Task 3 – API Security Risk Analysis Report

Cyber Security Internship – Future Interns

Name: Jatin Malik

---

1. Introduction

API security is an important part of modern applications. APIs are used to share data between applications and servers.

If APIs are not properly secured, attackers can misuse them to steal data or damage systems.

This report analyzes security risks found in a sample public API.

---

2. What is an API?

An API (Application Programming Interface) is a way for applications to communicate with each other.

For example, when a mobile app requests user data from a server, it uses an API to get that data.

---

3. API Selected for Analysis

API Name: JSONPlaceholder

Base URL: https://jsonplaceholder.typicode.com

Purpose:

JSONPlaceholder is a public demo API used for testing and learning. It provides sample data such as users, posts, and comments.

Authentication:

No authentication is required to access this API.

---

4. Identified Security Risks

1. Lack of Authentication

The API does not require login, API keys, or tokens.

Risk:

Any unauthorized user can access the API and misuse the data.

---

2. Open Endpoints

All endpoints like /users and /posts are publicly accessible.

Risk:

Attackers can easily collect large amounts of data.

---

3. No Rate Limiting

There is no limit on the number of requests sent to the API.

Risk:

The API can be abused or the server can be overloaded.

---

4. Data Exposure

The API returns complete datasets without filtering sensitive data.

Risk:

In real applications, this could lead to leakage of personal information.

---

5. Missing Input Validation

User input is not properly checked.

Risk:

Malicious inputs may cause unexpected behavior or vulnerabilities.

---

5. Impact Analysis

If these issues exist in real-world APIs, attackers could steal sensitive data, overload servers, and disrupt services.

This can cause financial loss and damage to an organization’s reputation.

---

6. Remediation Suggestions

- Implement authentication (API keys or tokens)
- Add rate limiting
- Validate all user inputs
- Restrict access to sensitive data
- Monitor API activity regularly

---

7. Conclusion

API security is essential for protecting applications and user data.

By implementing proper security controls, organizations can prevent misuse and cyber attacks.

---

8. Author

Jatin Malik