Skylos code-scan evidence mapped to OWASP Top 10 2025

Full edition: contains vulnerability detail. Confidential.

This document shows what Skylos, a code-scanning tool, found in the code of Example Co (fictional sample), mapped to OWASP Top 10 2025. Skylos Cloud generated it on 2026-11-10 09:00:00Z at the request of owner@example.com.

It is not an OWASP Top 10 assessment; only a qualified assessor can decide whether a requirement is met.

What a code scan can show here

Requirements listed	Need other evidence	A code scan can evidence	- no open findings	- open findings
10	0	10	7	3

A code scan can give evidence toward all 10 requirements listed.

For the 10: 7 had no open findings from the Skylos rules mapped to them and 3 had open findings. No open findings is not proof that a requirement is met.

Skylos scan-policy result (Skylos default security policy, revision 2). Not an OWASP Top 10 result or a determination of compliance:

Policy not met

At least one CRITICAL or HIGH security, secret or dependency finding is still open after its fix-by date.

2 projects in scope; 2 of 2 had a trusted, complete scan in the last 90 days with every check the policy needs. Scans of each repository's default branch, as resolved by Skylos Cloud at upload.

Do these first

1. Fix now: HIGH SQL injection (SKY-D211) in example-api, app/orders/db.py:48. Its fix-by date 2026-10-30 has passed.
2. Fix before the deadline: 2 open CRITICAL or HIGH findings, the first due 2026-11-14. After that date the policy will not pass.
3. Assessment-freshness deadline 2027-02-08 (example-api): after it, this report would stop counting the project's latest trusted scan (older than 90 days).

1 more action is in the full list of 4 under What to do next on the next page.

Check the record Skylos stored for this report (it is not signed), then compare its key facts with this copy:

https://skylos.dev/verify/report/00000000-0000-4000-8000-000000000010

How to read this report

- Trusted scan: A scan uploaded from CI (GitHub or GitLab OIDC, or a project token an admin marked for CI) or run by Skylos Cloud. Uploads from a developer machine are unverified and never count.
- Skylos scan-policy result: Skylos's own rule about open CRITICAL and HIGH findings and their fix-by dates. It reads "Policy met", "Policy met, fixes due", "Policy not met" or "Not assessed". Section 3 has the rule.
- Requirement status: What the scans show for one requirement, such as Open findings or No open findings from mapped rules. Section 8 defines each status.

What to do next

1. Fix now: HIGH SQL injection (SKY-D211) in example-api, app/orders/db.py:48. Its fix-by date 2026-10-30 has passed.
2. Fix before the deadline: 2 open CRITICAL or HIGH findings, the first due 2026-11-14. After that date the policy will not pass.
3. Assessment-freshness deadline 2027-02-08 (example-api): after it, this report would stop counting the project's latest trusted scan (older than 90 days).
4. 1 approved exception ends within 30 days (first 2026-12-10). Fix the finding or renew the exception before then.

Contents

How to read this report . . . 2
What to do next . . . 2
Report details . . . 2
1. Executive summary . . . 3
2. Scope and scans included in report . . . 3
3. Policy evaluation . . . 3
4. Standards mapping: OWASP Top 10 2025 . . . 4
5. Findings . . . 4
6. Exceptions and suppressions . . . 5
7. Trend and issues no longer detected . . . 5
8. Methodology and definitions . . . 6
9. Limitations and disclaimer . . . 7
10. Integrity and verification . . . 8

Report details

Prepared for	Example Co (fictional sample)
Generated at (UTC)	2026-11-10 09:00:00Z
Generated by	owner@example.com
Report ID	00000000-0000-4000-8000-000000000010
Projects analysed	2 of 2 projects assessed (trusted, complete, current scan of the reported branch); 2 of 2 also ran every check the policy needs (security, secrets, dependencies); 2 of 2 have at least one scan.
Branch rule	Scans of each repository's default branch, as resolved by Skylos Cloud at upload.
Analyses included	Static security analysis (SAST); Secret detection; Dependency vulnerabilities (SCA); Quality analysis
Window for issues no longer detected	2026-08-12 to 2026-11-10; findings and the policy result come from each project's latest assessed scan
Report SHA-256	509544e376ecea919d30318a2f1a5c2eb0b68a091b1ec92fe1e03e3af0d3a9e9
Signature	Unsigned: no signing key was configured in Skylos Cloud when this report was generated. The SHA-256 and the verification page still detect changes to the stored report.
Verify the stored record	The link at the foot of every page. Section 10 says what the verification page shows and how to check a copy.
Generator	Skylos Cloud build sample; mapping 2026-11-08.2; CLI rule catalog 5.6.0; renderer 2026-11-13.1

1. Executive summary

Policy status (Skylos default security policy, revision 2):

Policy not met

- 1 open CRITICAL or HIGH finding is past the fix deadline.

Before exceptions the policy status would be Policy not met. The status is about the stated policy, not a determination about OWASP Top 10.

Open in this report	CRITICAL	HIGH	Past fix-by	Suppressed	Active exceptions	New since previous	No longer detected in the period
4	1	2	1	1 (20%)	1	-	1

Requirements listed: 10. Open findings: 3; No open findings from mapped rules: 7; Scan activity recorded: 0; Deviation noted: 0; Not scanned: 0; Not evidenced by static analysis: 0.

Skylos scans give evidence toward 10 of the 10 listed requirements of OWASP Top 10 2025 (through mapped findings or scan activity); that is not proof they are met. The other 0 need manual, runtime or process evidence, or no Skylos rule checks them, and are listed with the reason. All 10 categories of the OWASP Top 10:2025.

2. Scope and scans included in report

2 of 2 projects assessed (trusted, complete, current scan of the reported branch); 2 of 2 also ran every check the policy needs (security, secrets, dependencies); 2 of 2 have at least one scan.

Project	Business criticality	Assessment	Scan, branch, commit	CLI, completed, how uploaded	Coverage
example-api example/example-api	High	**Assessed**	c47617ea-ee98-4cce-83e8-a5664a4cd767 main 761ccd2a5ff0bba9875cdeebd7c0f0370e8c6c35	5.6.0 2026-11-10 06:30:00Z Verified CI (GitHub OIDC)	complete (full repository); checks: security, secrets, dependencies, quality, dead_code; dependencies: 42 queried
example-api: Trusted (CI with GitHub OIDC), complete scan of the default branch.					
example-web example/example-web	Medium	**Assessed**	ebb16937-3208-48d8-845a-8f4bdb2cab30 main 7869ab6ed164fe7245bd2c2ace0cd1fa5c5c0ff2	5.6.0 2026-11-10 06:30:00Z Verified CI (GitHub OIDC)	complete (full repository); checks: security, secrets, dependencies, quality, dead_code; dependencies: 42 queried
example-web: Trusted (CI with GitHub OIDC), complete scan of the default branch.					

Not included in report

- AI-generated code defect checks: not run in the selected scans
- Deep scan (VulnHunter, optional): not run in the selected scans
- Dynamic testing (DAST): not performed by Skylos
- Manual penetration test: not performed by Skylos
- Third-party tool results (uploaded SARIF): not included
- Results of third-party tools uploaded as SARIF are not included.
- A software component inventory (SBOM) and license findings are not included.
- Reachability and exploitability of dependency vulnerabilities are not assessed in this report.

3. Policy evaluation

Policy	Skylos default security policy, revision 2
Policy status	Policy not met
Statement	No open CRITICAL or HIGH security, secret or dependency finding past its fix-by date, with every in-scope project assessed by a trusted, complete scan of the reported branch, no older than 90 days, that ran security, secrets and dependency checks. Small gaps the CLI names in full (at most 50 files and 2% of the files analysed, or of the dependencies checked) are disclosed limitations, not a reason to refuse the scan.
Fix deadlines	Skylos default fix deadlines (CRITICAL 7 days, HIGH 30 days from first seen); the workspace has not turned on fix deadlines.

Rules

Rule	Requirement	Findings	Status
Maximum severity past deadline	No open CRITICAL or HIGH security, secret or dependency finding past its fix-by date	1 finding past the fix-by date	Not met
Assessment coverage	Every in-scope project has a trusted, complete scan of the reported branch, no older than 90 days, that ran security, secrets, dependencies checks	2 of 2 projects meet it	Met

Scan requirements

Project	Frequency	Last performed	Assessment-freshness deadline	Status	Why
example-api	At least every 90 days	2026-11-10	2027-02-08	Met	
example-web	At least every 90 days	2026-11-10	2027-02-08	Met	

Remediation

Severity	Fix deadline	Findings exceeding	Status
CRITICAL	7 days (Skylos default)	0	Met
HIGH	30 days (Skylos default)	1	Not met
MEDIUM	None set	0	Not covered by policy
LOW	None set	0	Not covered by policy

4. Standards mapping: OWASP Top 10 2025

All 10 categories of the OWASP Top 10:2025. Mappings are Skylos's own (mapping 2026-11-08.2).

Requirement	Title	Status	Open	Suppr.	Reason
A01:2025	Broken Access Control	Open findings	1	0	1 open finding in 1 project.
A02:2025	Security Misconfiguration	No open findings from mapped rules	0	0	No open findings from the 8 mapped rules that ran in all 2 in-scope projects.
A03:2025	Software Supply Chain Failures	Open findings	1	0	1 open finding in 1 project.
A04:2025	Cryptographic Failures	No open findings from mapped rules	0	0	No open findings from the 12 mapped rules that ran in all 2 in-scope projects.
A05:2025	Injection	Open findings	2	0	2 open findings in 2 projects.
A06:2025	Insecure Design	No open findings from mapped rules	0	0	No open findings from the 4 mapped rules that ran in all 2 in-scope projects.
A07:2025	Authentication Failures	No open findings from mapped rules	0	1	No open findings from the 15 mapped rules that ran in all 2 in-scope projects. 1 suppressed finding is listed in the exceptions section.
A08:2025	Software or Data Integrity Failures	No open findings from mapped rules	0	0	No open findings from the 20 mapped rules that ran in all 2 in-scope projects.
A09:2025	Security Logging and Alerting Failures	No open findings from mapped rules	0	0	No open findings from the 1 mapped rule that ran in all 2 in-scope projects.
A10:2025	Mishandling of Exceptional Conditions	No open findings from mapped rules	0	0	No open findings from the 8 mapped rules that ran in all 2 in-scope projects.

5. Findings

This report lists the findings that map to OWASP Top 10 2025 or that the policy covers (CRITICAL or HIGH security, secret or dependency findings). Other findings not mapped to this framework: none. They do not count toward the policy status, requirement statuses or totals in this report.

CRITICAL: 1 open, 0 suppressed

Status	Rule and CWE	Location	First seen, fix by	Policy, effort	Recommendation
within deadline	SKY-SCA-GHSA-xxxx-yyyy-zzzz Dependency advisory GHSA-xxxx-yyyy-zzzz CWE-1395 Dependency on Vulnerable Third-Party Component	example-api requirements.txt:7 example-http-client 1.2.0 has a known vulnerability (fictional advisory)	2026-11-07 (3 d) fix by 2026-11-14	Fix required by policy low	Upgrade or replace the component with a maintained version that fixes the advisory (use the fixed-in version when the advisory names one), or remove it, then rescan.

HIGH: 2 open, 1 suppressed

Status	Rule and CWE	Location	First seen, fix by	Policy, effort	Recommendation
overdue	SKY-D211 SQL injection CWE-89 SQL Injection	example-api app/orders/db.py:48 User input reaches a SQL query without parameters	2026-09-30 (41 d) fix by 2026-10-30	Fix required by policy medium	Pass untrusted data as parameters (prepared statements, argument lists), never by building strings or code; validate input at the boundary.
within deadline	SKY-D226 Cross-site scripting: untrusted content marked safe CWE-79 Cross-site Scripting	example-web web/views/profile.py:91 Untrusted content is marked safe before rendering	2026-11-01 (9 d) fix by 2026-12-01	Fix required by policy medium	Encode untrusted output for where it lands (HTML, attribute, JavaScript, URL), keep the framework's auto-escaping on, and sanitize any HTML you must render instead of marking it safe.
suppressed	SKY-S101 Secret detected CWE-798 Use of Hard-coded Credentials	example-api tests/fixtures/settings.py:5 Hard-coded API key	2026-09-16 (55 d) fix by -	- medium	Remove the credential from code and history, rotate it, and load secrets at runtime from a secret manager or environment.

MEDIUM: 1 open, 0 suppressed

Status	Rule and CWE	Location	First seen, fix by	Policy, effort	Recommendation
no deadline	SKY-D215 Path traversal CWE-22 Path Traversal	example-web web/files/download.py:23 A request parameter is used in a file path	2026-10-21 (20 d) fix by -	- medium	Resolve paths against an allowed base directory, refuse links and traversal, and create temporary files with safe library functions.

LOW: 0 open, 0 suppressed

No LOW findings in this report.

6. Exceptions and suppressions

1 of 5 findings in this report suppressed (20%), 0 without an approval record. 1 active exception, 1 expiring within 30 days, 0 without an end date. Verdict before exceptions: Policy not met; after: Policy not met.

Project, rule	Status	Requested / approved by	Justification	Decided, expires
example-api SKY-S101	approved	developer@example.com security-lead@example.com	Test fixture key; it is not used in production Review: Accepted until the fixtures are regenerated	2026-10-22 2026-12-10

7. Trend and issues no longer detected

No earlier report of this framework and scope exists. Issues no longer detected below cover the last 90 days.

Scan history in the window

Trusted scans of each project's report branch from 2026-08-13 to 2026-11-10, with the longest stretch without one. Scans removed by your retention setting are not counted.

Project	Trusted scans	First	Last	Longest stretch without one
example-api	14	2026-08-15 00:00:00Z	2026-11-10 06:30:00Z	7 days
example-web	12	2026-08-15 00:00:00Z	2026-11-10 06:30:00Z	21 days

No longer detected in the window

1 of 1 CRITICAL or HIGH issue no longer detected in the window had the first scan without the finding by the fix-by date; 0 after it. That date shows when Skylos stopped detecting the finding, not when a change was merged or deployed.

Project, rule	Severity	Location	First scan without the finding	By the fix-by date	Closure evidence
example-api SKY-D212	HIGH	app/jobs/export.py:17	2026-10-29 09:00:00Z	Yes (due 2026-11-10)	Not present in trusted, complete scan 4ec5299c-ef87-4e43-8fc7-edb06a35bcba of main at commit 13ffc9a7f1deedd1015ceafa8322ec929a9d5f22 (2026-10-29T09:00:00.000Z).

8. Methodology and definitions

Analysis	What it does	What it cannot see
Static security analysis (SAST)	Skylos security rules on first-party code, configuration, CI pipelines and infrastructure files.	Runtime behaviour, deployed configuration and business logic.
Secret detection	Hard-coded credentials, keys and tokens in the scanned files.	Secrets in git history before the scanned commit, or outside the repository.
Dependency vulnerabilities (SCA)	Declared dependencies matched against public advisories (OSV) when the scan ran.	Whether a vulnerable function is reachable, and dependencies without a supported manifest or resolved version.
Quality analysis	Reliability and maintainability rules; counted here only where a rule maps to a requirement.	Security weaknesses outside its rule set.
AI-generated code defect checks	Hallucinated packages and APIs, weakened tests and other AI-agent mistakes.	Defects without a Skylos rule.
Deep scan (VulnHunter, optional)	An AI security review of the repository, each finding challenged by a second AI pass.	Anything outside its review budget; partial scans are labelled.

Staleness rule. Results from a scan older than 90 days at generation time do not count toward "Policy met": the project is shown as not assessed and its next scan is overdue.

Mapping. Findings map to requirements through CWE ids declared by the Skylos CLI (catalog 5.6.0), CWE ids Skylos Cloud assigns to 63 rules the CLI ships without one (each with a stated rationale), the finding kind (dependency advisory, code weakness, CI pipeline) and, for OWASP only, the CLI's OWASP 2021 category carried to 2025. When the CLI sends a finding's own CWE ids and they are a subset of its rule's, the finding maps through those alone. Every vulnerability finding (a security or secret finding with a CWE, a dependency advisory) and every CRITICAL or HIGH finding the policy covers also maps to the vulnerability-management requirement where the framework has one (SOC 2 CC7.1), which is tested by fix-by date on the policy's findings. Mapping version 2026-11-08.2. CWE™ content © The MITRE Corporation, used under the CWE Terms of Use. OWASP Top 10 © OWASP Foundation, CC BY-SA 4.0.

Requirement statuses

- Deviation noted: Vulnerability management (SOC 2 CC7.1): at least one open CRITICAL or HIGH security, secret or dependency finding is past its fix-by date, had its first scan without the finding after it in the window (when Skylos stopped detecting it, not a merge or deploy date), or is suppressed without an approval record. The counts are given, from the same findings as the policy result. This is Skylos's test of its own evidence, not an auditor's conclusion.
- Open findings: At least one open (not suppressed) finding in scope maps to this requirement.
- No open findings from mapped rules: Skylos rules map to this requirement, every in-scope project has a trusted, complete, current scan that ran those rules' checks, and none of them reported an open finding. This is not proof that the requirement is met.
- Not evidenced by static analysis: Static analysis cannot evidence this requirement (it needs process, runtime or organizational evidence), or no Skylos rule checks it. The reason is given.
- Not scanned: Skylos could evidence this requirement, but at least one in-scope project has no trusted, complete, current scan that ran the needed checks, so no claim is made.
- Scan activity recorded: The requirement is about running detection or review, and every in-scope project has a trusted, complete, current scan that ran the required checks. For vulnerability management (SOC 2 CC7.1) it also means no CRITICAL or HIGH security, secret or dependency finding is open past its fix-by date, had its first scan without the finding after it, or is suppressed without an approval record ("No deviations noted"); otherwise findings never count against it.

Policy outcomes

- Policy met, fixes due: Every in-scope project is assessed; open findings at a covered severity exist but all are still within their fix deadline.
- Policy not met: At least one open finding at a covered severity is past its fix deadline.
- Not assessed: No failure was found, but at least one in-scope project has no trusted, complete, current scan with the checks the policy needs (or nothing is in scope), so no pass is given.
- Policy met: Every in-scope project is assessed and no open finding is at a severity the policy covers.

Effort to fix

- High: a design change across components (for example adding missing authentication or authorization, replacing an unsafe serialization format).
- Low: a version, configuration value or single call changes (for example upgrading a dependency to a fixed version, pinning a CI action, turning certificate verification back on).
- Medium: code changes in one place, possibly with a credential rotation (for example parameterizing a query, replacing a weak algorithm, removing a hard-coded secret).

Terms

- Assessed project: A project whose scan is a trusted upload of the default branch (or the branch chosen for this report) that covered the whole repository, as the CLI reported it, and is no older than 90 days. Suppressions inside the scan (inline comments, Skylos config) do not stop a project being assessed; they are disclosed for that project. Neither do small gaps the CLI names in full: files it could not analyse (at most 50, and at most 2% of the files analysed) or dependencies it could not fully check (the same limits); each is a disclosed limitation.
- Before exceptions: The verdict computed as if no exception or suppression applied, so a reader can see what the exceptions change.
- Disclosed limitation: A part of the repository the scan named but did not fully analyse (files, or dependencies it could not fully check). Findings there, if any, are not in this report. The project still counts as assessed; the limitation is listed for that project and under Limitations.
- Fix required by policy: The finding is open, at a severity the policy covers (CRITICAL or HIGH security, secret or dependency finding), and must be fixed by its fix-by date for the policy to pass.
- Fix-by date: First seen date plus the deadline for the finding's severity, from the workspace's fix-deadline settings, or the Skylos defaults for CRITICAL and HIGH when none are set.
- Hidden in the scan: Findings a scan's own inline suppression comments or Skylos config kept out of its results. They are not uploaded, so the report cannot count or list them and has no approval record for them; the project's row says when this happened.
- Mapped rule: A Skylos rule whose CWE (declared by the CLI or assigned by Skylos Cloud) or finding kind falls under the requirement. Mappings are Skylos's own.
- Open finding: A finding in the selected scan that is not suppressed. Suppressed findings are listed separately with their approval record.
- Suppressed finding: A finding hidden by an approved exception, an inline suppression or a Skylos Cloud suppression.
- Trusted upload: A scan uploaded by CI with GitHub or GitLab OIDC, by Skylos Cloud itself, or with a project token an owner or admin marked for CI. Uploads with login tokens (`skylos login`) on developer machines are unverified.
- Vulnerability finding: A security or secret finding with a CWE id, a dependency advisory, or a deep scan finding with a CWE id; these map to SOC 2 CC7.1. CC7.1 tests the policy's findings (every CRITICAL and HIGH security, secret and dependency finding, with or without a CWE id) against their fix-by dates, the same population as the policy result and Skylos test SK-C2.1.

9. Limitations and disclaimer

- Findings and the policy result come from each project's latest assessed scan (point in time). Period evidence is limited to the scan history and the issues no longer detected in the window (with their fix-by dates); scans removed by retention are not counted. Changes, approvals and deployments over a period are in the change-history export, not here.
- Findings come from automated static analysis. Business logic, runtime configuration, deployed infrastructure and manual review are not covered.
- Dependency vulnerabilities are matched by the Skylos CLI against public advisories (OSV) when each scan ran; the advisory data snapshot date is not recorded.
- Projects that are not assessed contribute findings but no "no open findings" claims; an unverified upload can never make a requirement or the verdict look better.
- Suppressed findings are excluded from the verdict and listed with their approval record, if any. A high suppression rate weakens this evidence (NIST SP 800-53 SA-11(1)).

This report presents the results of automated static analysis by Skylos on the scope listed in the Scope section, at the time stated. Standard mappings are Skylos's own and show which findings relate to a requirement; they are not a determination of compliance, which only a qualified assessor (for example a PCI QSA, a SOC 2 or ISO/IEC 27001 auditor, or a notified body) can make. Absence of findings is not evidence of absence of vulnerabilities. Requirements marked "Not evidenced by static analysis" need manual review, runtime testing or process evidence. The full edition contains sensitive vulnerability detail; share the external summary with third parties.

10. Integrity and verification

Report ID	00000000-0000-4000-8000-000000000010
SHA-256 of the report JSON	509544e376ecea919d30318a2f1a5c2eb0b68a091b1ec92fe1e03e3af0d3a9e9
Canonical form	skylos-canonical-json/v1: UTF-8 JSON, object keys sorted by UTF-16 code units, no insignificant whitespace, members with undefined values omitted
Signature	Unsigned: no signing key was configured in Skylos Cloud when this report was generated. The SHA-256 and the verification page still detect changes to the stored report.
Verification URL	https://skylos.dev/verify/report/00000000-0000-4000-8000-000000000010
How to check a copy	The verification page says whether the record Skylos stored for this report is signed and unchanged, and shows its key facts (framework, dates, scope size, policy result and counts). A PDF, HTML or CSV copy is not itself verified: compare those facts with the copy in hand, or drop the JSON file on that page to have it hashed in your browser and compared with the stored SHA-256.
What a valid signature proves	A valid signature proves that Skylos Cloud generated exactly the stored report content (the report JSON) at the stated time, and that the stored content has not been changed since. It does not prove that the code is secure, that any requirement is met, or that a PDF, HTML or CSV copy is unchanged. Trusted scan results were vouched for by the CI provider (OIDC) or by a project token a workspace admin marked for CI; Skylos did not re-run the scans.

https://skylos.dev/verify/report/00000000-0000-4000-8000-000000000010