Security Report Copilot

PENETRATION TEST REPORT

Acme Corp — External Web Application Assessment

Prepared for Acme Corp

DATE
July 29, 2026

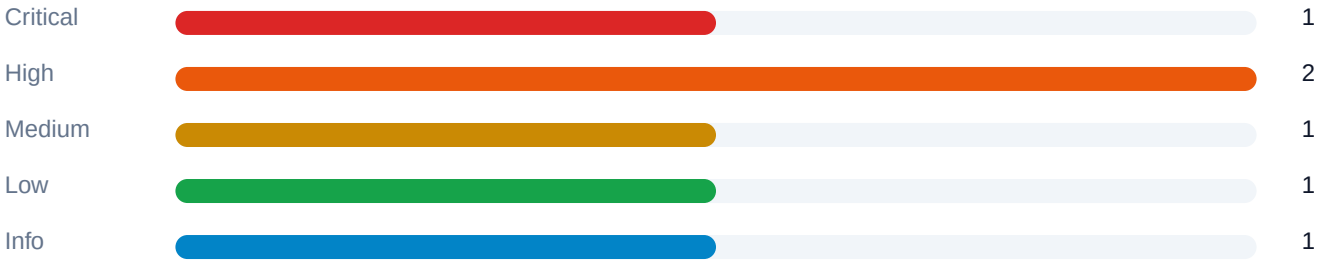
FINDINGS
6

Executive Summary

This assessment of Acme Corp identified 6 approved findings across the scope below. The severity breakdown and detailed findings follow.

Black-box penetration test of Acme Corp's customer-facing web application and supporting API, conducted over a five-day engagement window.

1	2	1	1	1
CRITICAL	HIGH	MEDIUM	LOW	INFO



Findings

CRITICAL

1. SQL Injection in the authentication endpoint

CVSS 9.8 • CWE-89 • https://app.acme.com/api/v1/login

DESCRIPTION

The `username` parameter of the login endpoint is concatenated directly into a SQL query without parameterization. A crafted payload (e.g. `' OR '1'='1' -- `) alters the query logic and bypasses authentication.

BUSINESS IMPACT

An unauthenticated attacker can bypass login, enumerate accounts, and exfiltrate the entire user database — including password hashes and PII. This is a full confidentiality and integrity compromise of the application's primary data store.

EVIDENCE

Request: POST /api/v1/login {"username":"' OR 1=1-- ","password":"x"}
Response: 200 OK with a valid session cookie for the first user in the table.

REMEDIATION

Use parameterized queries / prepared statements for all database access. Apply least-privilege to the application database role, and add a WAF rule as defence-in-depth. Re-test after remediation.

REFERENCES

https://owasp.org/www-community/attacks/SQL_Injection
https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

HIGH 2. Insecure Direct Object Reference (IDOR) on order records

CVSS 8.1 • CWE-639 • https://app.acme.com/api/v1/orders/{id}

DESCRIPTION

The orders API returns any order by numeric ID without verifying that the order belongs to the authenticated user. Incrementing the `id` discloses other customers' orders.

BUSINESS IMPACT

Any authenticated customer can read all other customers' orders, exposing names, addresses, and partial payment details across the entire customer base.

EVIDENCE

Authenticated as user A (order 10472), requesting /api/v1/orders/10471 returns user B's full order record.

REMEDIATION

Enforce object-level authorization on every request: verify the requested resource is owned by (or shared with) the authenticated principal. Prefer unguessable identifiers (UUIDs) as defence-in-depth.

REFERENCES

https://owasp.org/Top10/A01_2021-Broken_Access_Control/

HIGH 3. Stored Cross-Site Scripting (XSS) in user profile display name

CVSS 7.4 • CWE-79 • https://app.acme.com/profile

DESCRIPTION

The display-name field is rendered without output encoding. A payload stored in the profile executes in the browser of any user who views it, including administrators in the support console.

BUSINESS IMPACT

An attacker can hijack sessions, perform actions as the victim, or pivot to administrative accounts viewing the support console — leading to account takeover.

EVIDENCE

Setting display name to `<img src=x onerror=alert(document.domain)>` executes script when the profile is viewed in the admin support console.

REMEDIATION

Context-aware output encoding on all user-controlled data. Add a strict Content-Security-Policy. Validate and sanitize on input as a secondary control.

REFERENCES

https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

MEDIUM 4. Missing rate limiting on password-reset endpoint

CVSS 5.3 • CWE-307 • https://app.acme.com/api/v1/password-reset

DESCRIPTION

The password-reset endpoint accepts unlimited requests, enabling user enumeration via differing responses and facilitating token brute-force and email-bombing.

BUSINESS IMPACT

Attackers can enumerate valid accounts and abuse the endpoint to flood users with reset emails, harming deliverability and user trust.

EVIDENCE

1,000 requests in 30s all returned 200 with no throttling.

REMEDIATION

Apply per-IP and per-account rate limiting with exponential backoff. Return a uniform response regardless of account existence.

REFERENCES

https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

LOW 5. Security headers missing (HSTS, CSP, X-Content-Type-Options)

CVSS 3.7 • CWE-693 • https://app.acme.com/

DESCRIPTION

Responses lack key security headers. There is no HSTS, no Content-Security-Policy, and no X-Content-Type-Options, weakening defence-in-depth against downgrade and injection attacks.

BUSINESS IMPACT

Increases the exploitability and impact of other issues (e.g. XSS) and exposes users to protocol-downgrade and MIME-sniffing attacks.

EVIDENCE

Response headers reviewed across all endpoints; the above headers were absent.

REMEDIATION

Add Strict-Transport-Security, a tuned Content-Security-Policy, X-Content-Type-Options: nosniff, and Referrer-Policy at the edge/proxy layer.

REFERENCES

https://owasp.org/www-project-secure-headers/

INFO 6. Verbose error messages disclose stack traces

CWE-209 • https://app.acme.com/api/v1/*

DESCRIPTION

Unhandled errors return full stack traces and framework versions, revealing internal paths and dependency versions useful for targeting further attacks.

BUSINESS IMPACT

Information disclosure that aids an attacker in fingerprinting the stack and crafting targeted exploits.

EVIDENCE

Sending malformed JSON to several API endpoints returned a 500 with a full stack trace.

REMEDIATION

Return generic error responses to clients; log details server-side only. Disable debug mode in production.