API SECURITY RISK ANALYSIS

Read-Only Security Analysis of a Public Demo API

Prepared by: Anjali
Cyber Security Intern – Future Interns
Date : 19 jan 2026

Table of Contents

1.0 Executive Summary

This report presents the results of an API security risk analysis conducted on a publicly accessible demo API. The objective of the assessment was to identify common API security risks and evaluate how API endpoints handle access and data exposure.

The assessment was performed using read-only techniques by sending standard API requests and reviewing server responses. No authentication bypass, exploitation, or intrusive testing was conducted during this analysis.

The review identified several security concerns, including unauthenticated access to API endpoints, excessive data exposure, and lack of rate limiting. Although the analyzed API is intended for demonstration purposes, these findings highlight security risks that could have serious implications in production environments. Addressing these issues can significantly improve an API's overall security posture.

2.0 Introduction

Application Programming Interfaces (APIs) are a core part of modern applications and are widely used to enable communication between systems, mobile apps, and web services. While APIs make data exchange efficient, insecure API implementations can expose sensitive information and create serious security risks for organizations.

This report focuses on analyzing the security posture of a publicly available API to identify common security risks such as missing authentication, excessive data exposure, and improper access controls. The assessment is conducted using read-only techniques to ensure that no harm is caused to the target API.

The objective of this analysis is to explain API security risks in a simple and business-friendly manner and to provide practical recommendations that can help improve API security. This assessment is intended strictly for educational purposes and does not involve any exploitation or unauthorized access.

3.0 Scope Of Assessment

The scope of this API security risk analysis was limited to a publicly accessible demo API intended for testing and educational use. The selected API endpoints were analyzed to understand how data is exposed and accessed through standard HTTP requests.

The assessment focused on passive and read-only testing techniques using API request tools to observe request–response behavior, returned data structures, and access control mechanisms. Particular attention was given to identifying common API security risks such as lack of authentication, unrestricted access to resources, excessive data exposure, and informative error responses.

The following activities were **explicitly excluded** from this assessment:

- Authentication bypass or privilege escalation attempts
- Exploitation of identified weaknesses
- Modification, deletion, or injection of data
- Brute-force, fuzzing, or denial-of-service attacks

This assessment was conducted strictly for educational and learning purposes and did not involve any actions that could disrupt or negatively impact the target API or its underlying infrastructure.

3.1 Methodology of Assessment

The API security risk analysis was conducted using a structured and non-intrusive approach. The publicly available API endpoints were tested using Postman to send standard HTTP requests and observe server responses.

Initially, the API endpoints were identified and accessed without authentication to determine whether access controls were enforced. The responses were reviewed to understand the type and sensitivity of data returned by the API. Request headers, response bodies, HTTP status codes, and error messages were analyzed to identify potential security risks such as unrestricted data access and excessive information exposure.

All testing was performed in a read-only manner without attempting to manipulate, exploit, or alter any data. The findings were documented clearly, and identified risks were classified based on their potential impact. Practical and business-friendly recommendations were provided to address the observed issues.

4.0 API Overview

The API selected for this security risk analysis is **JSONPlaceholder**, a publicly available demo API commonly used for testing and learning purposes.

API Name: JSONPlaceholder
Base URL: https://jsonplaceholder.typicode.com

JSONPlaceholder provides fake online REST API endpoints that return sample data such as posts, comments, users, and todos. The API is designed for development and testing and does not require authentication for accessing most endpoints.

For this assessment, the following endpoint was tested:

- **GET /users** – Returns a list of user-related information

The purpose of analyzing this API was to understand how publicly accessible endpoints expose data and to identify potential security risks related to unrestricted access and data exposure using read-only techniques.

Findings Summary

ID	Finding Title	Risk Level	Brief Description	Recommendation
F-01	Unauthenticated Access to API Endpoint	Medium	The API endpoint allows access to user data without any authentication or authorization checks.	Implement authentication and authorization mechanisms for API access.
F-02	Excessive Data Exposure	Medium	The API returns complete user information, exposing more data than necessary for basic requests.	Limit API responses to only required fields and apply data minimization.
F-03	Lack of Rate Limiting	Low	The API does not appear to enforce request rate limits, which may allow abuse of the endpoint.	Implement rate limiting to prevent excessive or automated requests.

Detailed Findings

Finding F-01: Unauthenticated Access to API Endpoint

Description:
The API endpoint can be accessed without any authentication or authorization checks.

Why This Matters:
Unauthenticated access allows anyone to retrieve data, increasing the risk of unauthorized data exposure and misuse.

Risk Level:
Medium

Evidence:
Observed via GET requests sent through Postman without providing any authentication tokens.

Finding F-02: Excessive Data Exposure

Description:
The API returns complete user records, including fields that may not be necessary for basic functionality.

Why This Matters:
Exposing more data than required increases privacy risks and provides attackers with additional information that could be misused.

Risk Level:
Medium

Evidence:
API responses showed full user objects when accessing the `/users` endpoint.

Finding F-03: Lack of Rate Limiting

Description:
The API does not appear to restrict the number of requests that can be made within a specific time frame.

Why This Matters:
Without rate limiting, APIs can be abused through automated requests, leading to service abuse or performance issues.

Risk Level:
Low

Evidence:
Multiple consecutive requests returned successful responses without any rate-limit warnings or errors.

CONCLUSION

This API security risk analysis reviewed a publicly accessible demo API to identify common security risks related to access control and data exposure. The assessment was conducted using read-only techniques to observe API behavior without performing any exploitation or intrusive testing.

The analysis identified key security concerns such as unauthenticated access to API endpoints, excessive data exposure, and lack of rate limiting. While these issues were observed in a demo API environment, similar weaknesses in production systems could lead to unauthorized data access, privacy risks, and service abuse.

Implementing fundamental API security controls such as authentication, authorization, data minimization, and rate limiting can significantly reduce these risks. Regular security reviews and adherence to API security best practices are recommended to maintain a secure and reliable API ecosystem.