Vulnerability Assessment & Penetration Testing Report

Prepared for: Acme Corp (Sample)
Date: January 13, 2026

Classification: CONFIDENTIAL
Assessment Type: Black Box / Web Application
Version: 1.0

1. Executive Summary

WarnHack was commissioned to perform a Vulnerability Assessment and Penetration Test (VAPT) on the external web application infrastructure of Acme Corp. The objective was to identify security weaknesses that could be exploited by malicious actors to compromise the confidentiality, integrity, or availability of the systems.

During the engagement, our team identified a total of 8 vulnerabilities, including 1 Critical and 2 High severity issues. The most significant finding was a SQL Injection vulnerability in the login module which could allow an unauthenticated attacker to bypass authentication and access the database.

We strictly recommend addressing the Critical and High severity issues immediately to prevent potential data breaches.

Summary of Findings

1	2	5	0
CRITICAL	HIGH	MEDIUM	LOW

2. Technical Details

Severity: Critical | CVSS Score: 9.8

Description:
The application login endpoint (/api/auth/login) fails to properly sanitize user input in the "username" field. By injecting malicious SQL payloads, an attacker can manipulate the backend query.

Proof of Concept (PoC):

```
POST /api/auth/login HTTP/1.1
Host: target.com
Content-Type: application/json

{
    "username": "admin' OR '1'='1",
    "password": "anything"
}
```

Result: HTTP 200 OK - Logged in as Administrator.

Impact:
An attacker can bypass authentication, access all user accounts, extract the entire database, or modify data.

Remediation:
Use Parameterized Queries (Prepared Statements) for all database interactions. Input validation should also be enforced.

Severity: High | CVSS Score: 7.5

Description:
Authenticated users can access the profiles of other users by simply changing the "user_id" parameter in the URL. There is no check to ensure the requester owns the requested object.

Impact:
Unauthorized access to sensitive personal information (PII) of other users.

Remediation:
Implement proper access control checks on every API request accessing a specific object ID. Ensure "current_user.id == requested_user.id".

3. Methodology

Our methodology follows industry standards including OWASP Testing Guide v4, NIST SP 800-115, and OSSTMM.

- Information Gathering (OSINT)
- Threat Modeling
- Vulnerability Analysis (Automated Scanning + Manual Verification)
- Exploitation (Safe, Authorized)
- Reporting