rhyno

EXTERNAL NETWORK & WEB APPLICATION SCAN

Security Exposure Report

SAMPLE — ILLUSTRATIVE & REDACTED

TARGET	SCAN TYPE	FINDINGS
acme-sample.io	External + Web App	14 (3 critical)

This is a sample report. Targets, hosts and findings shown here are illustrative and redacted. Your scan reports on your own assets, with full, unredacted detail and step-by-step remediation.

Executive summary

3	6	5	14
Critical	High	Medium	Total

The assessment surfaced multiple paths an attacker could use to reach customer data directly — an exposed database, an unauthenticated admin panel, and world-readable cloud storage. None require sophisticated tooling; each is reachable from the open internet today. The critical items below should be remediated immediately; the recommended fixes are included with each finding.

Findings & fixes

CRITICAL Finding 01

Publicly exposed database — no authentication

`host [redacted].acme-sample.io : 5432/tcp (PostgreSQL)`

A production database was reachable directly from the public internet with authentication disabled. Anyone who found the host could read or modify every record.

RECOMMENDED FIX

Remove the database from the public internet (bind to private network / VPC), require authentication, and rotate all credentials.

CRITICAL Finding 02

Unauthenticated admin panel

`https://app.acme-sample.io/admin — 200 OK`

The administrative console returned 200 OK with no login required, exposing user management and configuration to unauthenticated visitors.

RECOMMENDED FIX

Put the admin panel behind authentication + IP allow-listing and audit recent access.

CRITICAL Finding 03

World-readable cloud storage rules

`firebase project [redacted] — rules: public`

Storage/security rules were set to public, exposing an estimated 1.2M customer records (PII) to anyone with the project URL.

RECOMMENDED FIX

Lock rules to authenticated, least-privilege access; review access logs for exposure.

HIGH Finding 04

API key leaked in frontend bundle

`https://acme-sample.io/static/main.js`

A live third-party API key was shipped into client-side JavaScript, where any visitor can extract and abuse it (billing fraud, data access).

RECOMMENDED FIX

Revoke the key, move the call server-side, and scan the bundle for other secrets.

HIGH Finding 05

Outdated SSH with known exploits

`host [redacted].acme-sample.io : 22/tcp — OpenSSH 7.4`

The exposed SSH service is several versions behind and matches 3 published CVEs with public exploit code.

RECOMMENDED FIX

Patch to a current release and restrict SSH exposure to a bastion / VPN.

MEDIUM Finding 06

Missing transport & content security headers

`https://acme-sample.io (all responses)`

HSTS and Content-Security-Policy were absent, widening exposure to downgrade and injection attacks.

RECOMMENDED FIX

Add HSTS, a tuned CSP, and the standard hardening headers at the edge.