Cloud API Penetration Testing Report

1. Introduction

This report summarizes a penetration test performed on a publicly available cloud-based demo API. The objective was to identify vulnerabilities using OWASP ZAP and propose mitigation steps before app deployment.

2. Setup and Configuration

OWASP ZAP was installed on a local Kali Linux environment. Proxy settings were configured to intercept API calls. Passive and active scanning features were utilized, along with the spidering tool to map the API structure.

3. Target API Overview

The test targeted a demo RESTful API available publicly at 'https://example-api.com'. This API simulates user registration, login, and data retrieval operations, mimicking a real mobile application backend.

4. Key Findings & Remediations

1. **Insecure Direct Object Reference (IDOR):** API exposed user account details via predictable user IDs. Remediation: Implement authorization checks on object-level access.

2. **SQL Injection:** Detected through query parameters in login endpoint. Remediation: Use parameterized queries and input validation.

3. **Excessive Data Exposure:** API responses contained full user objects, including sensitive metadata. Remediation: Use data filtering to return only necessary fields.

5. Conclusion & Recommendations

The OWASP ZAP tool successfully identified three high-severity vulnerabilities. Implementing the proposed mitigations will reduce the risk of data breaches, elevate API security, and ensure compliance with best practices. Continuous scanning is recommended as the API evolves.