01 / 09 · COVER

Penetration test report

Web application and API

SAMPLE · FICTITIOUS DATA

Acme is a made-up company and acme.example a reserved test domain. Every value in this report is invented to show the structure of a real one.

REPORT	RHE-RPT-2026-031
PREPARED FOR	Acme (fictitious)
TARGET	shop.acme.example · api.acme.example
TEST PERIOD	18.08.2026 to 31.08.2026
ISSUED	31.08.2026, version 1.0
TESTED AND SIGNED BY	Rheono · Samir Abis
STATE AT ISSUE	1 high open, fix due 15.09.2026

CONTENTS

01 Cover 1
02 Scope 2
03 Method 2
04 Summary 3
05 Findings 3
06 Worked finding 4
07 Retest 5
08 Control mapping 6
09 Signature 6

02 SCOPE AND RULES OF ENGAGEMENT

The customer signed this scope on 14.08.2026, before the first request. The authorization is valid for 90 days. A host that is not listed is never touched.

HOSTS IN SCOPE	shop.acme.example · api.acme.example
NOT IN SCOPE	mail · vpn · status · intranet.acme.example, never touched
API	/v1/* · OpenAPI spec attached
ROLES	admin · staff · customer (testuser1, testuser2), with your test accounts
TEST WINDOW	18.08.2026 to 31.08.2026
RATE LIMIT	1 request / second
DATA-CHANGING TESTS	Approved in writing, on the two test accounts only
EMERGENCY STOP	Portal pause · emergency channel

SIGNED · AUTHORIZATION ON FILE

03 HOW THE HUNT RAN

Agents mapped the hosts in scope, then tested them. The lead agent stays off the target and hands out one slice at a time: access control, authentication, business logic. Engineer agents come back with a working exploit, and a validator agent tries to break it before it counts.

MAP	Subdomains, endpoints and login flows on the hosts in scope, and nothing outside them.
EXPLOIT	Engineer agents work one slice at a time and come back with a working exploit, not a flag.
VALIDATE	Three checks, below. One check fails and the finding is dropped before it reaches you.
REVIEW AND SIGN	The signatory reviews every finding that goes into the report and signs it.
RETEST	When a fix is live, the original attack is replayed. The finding closes only when it fails.

THREE CHECKS BEFORE A FINDING COUNTS

01 FOUND	The engineer agent proves the weakness once, with a working exploit.
02 CHALLENGED	A validator agent in a separate session gets only the claim, the endpoint and the scope, and tries to reproduce it from scratch.
03 REPLAYED	Where the bug class allows, the exploit reruns as a scripted replay without a model, and the request and response are captured.

One candidate failed the second check in this period, an open redirect on the login page: the allowlist blocked every external host the validator tried. It was dropped and is not a finding.

SEVERITY

CVSS 3.1 base scores. Critical 9.0 to 10.0, High 7.0 to 8.9, Medium 4.0 to 6.9, Low 0.1 to 3.9.

NOT TESTED

- Denial of service or load testing, unless you approve it in writing
- Destructive attacks, and data-changing tests outside the two test accounts
- Hosts you did not authorize, and third-party services they call
- Internal networks, mobile binaries, social engineering and physical access

04 EXECUTIVE SUMMARY

CRITICAL	HIGH	MEDIUM	LOW
0	2	2	1

CLOSED AFTER RETEST	3
OPEN	1
RISK ACCEPTED	1

Acme's shop and order API were tested from 18.08.2026 to 31.08.2026, inside the signed scope. Five findings passed all three checks.

The most serious one let any logged-in customer read every other customer's orders, with addresses and payment references, and change the delivery address of their open orders. Acme fixed it in release 2026.08.2, and the retest on 26.08.2026 found it closed.

One high stays open: the login request passes input to the database, and it can be read without an account. The fix is due by 15.09.2026 and is retested once it is live.

WHAT TO DO FIRST

1. Ship the fix for RHE-2026-043 and ask for the retest.
2. Check ownership on the server in every /v1 endpoint that takes an ID, not only /v1/orders.
3. Encode user input in the staff views by default, so the next note field is safe too.

05 FINDINGS

ID	SEVERITY	FINDING	ASSET	CVSS	STATUS
RHE-2026-041	HIGH	IDOR: any customer reads and changes other customers' orders (CWE-639)	api.acme.example/v1/orders/{id}	8.1	Closed · retest passed 26.08.2026
RHE-2026-043	HIGH	SQL injection in the login request, read without an account (CWE-89)	shop.acme.example/api/login	7.5	Open · fix due 15.09.2026
RHE-2026-044	MEDIUM	Stored XSS: a customer's order note runs script in the staff order view (CWE-79)	shop.acme.example/account	5.4	Closed · retest passed 29.08.2026
RHE-2026-045	MEDIUM	SSRF: webhook URLs reach internal addresses, cloud metadata blocked (CWE-918)	api.acme.example/v1/webhooks	5.0	Closed · retest passed 30.08.2026
RHE-2026-046	LOW	Password reset timing shows whether an account exists (CWE-208)	shop.acme.example/login	3.7	Risk accepted by name · 28.08.2026

Every finding passed all three checks. Each one ships as a bundle like the worked finding in section 06.

06 WORKED FINDING

IDOR: sequential order IDs let any customer read and change other customers' orders

FINDING	RHE-2026-041
ASSET	https://api.acme.example/v1/orders
SEVERITY	High
CVSS	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N (8.1)
CWE	CWE-639
OWASP	API1:2023 Broken Object Level Authorization
VRT	Access Control (BAC)
CHECKS	3/3: found, challenged, replayed
ISO 27001	A.8.3 · A.8.26 (2022)
SOC 2	CC6.1
NIS2	Art. 21(2)(e) and (f)

IMPACT

Order IDs are sequential and the API never checks ownership. Any logged-in customer can read the full order history of any other customer, items, addresses and payment references, and change the delivery address of their open orders, by changing the ID. No privilege escalation: one low-value test account exposes every other account.

DESCRIPTION

GET and PATCH on /v1/orders/{id} accept any order id. The ownership check exists only in the frontend; the API accepts the session of any authenticated user for any order id.

REPRODUCTION

1. Log in as the provided test account (testuser1) and keep the session cookie.
2. GET /v1/orders/1001: own order, HTTP 200 (baseline).
3. GET /v1/orders/1002: another customer's order, HTTP 200, full payload (evidence/response-order-1002.json).
4. Run evidence/poc.sh: enumerates ids 1001 to 1010, all return 200 (evidence/enumeration-log.txt).
5. PATCH /v1/orders/2001, an open order of the second test account (testuser2), with a new delivery address from testuser1's session: HTTP 200, address changed, then reverted (evidence/patch-order-2001.http).

EVIDENCE

- evidence/poc.sh: working PoC (bash, read-only)
- evidence/request-order-1002.http: raw request
- evidence/response-order-1002.json: full order payload of a foreign account
- evidence/patch-order-2001.http: delivery address of the second test account changed, then reverted
- evidence/enumeration-log.txt: 41 foreign orders read

REMEDIATION

Enforce object-level authorization: resolve the owner server-side from the authenticated session and reject requests

where the resource owner does not match, for reads and writes; add regression test coverage.

THE DELIVERABLE, PER FINDING

```
RHE-2026-041-idor-orders.zip
|-- report.md
|-- evidence/
|   |-- poc.sh
|   |-- request-order-1002.http
|   |-- response-order-1002.json
|   |-- patch-order-2001.http
|   `-- enumeration-log.txt
|-- retest/
|   `-- retest-2026-08-26.log
`-- CHECKSUMS.txt
```

EVIDENCE/POC.SH

```
#!/usr/bin/env bash
# PoC: IDOR on /v1/orders/{id} (acme.example, fictitious sample)
# Read-only: uses the customer-provided test account, mutates nothing.
BASE="https://api.acme.example/v1"
COOKIE="session=***"   # testuser1

for id in $(seq 1001 1010); do
  code=$(curl -s -o /dev/null -w '%{http_code}' -H "Cookie: $COOKIE" "$BASE/orders/$id")
  echo "order $id -> HTTP $code"
done
# observed: 1001 = 200 (own), 1002..1010 = 200 (other customers' orders)
```

CHECKSUMS.TXT

```
3f2ac91e…  evidence/poc.sh
b81e44d0…  evidence/request-order-1002.http
d4c07a19…  evidence/response-order-1002.json
5c19e7a3…  evidence/patch-order-2001.http
9e5f22b6…  evidence/enumeration-log.txt
a07d3e58…  retest/retest-2026-08-26.log
```

SHA-256, shortened here. The file in the bundle carries the full hashes, so anyone can check that no evidence changed after signing.

07 RETEST

07 / 09 · SAMPLE

FIRST FOUND	24.08.2026
FIXED	25.08.2026 (release 2026.08.2)
RETESTED	26.08.2026, verified closed

RETEST RESULT

- GET /v1/orders/1002 from testuser1: HTTP 404.
- PATCH /v1/orders/2001 from testuser1: HTTP 404, the address of testuser2's order unchanged.
- poc.sh: 1001 returns 200 (own order), 1002 to 1010 return 404.
- Evidence: retest/retest-2026-08-26.log, a07d3e58… in CHECKSUMS.txt.

One high (SQL injection in /api/login) stays open in the next cycle, because that is the honest state. It closes after fix and retest, by 15.09.2026 at the latest.

08 CONTROL MAPPING

The usual mapping, not a certification. Your auditor decides what counts for your audit.

FRAMEWORK	CLAUSE	WHAT THIS REPORT EVIDENCES
NIS2, Directive (EU) 2022/2555	Art. 21(2)(e)	Vulnerability handling: each finding with its fix and a dated retest that shows it closed.
NIS2, Directive (EU) 2022/2555	Art. 21(2)(f)	A dated check that the measures work: an attacker's attempt against them, inside the signed scope.
ISO 27001, ISO/IEC 27001:2022	A.8.8	Management of technical vulnerabilities: findings with CVSS, remediation and retest results.
ISO 27001, ISO/IEC 27001:2022	A.8.29	Security testing in development and acceptance: a test after each release you approve, with dates.
ISO 27001, ISO/IEC 27001:2022	A.8.34	Protecting systems during testing: the signed rules of engagement in section 02.
SOC 2, AICPA Trust Services Criteria	CC4.1	A separate evaluation. Penetration testing is one of the kinds the points of focus list.
SOC 2, AICPA Trust Services Criteria	CC7.1	Procedures that find vulnerabilities, with each one fixed and retested.

cSquare GRC, our GRC partner, can map the signed report to the controls you carry and track the fixes. Neither of us audits or certifies you.

09 SIGNATURE

ATTESTATION

Rheono tested the scope above externally and non-destructively. Every finding was validated with a working proof of concept and reviewed by the signatory, Samir Abis. No guarantee of the completeness of all weaknesses and no guarantee of regulatory compliance.

Next snapshot: by 08.12.2026 or right after the next release.

SIGNATURE

Samir Abis · signatory, rheono

Signed 31.08.2026

`Advanced electronic signature (eIDAS, PAdES-B-T) + RFC 3161 timestamp`

The signature proves who issued the report and that it has not changed since. It is not an audit opinion: only your auditor signs a SOC 2 report or issues an ISO 27001 certificate.