API SECURITY RISK ANALYSIS REPORT

TARGET API: JSONPLACEHOLDER

CYBER SECURITY INTERNSHIP – TASK 3

ORGANIZATION:
FUTURE INTERNS
PREPARED BY:
MAHADEV SAI CHANDRA

INTRODUCTION

APIS ARE A FUNDAMENTAL COMPONENT OF MODERN APPLICATIONS, PLAYING A CRUCIAL ROLE IN ENABLING DATA EXCHANGE BETWEEN DIFFERENT SYSTEMS. HOWEVER, IF APIS ARE NOT PROPERLY SECURED, THEY CAN EXPOSE SENSITIVE DATA, POTENTIALLY LEADING TO SERIOUS SECURITY INCIDENTS. THIS REPORT PROVIDES AN IN-DEPTH ANALYSIS OF A PUBLIC DEMO API TO IDENTIFY AND EXAMINE COMMON SECURITY RISKS ASSOCIATED WITH APIS.

TOOLS & METHODOLOGY

T**ools Used:**

- Postman
- Browser-based API testing
- Browser Developer Tools
- Public demo API

Methodology

The API endpoints were thoroughly tested using GET requests to observe the behavior related to authentication, authorization, and data exposure. The analysis was passive, meaning that it focused on observing the system's responses without engaging in any active exploitation or intrusive actions. This approach ensured that the testing process remained non-invasive, allowing for a detailed examination of the endpoints' security measures and potential vulnerabilities without compromising the system's integrity.

API RISK SUMMARY TABLE

API Risk	Risk Level	Business Impact
No Authentication	High	Unauthorized access
No Authentication	High	Privilege misuse
Lack of Authorization	Medium	Data leakage
Excessive Data Exposure	Medium	API abuse
No Rate Limiting	Medium	Injection risks

RISK 1: NO AUTHENTICATION

Risk Level: High

Description:
The API allows access to endpoints without requiring authentication.

Business Impact:
Any user can access sensitive data without verification.

Remediation:
Implement authentication using API keys or OAuth.

RISK 2: LACK OF AUTHORIZATION

Risk Level: High

Description:
The API does not enforce role-based access controls.

Business Impact:
Users may access data beyond their intended permissions.

Remediation:
Apply authorization checks for each API endpoint.

RISK 3: EXCESSIVE DATA EXPOSURE

Risk Level: Medium

Description:
The API returns more data than necessary in responses.

Business Impact:
Attackers can collect unnecessary user information.

Remediation:
Limit API responses to required data fields only.

RISK 4: NO RATE LIMITING

Risk Level: Medium

Description:
The API does not restrict the number of requests.

Business Impact:
The API may be abused or overloaded.

Remediation:
Implement rate limiting and request throttling.

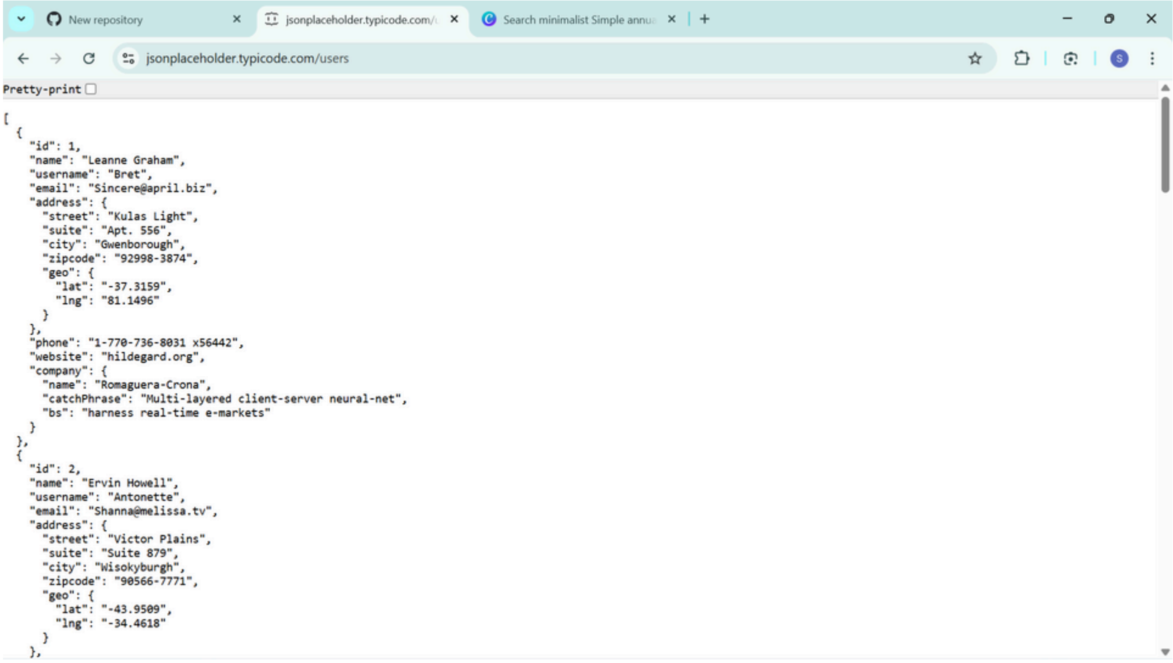
RISK 5: MISSING INPUT VALIDATION

Risk Level: Medium

Description:
User inputs are not validated properly.

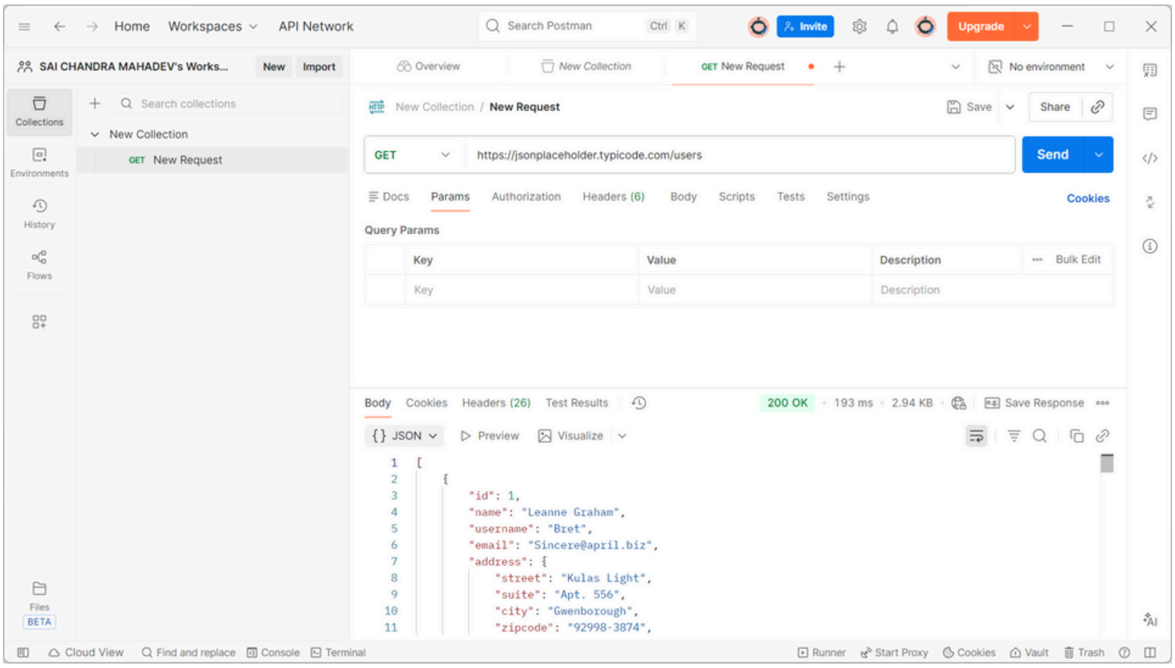
Business Impact:
This may lead to malformed or malicious requests.

Remediation:
Validate and sanitize all incoming API inputs.


New repository
jsonplaceholder.typicode.com/
Search minimalist Simple annu
jsonplaceholder.typicode.com/users
Pretty-print □

```
[
  {
    "id": 1,
    "name": "Leanne Graham",
    "username": "Bret",
    "email": "Sincere@april.biz",
    "address": {
      "street": "Kulas Light",
      "suite": "Apt. 556",
      "city": "Gwenborough",
      "zipcode": "92998-3874",
      "geo": {
        "lat": "-37.3159",
        "lng": "81.1496"
      }
    },
    "phone": "1-770-736-8031 x56442",
    "website": "hildegard.org",
    "company": {
      "name": "Romaguera-Crona",
      "catchPhrase": "Multi-layered client-server neural-net",
      "bs": "harness real-time e-markets"
    }
  },
  {
    "id": 2,
    "name": "Ervin Howell",
    "username": "Antonette",
    "email": "Shanna@melissa.tv",
    "address": {
      "street": "Victor Plains",
      "suite": "Suite 879",
      "city": "Wisokyburgh",
      "zipcode": "90566-7771",
      "geo": {
        "lat": "-43.9509",
        "lng": "-34.4618"
      }
    },
```

Figure tells about the unauthorized access of the website



New Collection / New Request

GET https://jsonplaceholder.typicode.com/users

200 OK · 193 ms · 2.94 KB

```
[
    {
        "id": 1,
        "name": "Leanne Graham",
        "username": "Bret",
        "email": "Sincere@april.biz",
        "address": {
            "street": "Kulas Light",
            "suite": "Apt. 556",
            "city": "Gwenborough",
            "zipcode": "92998-3874",
```

Figure: API response observed during testing

CONCLUSION

The API security assessment revealed a number of substantial risks that could potentially lead to unauthorized access and the exposure of sensitive data. These vulnerabilities could have serious implications for the integrity and confidentiality of the information being handled by the API. To address these concerns and bolster the security measures, it is crucial to implement robust authentication mechanisms to verify the identity of users accessing the API. Additionally, integrating comprehensive authorization protocols will ensure that users have appropriate permissions to access specific resources and perform certain actions. Furthermore, the introduction of rate limiting will help manage the frequency of requests and prevent abuse or overuse of the API, thereby enhancing both security and reliability. By taking these steps, the API will be better protected against potential threats, ultimately safeguarding user data and improving overall system stability.