API Security Risk Analysis

Project : 03 Assessment

Type: API security Testing

Date: 17-01-2026

1. Public Demo API Walkthrough

Target: Fake Store API - https://fakestoreapi.com
Purpose: Demo e-commerce API for testing and learning
Scope: Read-only analysis, documentation-based testing

2. Review API Documentation

Key Observations from Docs - https://fakestoreapi.com/docs

- No authentication required for most endpoints
- Focused on products, carts, users
- Designed for demo/testing, not production

Example Endpoints

Endpoint	Method	Purpose
/products	GET,POST	List all products
/products/{id}	GET,PUT,DELETE	Product details
/users	GET,POST	List users
/users/{id}	GET,PUT,DELETE	User details
/carts	GET,POST	Shopping carts
/carts/{id}	GET,PUT,DELTE	Cart details
/auth/login	POST	Login

Even demo APIs simulate real-world patterns. Any weakness here mirrors what often appears in production systems.

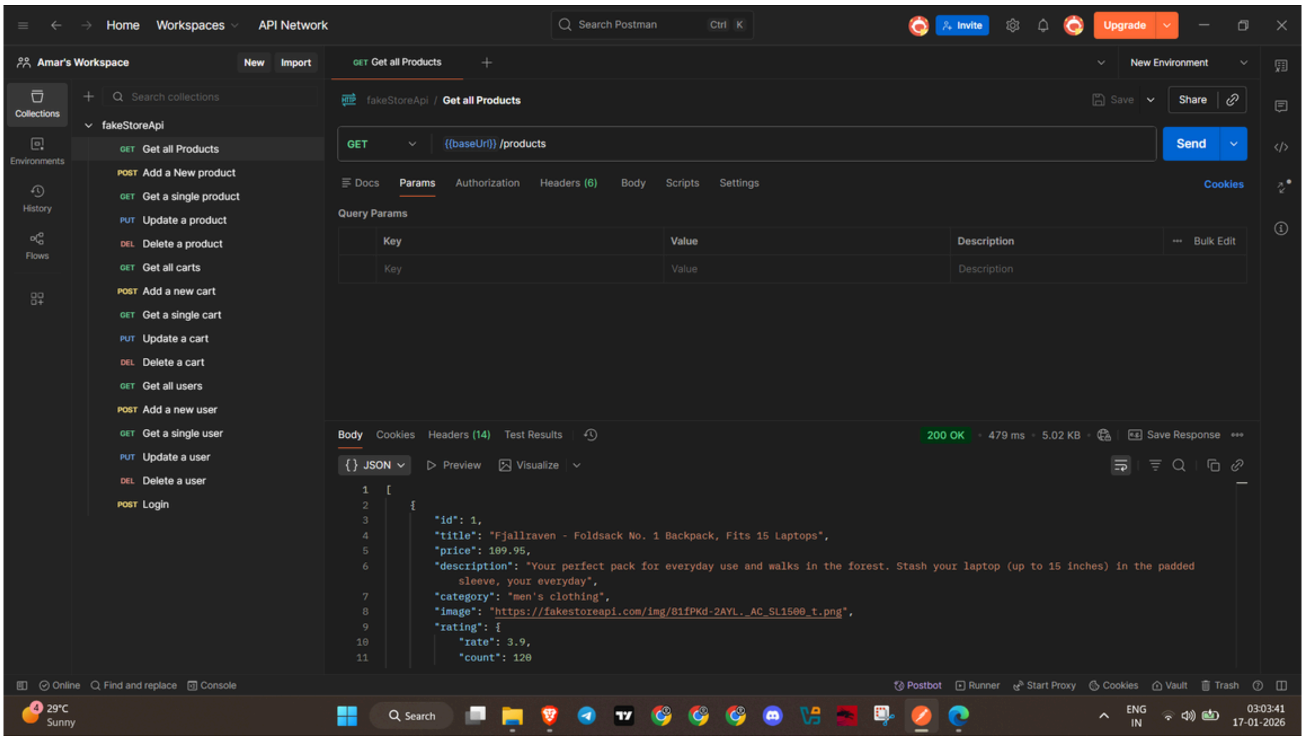
3. Test Endpoints Using Postman / Insomnia :

I used Postman

{{baseUrl}} - https://fakestoreapi.com - Variable added for this collection

API ENDPOITNS

- Products
  - GET - get all products - **GET {{baseUrl}}/products**



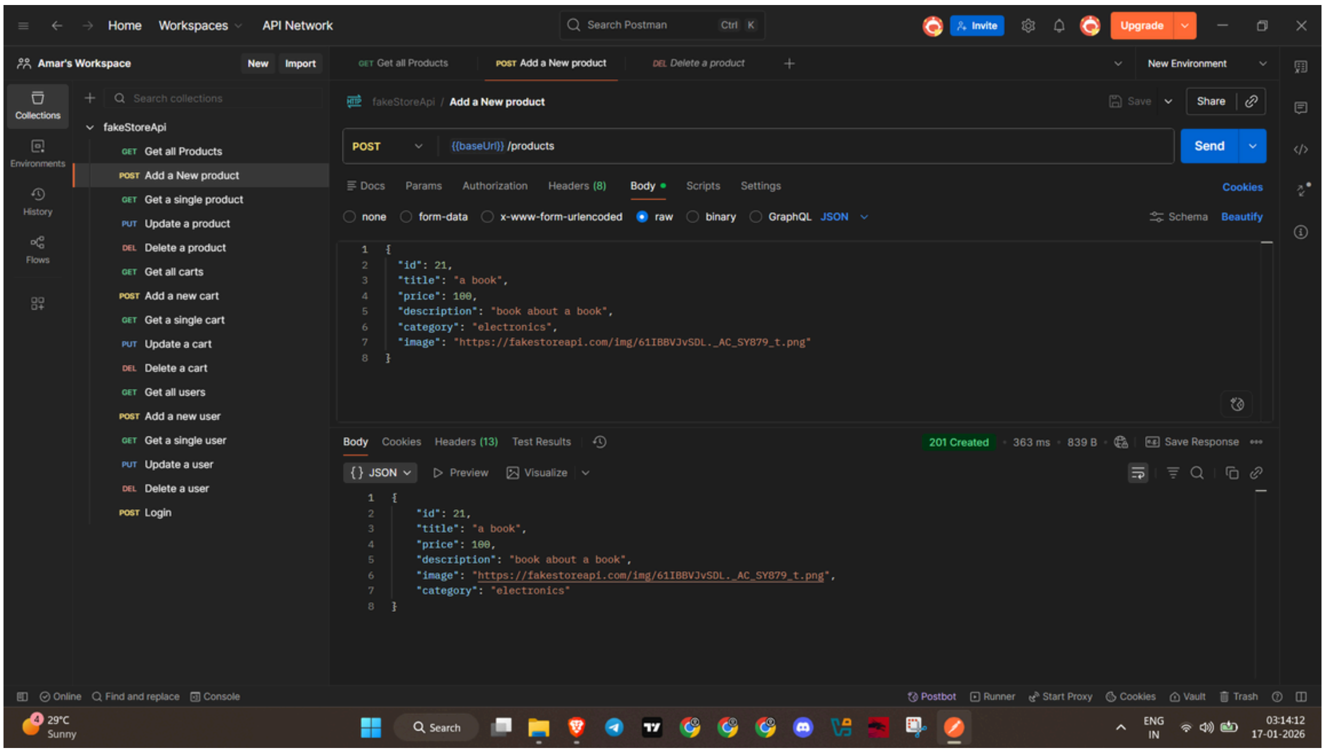
fakeStoreApi / Get all Products

GET {{baseUrl}} /products

Body — 200 OK · 479 ms · 5.02 KB

```
[
    {
        "id": 1,
        "title": "Fjallraven - Foldsack No. 1 Backpack, Fits 15 Laptops",
        "price": 109.95,
        "description": "Your perfect pack for everyday use and walks in the forest. Stash your laptop (up to 15 inches) in the padded
            sleeve, your everyday",
        "category": "men's clothing",
        "image": "https://fakestoreapi.com/img/81fPKd-2AYL._AC_SL1500_t.png",
        "rating": {
            "rate": 3.9,
            "count": 120
```

- POST - add a new product - **POST {{baseUrl}}/products**



fakeStoreApi / Add a New product

POST {{baseUrl}} /products

Body: none | form-data | x-www-form-urlencoded | [✓ raw] | binary | GraphQL — JSON

```
{
    "id": 21,
    "title": "a book",
    "price": 100,
    "description": "book about a book",
    "category": "electronics",
    "image": "https://fakestoreapi.com/img/61IBBVJvSDL._AC_SY879_t.png"
}
```

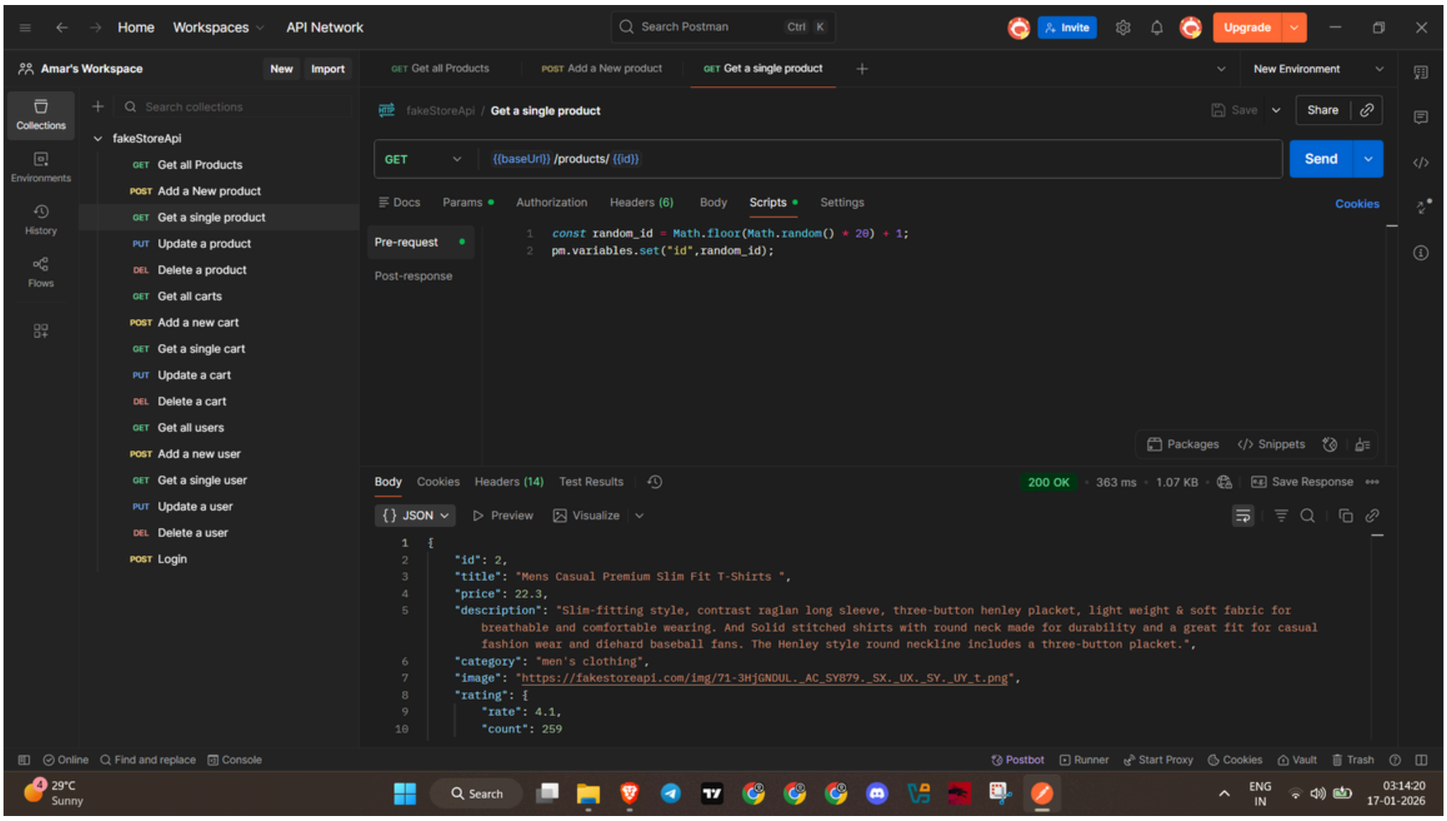
Body — 201 Created · 363 ms · 839 B

```
{
    "id": 21,
    "title": "a book",
    "price": 100,
    "description": "book about a book",
    "image": "https://fakestoreapi.com/img/61IBBVJvSDL._AC_SY879_t.png",
    "category": "electronics"
}
```

BODY - raw - json format :

```
{
  "id": 21,
  "title": "a book",
  "price": 100,
  "description": "book about a book",
  "category": "electronics",
  "image": "https://fakestoreapi.com/img/61IBBVJvSDL._AC_SY879_t.png"
}
```

- GET - get a single product - **GET {{baseUrl}}/products/{{id}}**



```
GET {{baseUrl}} /products/ {{id}}
```

```
const random_id = Math.floor(Math.random() * 20) + 1;
pm.variables.set("id",random_id);
```

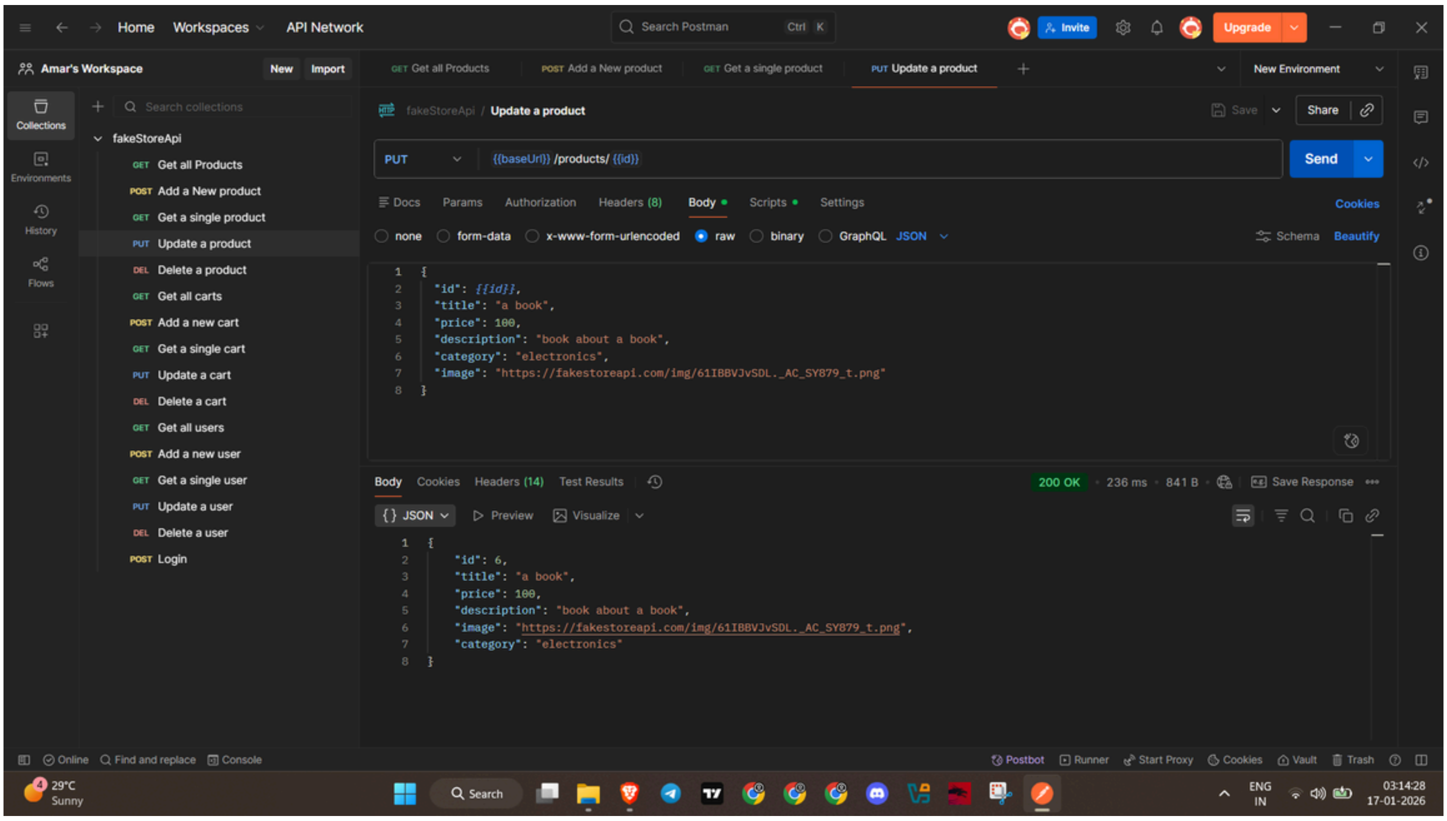
200 OK · 363 ms · 1.07 KB

```
{
    "id": 2,
    "title": "Mens Casual Premium Slim Fit T-Shirts ",
    "price": 22.3,
    "description": "Slim-fitting style, contrast raglan long sleeve, three-button henley placket, light weight & soft fabric for
        breathable and comfortable wearing. And Solid stitched shirts with round neck made for durability and a great fit for casual
        fashion wear and diehard baseball fans. The Henley style round neckline includes a three-button placket.",
    "category": "men's clothing",
    "image": "https://fakestoreapi.com/img/71-3HjGNDUL._AC_SY879._SX._UX._SY._UY_t.png",
    "rating": {
        "rate": 4.1,
        "count": 259
```

Pre-request Script :

const random_id = Math.floor(Math.random() * 20) + 1;
pm.variables.set("id",random_id);

- PUT - update a product - **PUT {{baseUrl}}/products/{{id}}**



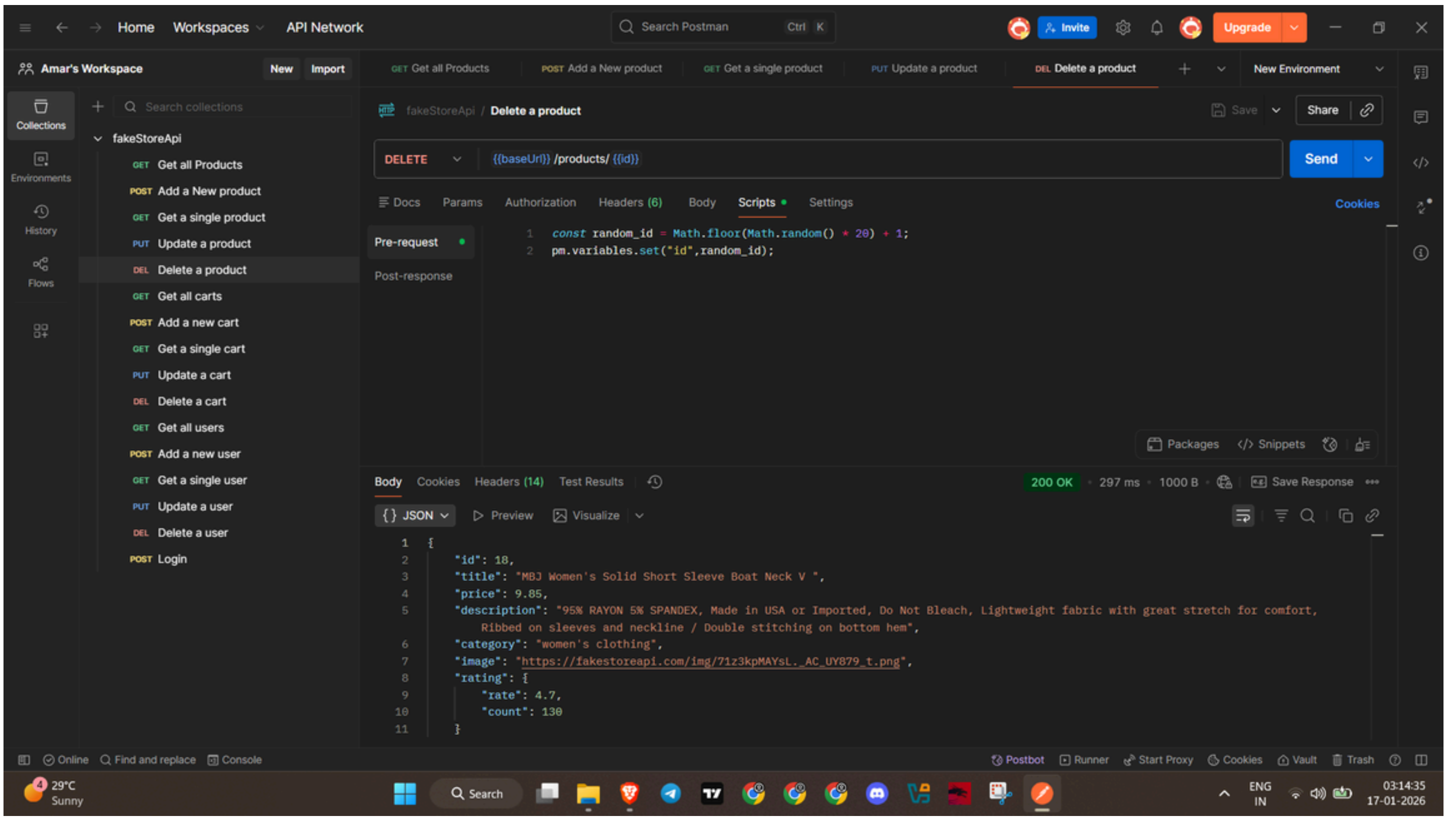
```
PUT {{baseUrl}} /products/ {{id}}
```

```
{
  "id": {{id}},
  "title": "a book",
  "price": 100,
  "description": "book about a book",
  "category": "electronics",
  "image": "https://fakestoreapi.com/img/61IBBVJvSDL._AC_SY879_t.png"
}
```

200 OK · 236 ms · 841 B

```
{
    "id": 6,
    "title": "a book",
    "price": 100,
    "description": "book about a book",
    "image": "https://fakestoreapi.com/img/61IBBVJvSDL._AC_SY879_t.png",
    "category": "electronics"
}
```

- DELETE - delete a product - **DELETE {{baseUrl}}/products/{{id}}**



fakeStoreApi / Delete a product

DELETE {{baseUrl}} /products/ {{id}}

Pre-request

```
const random_id = Math.floor(Math.random() * 20) + 1;
pm.variables.set("id",random_id);
```

200 OK · 297 ms · 1000 B

```
{
    "id": 18,
    "title": "MBJ Women's Solid Short Sleeve Boat Neck V ",
    "price": 9.85,
    "description": "95% RAYON 5% SPANDEX, Made in USA or Imported, Do Not Bleach, Lightweight fabric with great stretch for comfort,
        Ribbed on sleeves and neckline / Double stitching on bottom hem",
    "category": "women's clothing",
    "image": "https://fakestoreapi.com/img/71z3kpMAYsL._AC_UY879_t.png",
    "rating": {
        "rate": 4.7,
        "count": 130
    }
}
```

- **CARTS**
  - GET - get all carts- **GET {{baseUrl}}/carts**
  - POST - add a new cart- **POST {{baseUrl}}/carts**
  - GET - get a single cart- **GET {{baseUrl}}/carts/{{id}}**
  - PUT - update a cart- **PUT {{baseUrl}}/carts/{{id}}**
  - DELETE - delete a cart**- DELETE {{baseUrl}}/carts/{{id}}**

- **USERS**
  - GET - get all users- **GET {{baseUrl}}/**users
  - POST - add a new user- **POST {{baseUrl}}/**users
  - GET - get a single user- **GET {{baseUrl}}/**users**/{{id}}**
  - PUT - update a user- **PUT {{baseUrl}}/**users**/{{id}}**
  - DELETE - delete a user**- DELETE {{baseUrl}}/**users**/{{id}}**

- **LOGIN**
  - POST - Authenticate a user - **POST {{baseUrl}}/auth/login**

LINK TO ACCESS THIS COLLECTION - https://elements.getpostman.com/redirect?entityId=51533843-884ae673-268c-4caf-bb9a-d25aa66d109d&entityType=collection

4. Identify Security Findings :

Finding 1: Open / Unauthenticated User Endpoints

Observation:

- /users , /users/{id} , /carts and /carts/{id} are accessible without authentication

Business Impact :

Anyone on the internet can retrieve user profile data without proving identity, increasing privacy and compliance risks.

Severity : HIGH

Remediation :

- Enforce authentication for all user-related endpoints
- Implement token-based access (OAuth2 / JWT)
- Restrict unauthenticated access to non-sensitive resources only

OWASP Mapping :

- **API1:2023 – Broken Object Level Authorization**
- **API2:2023 – Broken Authentication**

Finding 2: Excessive Data Exposure in API Responses

Observation :
User responses include:

- Email addresses
- Username
- Password hashes (even if fake)
- Address and phone data

Business Impact :

The API exposes more personal data than necessary, increasing the risk of data leakage and regulatory violations.

Severity : HIGH

Remediation :

- Apply response filtering (return only required fields)
- Use separate DTOs for public vs internal responses
- Mask or omit sensitive fields entirely

OWASP Mapping :

- **API3:2023 – Excessive Data Exposure**

Finding 3: Lack of Authorization Controls

Observation :

- Users and carts are accessed directly via /users/{id} , /carts/{id}
- No ownership or role validation

Business Impact :

A logged-in user could potentially access other users' data, leading to account takeover and trust loss.

Severity : HIGH

Remediation :

- Enforce object ownership checks
- Use server-side authorization logic
- Avoid direct object references without validation

OWASP Mapping :

- **API1:2023 – Broken Object Level Authorization**

Finding 4: Missing Rate Limiting

Observation :

- No rate-limit headers
- No throttling mentioned in documentation

Business Impact :

Attackers could scrape the entire database or abuse the API, impacting availability and business operations.

Severity : MEDIUM

Remediation :

- Implement IP- or token-based rate limiting
- Add monitoring and alerting
- Return 429 Too Many Requests

OWASP Mapping :

- **API4:2023 – Unrestricted Resource Consumption**

Finding 5: Weak Security Headers

Observation :

- No visible security-related response headers
- No cache-control for sensitive data

Business Impact :

Data may be cached or exposed unintentionally through browsers or intermediaries.

Severity: LOW

Remediation :

- Add Cache-Control: no-store
- Configure CORS (Cross Origin Resource sharing) properly
- Avoid exposing sensitive data in responses

OWASP Mapping

- **API7:2023 – Security Misconfiguration**

5. Ready-to-Use API Security Assessment :

You can reuse this for any API: https://elements.getpostman.com/redirect?entityId=51533843-884ae673-268c-4caf-bb9a-d25aa66d109d&entityType=collection

6.Findings Summary :

ID	Risk	Severity	OWASP
01	Unauthenticated user access	High	API2
02	Excessive data exposure	High	API3
03	Authorization flaws	High	API1
04	Missing rate limiting	Medium	API4
05	Security headers missing	Low	API7

Key Risks

1. User data is accessible without authentication
2. APIs expose more personal data than required
3. Authorization checks are missing
4. No protections against abuse or scraping

Why This Matters

These issues increase the risk of data leakage, privacy violations, service abuse, and loss of customer trust.

Recommended Actions

- Enforce authentication and authorization
- Minimize response data
- Implement rate limiting
- Apply standard API security headers

Overall Risk Rating

High – due to unrestricted access to user-related data

DISCLAIMER :

Fake Store API is a stateless mock API. DELETE endpoints return a simulated response but do not persist data changes. This limits its use to functional testing and learning, not security validation.