Acme Inc.

Pentest by Strac Comply

SOC 2 Evidence

Compliance Evidence

Report ID	`sample-acme-2026-08-14`
Version	3
Report date	14 August 2026
Classification	Confidential: shareable under NDA
Entity	Acme Inc.
System owner	Platform Engineering
Prepared for	Acme Inc. Audit Committee

Executive Summary

An external application penetration test of https://app.acme.example was performed on 14 August 2026 using OWASP Web Security Testing Guide 4.2 and OWASP API Security Top 10 2023. 4 findings were identified: 1 critical, 2 medium and 1 low. The most severe is **SQL Injection in /api/search**.

Of these, 4 were demonstrated during testing.

1 critical or high finding of the 5 tracked against this target, including findings carried over from earlier tests, remains outstanding at the date of this report.

Compliance Evidence Summary

Test period	14 August 2026
Environment	Production
Test type	External application penetration test
Test trigger	Periodic (scheduled)
Scope	• app.acme.example
Target tested	https://app.acme.example
Methodology	Testing drew on test cases from the OWASP Web Security Testing Guide v4.2 and the OWASP API Security Top 10 (2023), and followed the phases of NIST SP 800-115 and the PCI SSC Penetration Testing Guidance (2017). Findings are rated with CVSS 3.1.
Authentication	Credentials supplied by the customer; authenticated testing performed
Tester	Strac's automated testing platform
Authorisation	Domain ownership verified by DNS. *This is a technical proof of domain control.*
Tester independence	Independence is asserted on an organizational basis, and testing was automated.
Tester qualification	Automated testing platform *Review and Acceptance has space for a named, qualified reviewer.*

Findings by severity

Critical	High	Medium	Low	Info	Not rated
1	0	2	1	0	0

Counts the 4 findings identified by this test. The remediation figures below cover every finding tracked against this target.

Remediation status

High / critical verified fixed	Findings retested	Outstanding critical / high
1 / 2	1 / 5	1

Counts cover every finding tracked against this target, including findings from earlier tests. Verified fixed means a retest confirmed the finding no longer reproduces.

Remediation history in this report covers 11 March 2026 to 14 August 2026. Keep this report and your remediation records for your audit period.

Using this report as audit evidence

This copy carries no proof-of-concept material or captured traffic. Acme Inc. may share it with its customers, prospects and auditors under a non-disclosure agreement. The full technical report for this run carries that material for 1 of the 4 findings above. To confirm a finding independently, request the technical report alongside this copy.

Testing Methodology

Testing was performed by AI agents that explore the target and attempt attacks, rather than by a fixed scanning playbook or a signature database. Each step below gives this run's figures.

1. **Reconnaissance.** The agent first maps the reachable attack surface of the target and the technologies behind it, rather than testing a predetermined list of paths. 29 distinct endpoints were exercised in this run.
2. **Hypothesis.** From what recon found, the agent forms specific, target-shaped hypotheses about where a control may fail, and pursues them as separate lines of work. What it attempted is listed under Testing Performed.
3. **Exploitation.** The agent attempts to demonstrate each hypothesis by executing it against the target and observing the result, not by matching a response against a signature. 2431 individual actions were recorded.
4. **Validation.** Where an exploit ran and its effect was observed, the finding is marked validated. Other findings are reported from observed indicators. In this run 4 of 4 findings were validated.
5. **Independent severity review.** A separate review stage re-rates each finding on the OWASP Risk Rating likelihood-by-impact matrix, and each re-rated finding states the change.

Every step above was performed by an automated testing platform. A named reviewer at the assessed entity can take responsibility for its conclusions under Review and Acceptance.

Changes Since Last Report (since 19 May 2026)

Remediated and verified	New findings	Reopened	Risk accepted	Open past 90 days
1	2	0	1	1

SOC 2 Control Mapping

What this document is

This test ran on 14 August 2026 and evidences the design and existence of controls on that date. Operating effectiveness over a review period is evidenced by a series of tests across that period.

CC4.1 asks for ongoing *and* separate evaluations. One test evidences one evaluation. For a Type II examination covering a review period, the evidence is a series of these reports spanning that period, retained together with the remediation record for each, so that the cadence itself is visible.

This document is technical evidence for a SOC 2 examination. It is not an examination, an opinion, or a report issued under AT-C 205, and it confers no compliance status.

Controls this test supports

Controls for which this engagement provides positive evidence.

Built from the 4 findings identified by this test. Findings carried over from earlier tests appear in Remediation Tracking and are not mapped here. Rows evidencing a control about REMEDIATION draw on every finding tracked against this target, because a fix verified since the last test is a fix to a finding identified earlier; they are listed in Remediation Tracking.

Control	Name	Evidenced by
CC4.1	Ongoing and/or separate evaluations of controls	**All 4 findings identified by this test.**
CC4.2	Deficiencies evaluated and communicated	**All 4 findings identified by this test.**
CC7.1	Vulnerability and malware detection	**All 4 findings identified by this test.**
CC7.5	Vulnerabilities remediated	Reflected XSS in /support

Controls this test evidences in part

Each control below is evidenced in part. The limb this engagement evidences is stated beside it.

Built from the 4 findings identified by this test. Findings carried over from earlier tests appear in Remediation Tracking and are not mapped here.

Control	Name	What this test evidences
CC4.2	Deficiencies evaluated and communicated	Deficiencies identified and evaluated: each finding in this report carries a severity rating.

Control gaps this test identified

Controls the findings below indicate are **deficient**. Each row is evidence of a gap in the control, shown by the finding beside it.

Built from the 4 findings identified by this test. Findings carried over from earlier tests appear in Remediation Tracking and are not mapped here.

Control	Name	Finding indicating the gap
CC6.1	Logical access controls	SQL Injection in /api/search

Control mapping version 2.1.0.

Testing Performed

29 endpoints exercised across 2431 recorded actions.

Areas tested:

- Injection
- Authentication
- Cross-Site Scripting
- IDOR / Broken Access Control
- Server-Side Request Forgery

Findings

Applies to every finding below

- Every CVSS metric below was assessed by automated review.

SQL Injection in /api/search

Critical

`A05:2025 Injection · CWE-89 · https://app.acme.example/api/search · CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (9.8)`

Description

The `q` parameter is concatenated into a SQL statement without parameterization.

Impact

Unauthenticated read access to the entire application database, including password hashes.

Proof-of-concept material and captured traffic are in the full technical report.

Validated. Demonstrated against the target during testing.

Remediation

Use parameterized queries. Rotate all stored credentials.

Session cookie missing the Secure attribute

Medium

`A02:2025 Security Misconfiguration · CWE-614 · https://app.acme.example/login · CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N (5.3)`

Description

The `acme_session` cookie is set without the `Secure` attribute.

Impact

The session cookie can be transmitted over cleartext HTTP if a downgrade occurs.

No proof-of-concept material was recorded for this finding.

Validated. Demonstrated against the target during testing.

Remediation

Set `Secure` and `SameSite=Lax` on all session cookies.

Verbose error pages disclose stack traces

Medium

`A10:2025 Mishandling of Exceptional Conditions · API8:2023 Security Misconfiguration · CWE-209 · https://app.acme.example/api/* · CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N (5.3)`

Description

Unhandled exceptions return a full framework stack trace.

Impact

Discloses library versions and internal file paths, easing further attack.

No proof-of-concept material was recorded for this finding.

Validated. Demonstrated against the target during testing.

Remediation

Return a generic error body in production.

Missing HTTP Strict-Transport-Security header

Low

`A06:2025 Insecure Design · CWE-693 · https://app.acme.example/ · CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N (3.1)`

Description

Responses do not carry an HSTS header.

Impact

A first-visit downgrade attack is not prevented.

No proof-of-concept material was recorded for this finding.

Validated. Demonstrated against the target during testing.

Remediation

Add `Strict-Transport-Security: max-age=31536000; includeSubDomains`.

Remediation Tracking

The corrective-action record for all 5 findings tracked against this target, including findings from earlier tests. **Last retest** shows the date of the most recent retest and its outcome. A fix is verified when a retest confirms the finding no longer reproduces.

Finding	Severity	Status	First seen	Last retest	Closed
SQL Injection in /api/search	Critical	Open	14 August 2026	Not retested	Not closed
Session cookie missing the Secure attribute	Medium	Open	02 May 2026	Not retested	Not closed
Verbose error pages disclose stack traces	Medium	Open	14 August 2026	Not retested	Not closed
Reflected XSS in /support	High	Fixed: confirmed by retest on 10 August 2026	18 April 2026	10 August 2026 *not reproduced*	10 August 2026
Missing HTTP Strict-Transport-Security header	Low	Risk accepted by Acme Inc. on 1 June 2026 *Accepted by the customer on 01 June 2026: Accepted pending CDN migration in Q4.*	11 March 2026	Not retested	Not closed

Review and Acceptance

This report was produced by an automated testing platform.

Your named reviewer signs here.

Reviewed by

Role and qualification	
Date of review	
Signature	

The engagement record names Jordan Avery, Head of Security as the attesting officer for this entity: the person who accepted the engagement. The block above records who reviewed this report.

Document Control

Document	Report sample-acme-2026-08-14, version 3
Issued	14 August 2026
Prepared by	Strac's automated testing platform
Review and approval	Generated by an automated testing platform. A named reviewer at the assessed entity can sign under Review and Acceptance.
Evidence model	model 1.0.0; control mapping 2.1.0
Supersedes	Version 2 of this report. Earlier versions describe the same test; remediation status moves between them.

Acme Inc. may share this document with its customers, prospects and auditors under a non-disclosure agreement.