REPORT

API SECURITY RISK ANALYSIS

TITLE:API SECURITY RISK ANALYSIS
SUMBITTED BY:RENUGA P
COURSE:CYBER SECURITY LAB

Introduction

APIs (Application Programming Interfaces) are essential for modern applications because they enable communication between systems, mobile apps, and web services. However, insecure APIs can expose sensitive data, allow unauthorized access, and lead to cyberattacks. This report analyzes common API security risks, their impact, and recommended mitigation strategies.

Tools Used

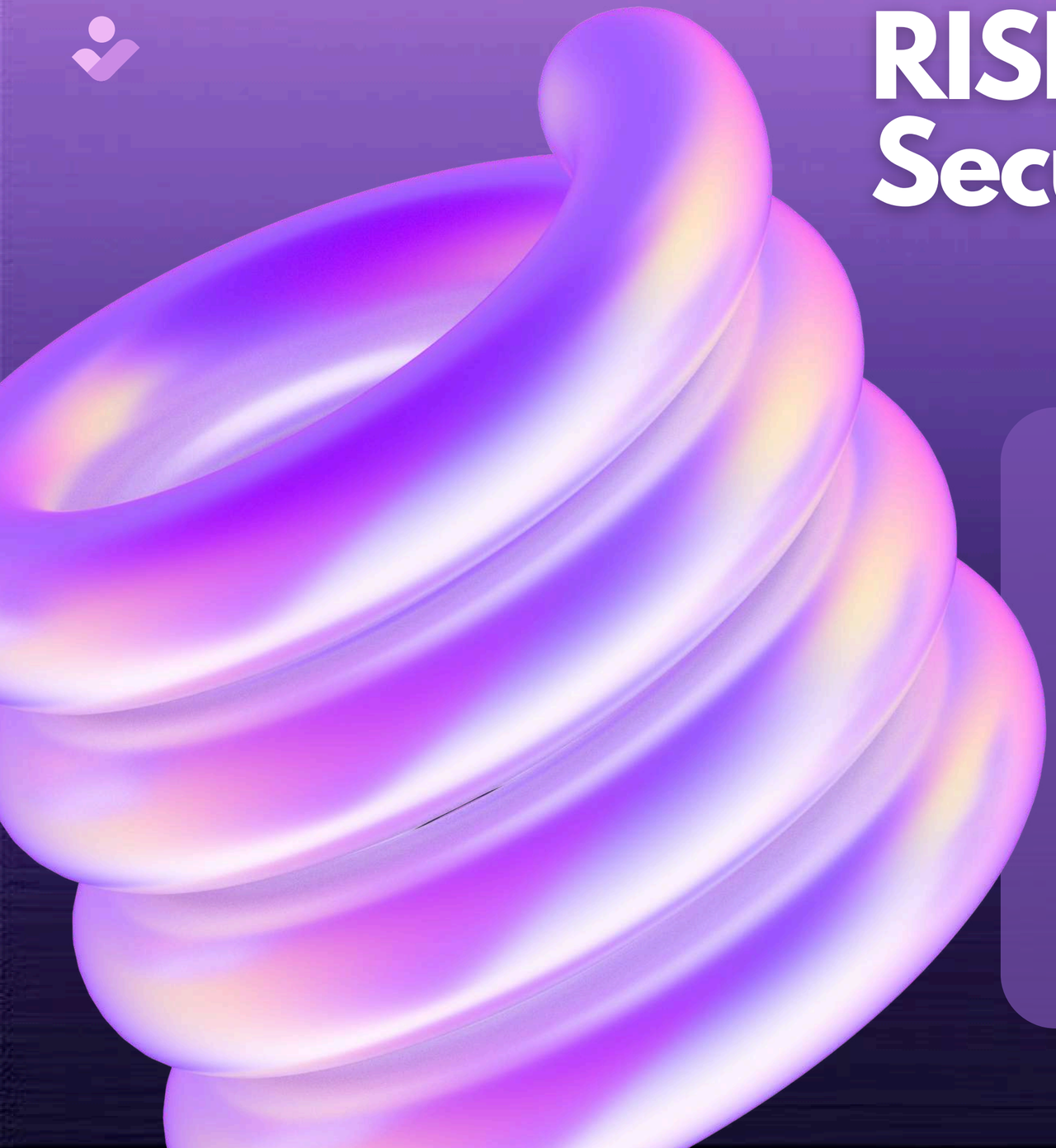
- Postman (API testing)
- Browser Developer Tools
- Sample Public Test APIs
- Documentation using MS Word / Google Docs

Methodology

The following steps were used to perform the API security assessment:

1. Identified available API endpoints.
2. Tested authentication and authorization mechanisms.
3. Checked for sensitive data exposure in responses.
4. Verified input validation and error handling.
5. Tested for rate limiting and access control.

RISK 1:dentified Security Risks



Risk 1: Broken Authentication

Description: Weak or missing authentication allows attackers to access APIs without proper login.
Impact: Unauthorized users may access private data.
Example: API accepts requests without tokens.

Remediation:

Implement strong authentication (JWT, OAuth)
Enforce token expiration and secure storage

Risk 2: Broken Authorization

Description: API does not properly verify user permissions.
Impact: Users can access or modify other users' data.

Remediation:
Apply role-based access control (RBAC).
Validate user identity on every request.

Risk 3: Sensitive Data Exposure

Description: API responses contain confidential data such as passwords or personal information.
Impact: Data leaks may lead to identity theft or privacy breaches.

Remediation:

Encrypt sensitive data.
Avoid sending unnecessary information in API responses.

Risk 4: Lack of Rate Limiting

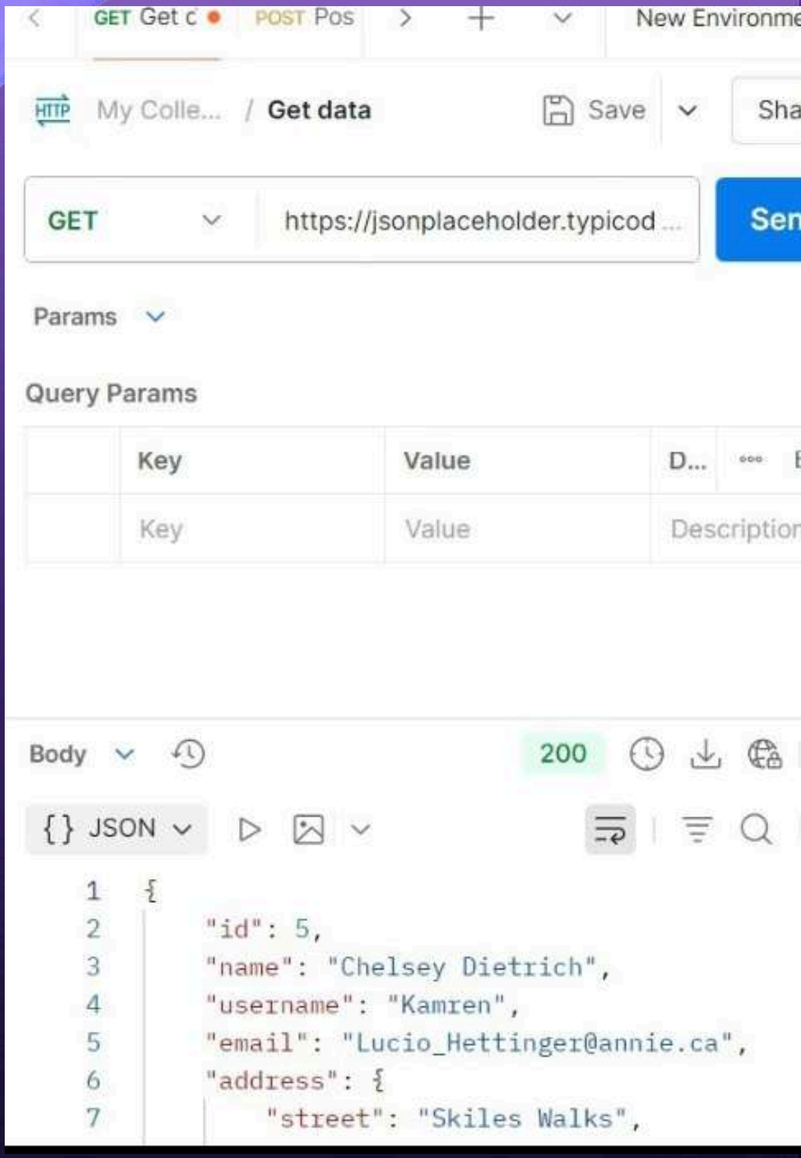
Description: No restriction on request frequency.
Impact: Attackers can perform brute force or denial-of-service attacks.

Remediation:
Implement rate limiting.
Use throttling and request monitoring.

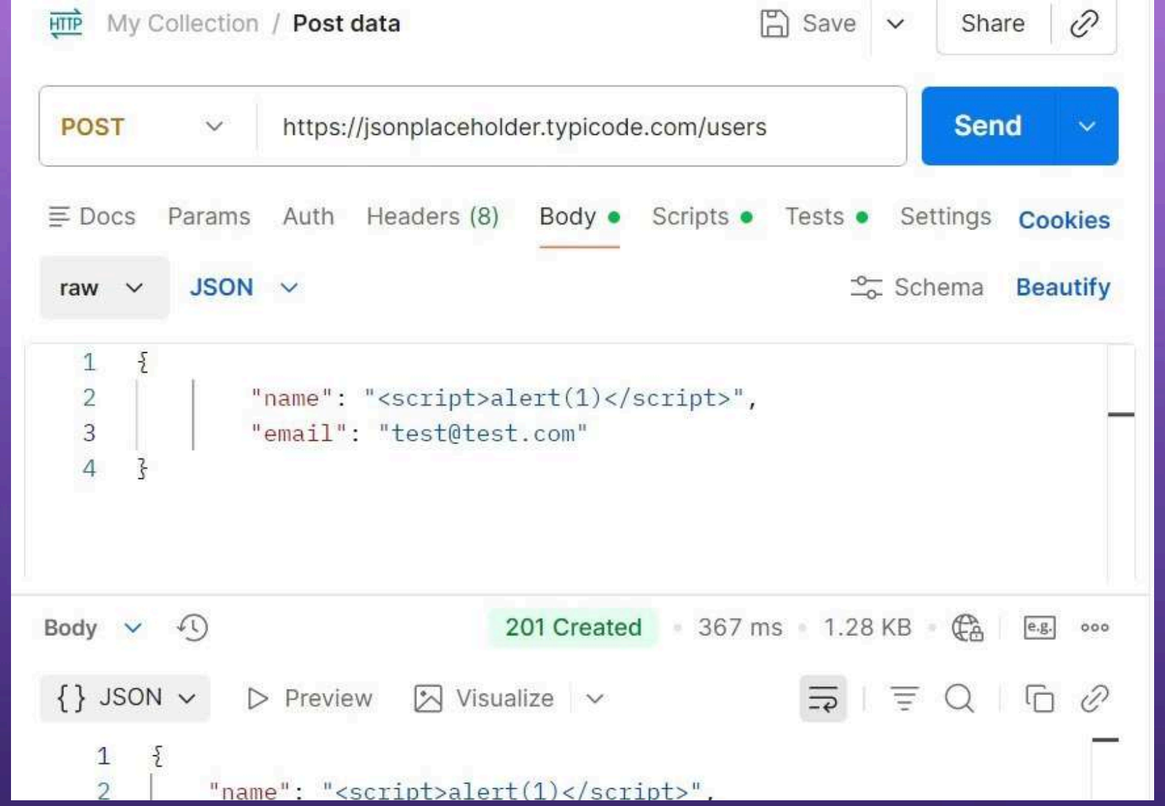
Risk 5: Improper Input Validation

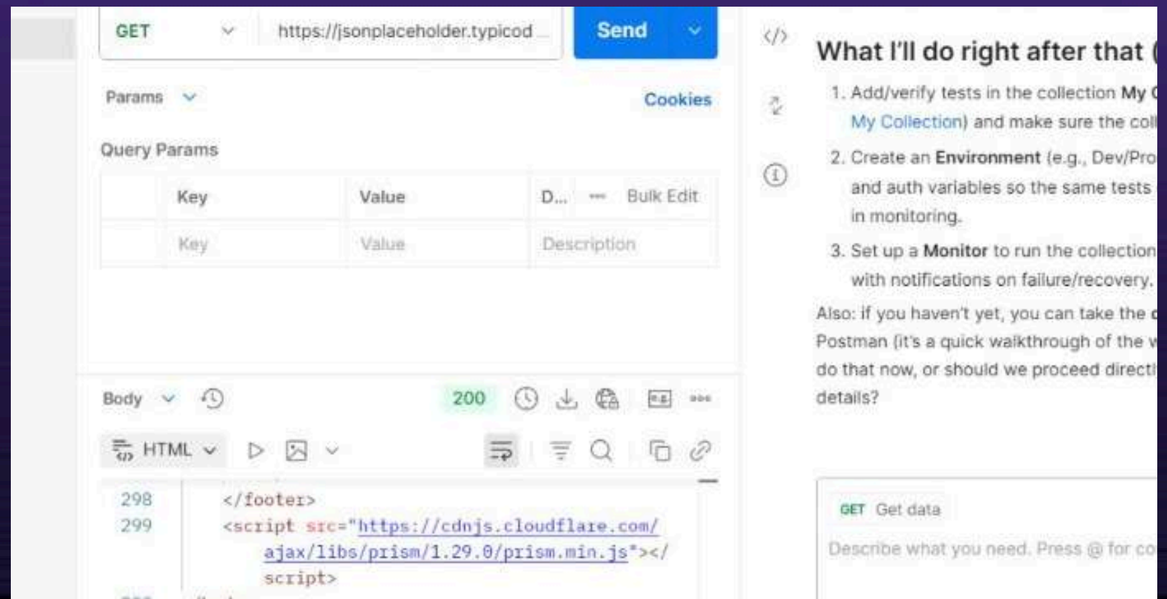
Description: API accepts invalid or malicious input.
Impact: May lead to injection attacks or system crashes.

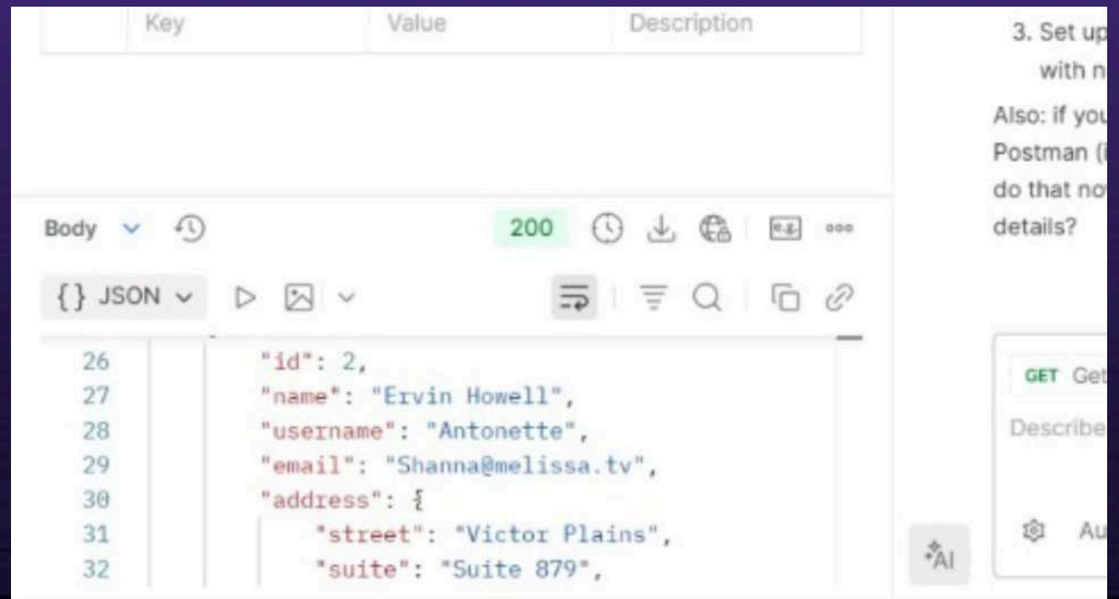
Remediation:
Validate all user inputs.
Use input filtering and sanitization.



Tool used:postman







Risk Impact Summary

Risk Type| Severity| Impact
Broken Authentication| High| Unauthorized access
Broken Authorization| High| Data manipulation
Data Exposure| High| Privacy breach
No Rate Limiting| Medium| System overload
Poor Validation| Medium| Injection attacks

Conclusion

The API security analysis identified multiple risks related to authentication, authorization, data protection, and input validation. Implementing strong security controls, monitoring mechanisms, and proper validation techniques will significantly reduce the risk of cyberattacks and improve overall API security.

Recommendations

Use secure authentication methods.
Encrypt sensitive data transmissions.
Implement access control policies.
Apply rate limiting and logging.
Conduct regular API security testing.

References

OWASP API Security Top 10
API Security Best Practices ocumentation
Cybersecurity Fundamentals Study Materials