

API Security Testing Report

Introduction:

API (Application Programming Interface) security testing is the process of analyzing APIs to identify security weaknesses and vulnerabilities that could be exploited by attackers. APIs are widely used in web and mobile applications to transfer data between client and server. If not properly secured, APIs can expose sensitive information, allow unauthorized access, and lead to data breaches.

API security testing ensures confidentiality, integrity, and availability of data by checking authentication, authorization, input validation, encryption, and error handling mechanisms.

Objectives of API Security Testing:

- 1 Identify security vulnerabilities in APIs
- 2 Ensure proper authentication and authorization
- 3 Protect sensitive data from exposure
- 4 Prevent unauthorized access and attacks
- 5 Improve overall application security

Testing Methodology:

The API security testing process included reviewing API endpoints, testing authentication mechanisms, validating input parameters, checking data exposure, and monitoring server responses. Tools such as Postman and basic penetration testing techniques were used to analyze API behavior and responses.

Identified Vulnerabilities Mapped to OWASP API Risks:

- 1 Broken Object Level Authorization (OWASP API1): API allowed access to other users' data without proper authorization checks.
- 2 Broken Authentication (OWASP API2): Weak login mechanism allowed multiple failed login attempts without account lockout.
- 3 Excessive Data Exposure (OWASP API3): API responses exposed sensitive user information such as email and phone numbers.
- 4 Lack of Rate Limiting (OWASP API4): No restriction on repeated requests, making API vulnerable to brute-force and DoS attacks.
- 5 Security Misconfiguration (OWASP API7): Default settings and unnecessary services enabled on server.
- 6 Improper Assets Management (OWASP API9): Old and unused API endpoints still active and accessible.

Recommendations:

Implement strong authentication and authorization controls, enable rate limiting, encrypt sensitive data, disable unused endpoints, and regularly monitor API logs. Conduct periodic security testing and follow OWASP API Security Top 10 guidelines to enhance security.

Conclusion:

API security testing is essential to protect modern web and mobile applications. Identifying

vulnerabilities and mapping them to OWASP risks helps organizations strengthen their security posture and prevent data breaches. Regular monitoring and secure coding practices are necessary for maintaining safe and reliable APIs.