
API

Table of Contents

1. APIs Tested

The following APIs were tested using **Postman** with GET requests on the DummyJSON public API:

- **GET /users**
- **GET /products**
- **GET /carts**
- **GET /recipes**
- **GET /comments**
- **GET /todos**

Base URL: https://dummyjson.com

2. Identified Risks, Severity, Business Impact & Remediation

Risk 1: No Authentication / Authorization

Description:
All APIs are accessible without any authentication token or authorization mechanism. Any user can fetch sensitive data.

- **Affected APIs:** All (users, products, carts, comments, todos, recipes)
- **Severity: High**
- **Business Impact:**
    - Unauthorized access to user data
    - Data scraping and misuse
    - Compliance violations (GDPR, privacy laws)
- **Remediation Suggestions:**
    - Implement authentication (OAuth 2.0, JWT)
    - Enforce role-based access control (RBAC)
    - Restrict sensitive endpoints to authorized users only

Risk 2: Exposure of Sensitive User Information

Description:
The /users API exposes sensitive personal data such as:

- Email
- Phone number
- Password (plain text)
- IP address
- Address details
- **Severity: High**
- **Business Impact:**
    - Identity theft
    - Account compromise
    - Loss of user trust
- **Remediation Suggestions:**
    - Never return passwords in API responses
    - Mask or remove PII fields
    - Apply data minimization principles

Risk 3: Missing Rate Limiting Protection

Description:
Although rate-limit headers are present, APIs are freely accessible and can be repeatedly hit.

- **Severity: Medium**
- **Business Impact:**
    - API abuse
    - Denial of Service (DoS) risk
    - Increased infrastructure cost

- **Remediation Suggestions:**
    - Enforce strict rate limits per IP/user
    - Introduce API throttling
    - Monitor abnormal traffic patterns

Risk 4: Excessive Data Exposure

Description:
APIs return full objects even when partial data would suffice (e.g., products, carts, users).

- **Severity: Medium**
- **Business Impact:**
    - Larger attack surface
    - Easier data harvesting
- **Remediation Suggestions:**
    - Implement field-level filtering
    - Use pagination and limited response fields
    - Follow “least privilege” for data exposure

Risk 5: No Input Validation or Query Restrictions

Description:
Query parameters are unrestricted and unvalidated.

- **Severity: Low**
- **Business Impact:**
    - Potential future injection risks
    - Unexpected server behavior
- **Remediation Suggestions:**
    - Validate and sanitize query parameters
    - Define strict API contracts

- Reject malformed or unexpected inputs

3. Overall Risk Summary

Risk Area	Severity
Authentication & Authorization	High
Sensitive Data Exposure	High
Rate Limiting	Medium
Data Overexposure	Medium
Input Validation	Low

4. Conclusion

The tested APIs demonstrate **functional correctness** but lack essential **security controls**. The most critical issues are **missing authentication** and **exposure of sensitive user data**, which can lead to serious business, legal, and reputational damage if deployed in a production environment.