EXCERPT · FICTIONAL CLIENT

SECTRICITY
OUTSMART HACKERS

PENETRATION TEST REPORT EXCERPT

External pentest web platform and API

Acme Logistics Ltd · customer portal, public API and login flow

CLIENT
Acme Logistics Ltd

TEST PERIOD
2 to 13 March

METHOD
OWASP WSTG · grey box

CLASSIFICATION
Confidential

01 · EXECUTIVE SUMMARY

Where does Acme stand today?

An attacker can view other customers' data through the public API. Two findings need a fix this week; the rest fits into normal planning.

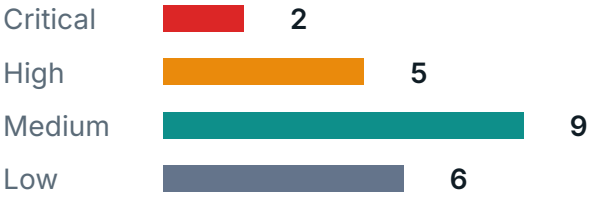
OVERALL RISK



High

expected after retest: low

Findings by severity



22 findings · all confirmed by hand

Top 3 to fix first

CRITICAL	**Access to other customers' orders**	API does not check who owns the order
CRITICAL	**Password reset without rate limit**	Reset codes can be guessed
HIGH	**Outdated component in portal**	Known vulnerability, update available

Advice. Fix the two critical issues, then schedule the retest. It is included and confirms the fix works.

This week
Fix 2 critical issues

Within 30 days
5 high issues

Within 90 days
Medium and low, then retest

02 · FINDING SEC-01

Access to other customers' orders

9.1
CVSS · CRITICAL

Component	Impact	Status
Public API	**Customer data leak**	**Open**

What we found

By changing the order number in the request, a logged-in customer can see other customers' orders, addresses and invoices.

Evidence

```
GET /api/v2/orders/10482 HTTP/1.1
Authorization: Bearer [redacted]

200 OK {"order":10482,"customer":"[redacted]","address":"[redacted]"}
```

How to fix it

1. Check on every request that the order belongs to the logged-in customer.
2. Use unpredictable order IDs.
3. Log and alert on many sequential IDs.

Why this matters

Personal data of all customers is open to anyone with an account. That is a data breach you must report under GDPR.

Retest: **included** within 90 days of the report

03 · REMEDIATION PLAN

What to do when?

Every finding gets a deadline, based on severity and how easily an attacker can exploit it.

THIS WEEK

Critical

- SEC-01 · Access to other customers' orders
- SEC-02 · Password reset without rate limit

WITHIN 30 DAYS

High

- SEC-03 · Outdated component
- SEC-04 · Session stays valid after logout
- SEC-05 · CORS setting too permissive

WITHIN 90 DAYS

Medium and low

- 9 medium findings
- 6 low findings
- Header hardening

What is already good

- ✓ Strong encryption of traffic
- ✓ Admin panel not reachable from the internet
- ✓ No sensitive data in error messages

Retest Included within 90 days of the report. We test every fixed finding again and confirm in writing that the fix works.