SECURITY ASSESSMENT | SAMPLE REPORT

Web Application & API Security Assessment

An illustrative sample of the assessment report Offload Security delivers — findings, evidence, remediation, and full OWASP / SOC 2 / ISO 27001 / GDPR mapping.

Target	app.example-demo.com (illustrative)
Assessment type	Web application + API security assessment
Standards	OWASP Top 10, OWASP API Top 10, OWASP ASVS, SOC 2, ISO 27001:2022, GDPR
Prepared by	Offload Security
Classification	Sample / illustrative data — not a real engagement

This is a **sample document** using illustrative data to demonstrate report structure and depth. It does not describe a real system or engagement.

1. Executive summary

The assessment identified **7 findings** across the web application and its APIs: **1 Critical**, **2 High**, **3 Medium** and **1 Low**. The most serious issue is a SQL injection vulnerability in the reporting API (SAMPLE-01) that allows unauthenticated extraction of database contents; it should be remediated immediately. A broken object-level authorization flaw (SAMPLE-02) lets authenticated users access other tenants' records. The remaining findings are configuration and hardening gaps that materially reduce the application's resilience.

Overall security rating: **C — Needs improvement.** Closing the Critical and High findings would raise the rating to B. None of the findings require architectural redesign; all have clear, documented remediation.

Findings by severity

Severity	Count	Example
Critical	1	SQL injection in reporting API
High	2	Broken object-level authorization; weak session expiry
Medium	3	Missing security headers; verbose errors; outdated library
Low	1	Cookie without SameSite attribute

2. Scope & methodology

Scope: the web application at app.example-demo.com and its REST API (/api/v1). Authenticated (standard user) and unauthenticated testing. Out of scope: infrastructure, physical, and social engineering.

Methodology: testing followed OWASP ASVS and combined automated scanning (OWASP ZAP, Nuclei, an OWASP API Top-10 scanner) with manual verification. Every reported finding was manually confirmed and risk-scored with CVSS, enriched by CISA KEV and EPSS exploitability.

3. Standards coverage

Each finding in this report is mapped to the controls below, so security and audit teams work from one result.

Finding	OWASP	API	SOC 2	ISO 27001	GDPR
SAMPLE-01 SQL injection	A03	—	CC7.1	A.8.28	Art. 32
SAMPLE-02 Broken object auth	A01	API1	CC6.1, CC6.3	A.5.15, A.8.3	Art. 32
SAMPLE-03 Missing security headers	A05	API8	CC6.6	A.8.9	Art. 32
SAMPLE-04 Weak session expiry	A07	API2	CC6.1	A.5.16	Art. 32
SAMPLE-05 Outdated component	A06	—	CC7.1	A.8.8	Art. 32

4. Detailed findings

SAMPLE-01 — SQL Injection in reporting API	CRITICAL
OWASP	A03: Injection
Affected asset	POST /api/v1/reports/query — 'filter' parameter
Description	The 'filter' parameter is concatenated directly into a SQL query without parameterization. An unauthenticated attacker can inject SQL to read or modify arbitrary database contents.
Evidence	`filter=1' UNION SELECT username,password_hash FROM users-- → returned 4,182 user records`
Impact	Full database disclosure including credentials; potential data modification. Directly exploitable, no authentication required.
Remediation	Use parameterized queries / prepared statements for all database access. Add input validation and least-privilege DB credentials. Deploy a WAF rule as an interim control.
Control mapping	OWASP A03 • SOC 2 CC7.1 • ISO 27001 A.8.28 • GDPR Art. 32 • CVSS 9.8 • EPSS High

SAMPLE-02 — Broken Object-Level Authorization (BOLA)	HIGH
OWASP	A01 / API1: BOLA
Affected asset	GET /api/v1/accounts/{id}
Description	The API returns account records by ID without verifying the requester owns the account. Changing {id} returns other tenants' data.
Evidence	`GET /api/v1/accounts/1043 (as user for account 2290) → 200 OK, returned foreign account data`
Impact	Cross-tenant data exposure; a standard user can enumerate and read every account. High regulatory impact under GDPR.
Remediation	Enforce object-level authorization on every request server-side; verify the authenticated principal owns the requested object. Use unpredictable identifiers.
Control mapping	OWASP A01 / API1 • SOC 2 CC6.1, CC6.3 • ISO 27001 A.5.15, A.8.3 • GDPR Art. 32 • CVSS 8.1

SAMPLE-03 — Missing security headers	MEDIUM
OWASP	A05: Security Misconfiguration
Affected asset	All application responses
Description	Responses omit Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options and X-Frame-Options, increasing exposure to XSS, clickjacking and protocol-downgrade attacks.
Evidence	`Response headers: (no CSP, no HSTS, no X-Frame-Options observed)`
Impact	Weakens defense-in-depth; makes client-side attacks easier to land if another flaw is present.
Remediation	Add CSP, HSTS (with preload), X-Content-Type-Options: nosniff and X-Frame-Options: DENY at the edge/app layer.
Control mapping	OWASP A05 / API8 • SOC 2 CC6.6 • ISO 27001 A.8.9 • GDPR Art. 32 • CVSS 5.3

5. Appendix — tools & methodology

Tool	Purpose	Version
OWASP ZAP	Web application scanning & active testing	2.15.x
Nuclei	Template-based vulnerability detection	3.x
API Top-10 scanner	OWASP API Security Top 10 testing	current
testssl.sh	TLS / certificate analysis	3.2.x
Manual testing	Verification, business-logic & auth testing	—

Severity is scored with CVSS v3.1 and enriched with CISA KEV (known-exploited) and EPSS (exploit-probability) context. All findings in this sample are illustrative.