PENETRATION TEST REPORT

Security Assessment
Sample Report

Client: Acme Technologies Inc. (Anonymized)
Scope: Web Application + REST API
Type: Grey-box Penetration Test
Date: March 2025
Prepared by: Silentfault Security LLC

2	3	4	2
CRITICAL	HIGH	MEDIUM	LOW

Total: 11 findings identified across all severity levels

Executive Summary

Silentfault conducted a grey-box penetration test of Acme Technologies Inc.'s web application and REST API between March 10–17, 2025. The engagement was scoped to the primary SaaS platform at **app.acmeinc.com** and its underlying API endpoints. The testing team was provided with standard user-level credentials to simulate a realistic authenticated attacker scenario.

The assessment revealed **11 security vulnerabilities**, including 2 Critical-severity findings that could allow an unauthenticated attacker to fully compromise the platform and access all customer data. Immediate remediation is strongly recommended before the next funding round or SOC2 audit. All findings have been communicated with actionable remediation guidance and will be validated during the retest phase included in this engagement.

Risk Distribution

Severity	Count	Examples	Status
Critical	2	SQL Injection, Auth Bypass	Remediation Required
High	3	BOLA, JWT Bypass, SSRF	Remediation Required
Medium	4	Rate Limiting, Exposed Endpoints	Recommended
Low	2	Security Headers, Verbose Errors	Best Practice

Engagement Scope

Target	Details
Web Application	app.acmeinc.com (primary SaaS platform)
REST API	api.acmeinc.com/v2 — 47 endpoints tested
Authentication	Standard user + admin role credentials provided
Out of Scope	Mobile apps, third-party integrations, physical security

Methodology

All testing was conducted in accordance with industry-standard frameworks and methodologies. Our team follows a structured approach to ensure comprehensive coverage while minimizing impact on production systems.

Framework	Application
OWASP Top 10 (2021)	Full coverage of all 10 vulnerability categories including A01-A10
PTES	Penetration Testing Execution Standard for structured methodology
NIST SP 800-115	Technical guide for information security testing and assessment
CVSS v3.1	Common Vulnerability Scoring System for severity classification

Tools Used

Category	Tools
Web App Testing	Burp Suite Professional, OWASP ZAP
Network Scanning	Nmap, Masscan, Shodan
Exploitation	Metasploit Framework, custom scripts
API Testing	Postman, custom Python scripts, ffuf
Recon	Amass, Subfinder, theHarvester, Wayback Machine

Testing Timeline

Phase	Dates	Activities
Kickoff & Scoping	Mar 10	Scope definition, credential setup, rules of engagement
Reconnaissance	Mar 11	Passive & active recon, endpoint enumeration
Active Testing	Mar 12–15	Manual exploitation, vulnerability validation

Reporting	Mar 16–17	Report writing, evidence compilation, recommendations
Retest	Apr 3	Validation of all critical & high severity remediations

Detailed Findings

Critical SQL Injection — Authentication Bypass — CVSS 9.8

ID: SF-001	**Endpoint:** POST /api/v2/auth/login	**Parameter:** username

Description

The login endpoint is vulnerable to SQL injection via the **username** parameter. An unauthenticated attacker can bypass authentication entirely by injecting a malicious SQL payload, gaining access to any account including administrator accounts without knowledge of the password.

Business Impact

Full authentication bypass. An attacker can log in as any user, including administrators, without valid credentials. This allows complete takeover of the platform and access to all customer data stored in the database.

Steps to Reproduce

1. Send POST request to /api/v2/auth/login
2. Set username parameter to: admin' OR '1'='1'--
3. Set password to any value
4. Server returns 200 OK with valid JWT token for admin account

Remediation

Use parameterized queries or prepared statements for all database interactions. Never concatenate user input directly into SQL queries. Implement an ORM layer if not already in use. Validate and sanitize all input server-side.

Critical Broken Object Level Authorization (BOLA) — CVSS 9.1

ID: SF-002	**Endpoint:** GET /api/v2/users/{id}/data	**Parameter:** id (path parameter)

Description

The API does not validate that the authenticated user has permission to access the requested resource. By manipulating the **id** parameter in the URL, any authenticated user can access the data of any other user, including billing information, personal details, and API keys.

Business Impact

Complete horizontal privilege escalation. Any authenticated user can access the full profile, payment methods, and API keys of every other user in the system. This represents a critical data breach risk affecting all customers.

Steps to Reproduce

1. Log in as user A (ID: 1001)
2. Send GET /api/v2/users/1002/data with user A's token
3. Server returns full profile data for user 1002
4. Iterate IDs to enumerate all user records

Remediation

Implement object-level authorization checks on every API endpoint. Verify that the authenticated user's ID matches the requested resource owner. Use indirect object references (UUIDs) instead of sequential IDs. Conduct a full audit of all API endpoints for similar authorization issues.

High

JWT None Algorithm Accepted

CVSS 8.1

ID: SF-003	Endpoint: All authenticated endpoints	Parameter: Authorization header

Description

The application accepts JWT tokens signed with the **none** algorithm, which means an attacker can forge valid tokens without knowing the secret key. By modifying any valid JWT and changing the algorithm to "none", an attacker can impersonate any user including administrators.

Business Impact

Authentication bypass via token forgery. An attacker can create a token for any user ID and access their account with full privileges without needing the signing secret.

Steps to Reproduce

1. Obtain a valid JWT token through normal login
2. Base64-decode the header and change alg to 'none'
3. Modify the payload to change the user ID to target
4. Remove the signature and send the forged token
5. Server accepts the token and grants access to target account

Remediation

Explicitly reject the "none" algorithm in JWT validation. Maintain an allowlist of accepted algorithms (e.g., RS256, HS256). Use a well-maintained JWT library with secure defaults. Rotate the current signing secret immediately.

High

Server-Side Request Forgery (SSRF)

CVSS 7.5

ID: SF-004	Endpoint: POST /api/v2/integrations/webhook	Parameter: url

Description

The webhook integration endpoint accepts a URL parameter that is fetched server-side without validation. An attacker can supply internal URLs to probe the internal network, access cloud metadata endpoints (AWS/GCP), or interact with internal services not exposed to the internet.

Business Impact

Internal network exposure. An attacker can enumerate internal services, access cloud provider metadata (including IAM credentials via AWS metadata endpoint at 169.254.169.254), and potentially pivot to internal systems.

Steps to Reproduce

1. Send POST /api/v2/integrations/webhook
2. Set url to: http://169.254.169.254/latest/meta-data/iam/security-credentials/
3. Server fetches URL and returns AWS IAM credentials in response

Remediation

Implement a strict allowlist of permitted URL schemes and domains. Block requests to private IP ranges (10.x, 172.16.x, 192.168.x) and cloud metadata endpoints. Use a dedicated outbound proxy for webhook requests. Disable internal DNS resolution for user-supplied URLs.

Retest Results

A retest was conducted on April 3, 2025 to validate remediation of all Critical and High severity findings. The following table summarizes the remediation status of each finding.

ID	Finding	Severity	Status	Notes
SF-001	SQL Injection — Auth Bypass	Critical	Fixed	Parameterized queries implemented. Verified.
SF-002	Broken Object Level Authorization	Critical	Fixed	Auth checks added to all endpoints. Verified.
SF-003	JWT None Algorithm Accepted	High	Fixed	Algorithm allowlist enforced. Secret rotated.
SF-004	Server-Side Request Forgery	High	In Progress	Partial fix applied. Allowlist incomplete.
SF-005	Missing Rate Limiting on Login	Medium	Fixed	Rate limiting added: 5 attempts/minute.
SF-006	Exposed Internal API Endpoints	Medium	Fixed	Endpoints moved behind auth middleware.
SF-007	Verbose Error Messages	Low	Fixed	Generic error messages returned in production.
SF-008	Missing Security Headers	Low	Fixed	CSP, HSTS, X-Frame-Options headers added.

7 of 8 findings resolved · 1 In Progress · 0 Accepted Risk

Penetration Test Attestation Letter

April 3, 2025

To Whom It May Concern,

This letter serves as formal attestation that **Silentfault Security LLC** conducted a comprehensive penetration test of the web application and API infrastructure operated by **Acme Technologies Inc.** between **March 10–17, 2025**.

The assessment was conducted by certified security professionals holding active credentials including CEH, OSCP, eCPPT, and AWS Red Team certifications. The engagement followed industry-standard methodologies including OWASP Top 10 (2021), PTES, and NIST SP 800-115.

A total of **11 security vulnerabilities** were identified and reported to the client's engineering team with full technical details and remediation guidance. A formal retest was conducted on **April 3, 2025**, confirming that **7 of 8 critical and high severity findings have been fully remediated**. One High severity finding remains in progress.

This report and attestation may be shared with investors, auditors, and enterprise customers as evidence of security due diligence. This engagement satisfies the penetration testing requirements for SOC2 Type II compliance under the Availability and Security trust service criteria.

Sincerely,

Silentfault Security LLC

Penetration Testing & Security Assessment

hello@silentfault.io · silentfault.com