The API was analyzed using browser-based requests and optional Postman testing. Only GET requests were performed. No attempt was made to modify, delete, or manipulate data.

5. Findings & Risk Analysis

🔹 Finding 1: Unauthenticated API Endpoints

Risk Level: Medium

Description:
The API allows access to endpoints such as /users and /posts without requiring authentication or API keys.

Impact:
Unauthenticated access may lead to unauthorized data exposure if similar configurations exist in production environments.

Recommendation:
Implement authentication mechanisms such as API keys, OAuth tokens, or JWT-based access control.

◆ Finding 2: Excessive Data Exposure

Risk Level: Medium

Description:
API responses return complete user objects, including email addresses and identifiers, even when minimal data may be required.

Impact:
Excessive data exposure increases the risk of data misuse and privacy concerns.

Recommendation:
Limit API responses to only necessary fields using data filtering and response validation.

◆ Finding 3: Lack of Rate Limiting Controls

Risk Level: Low

Description:
No visible rate-limiting mechanisms were observed during repeated requests.

Impact:
Absence of rate limiting can expose APIs to abuse or denial-of-service risks.

Recommendation:
Implement rate-limiting and request-throttling mechanisms.

6. Overall Risk Summary

Area	Observation
Authentication	Not enforced
Data Exposure	Excessive
Rate Limiting	Not observed
API Purpose	Demo / Testing

7. Conclusion

This API security risk analysis highlights common weaknesses that can occur when APIs are exposed without proper security controls. While the analyzed API is intended for testing purposes, similar configurations in production environments could pose significant security risks. Implementing authentication, limiting data exposure, and enforcing rate controls are essential for secure API design.

“All observations were performed using browser-based GET requests without authentication. No intrusive testing or exploitation was conducted.”