DSA / RESEARCH SERIES 2026

Hacken: measuring public audit-record completeness

The public API enables a reproducible completeness check, while its records and report narratives serve different purposes.

DSA research, prepared with AI assistance

Published September 5, 2026 | Version 1.0

Public-source research; independent expert review pending

This document reviews cited public evidence. It is not a code audit, a certification, or an endorsement by an appointed expert panel.

Measurements in this report

Returned API records	1373
SCA records dated no later than check date	1123
Nonempty repository fields	1100
Nonempty commit fields	1043
Records with both fields nonempty	1042
Nonempty asset lists	637
Nonempty issue lists	670
Nonempty report links	1373
Placeholder commit values	21
Single 7-to-40-digit hex commit strings	963

Read online: https://defisec.info/reports/hacken-evidence-review-2026

Evidence coverage against the seven criteria

All scores are withheld. These are source-evidence observations, not independent technical assessments.

Technical finding quality | Not scored

Published finding narratives available. Exploits have not been reproduced by DSA.

Depth and threat model | Not scored

Scope and method material available. Test adequacy and omitted threats need expert review.

Scope and version traceability | Not scored

Version or deployed-address anchors are recorded. Independent repository/build validation is pending.

Demonstrated specialization | Not scored

Sampled projects identify relevant technologies. Assigned-team fit remains unverified.

Fix verification | Not scored

Resolution narratives inspected. Accepted risk is kept separate from a verified code fix.

Internal quality control and response | Not scored

No independent internal QA workpapers inspected.

Transparency and conflicts | Not scored

Public identity sources are available. Reviewer and commercial conflict declarations have not been collected.

Dataset and reproducible counting rules

We requested the documented public audits endpoint on September 5, 2026. It returned 1,373 records. We counted a field as present only when its trimmed string was nonempty, or, for asset and issue lists, when the array contained at least one item. These are counts of returned records, without deduplication or an assumption that the endpoint contains every Hacken engagement.

Original measurement

Of the 1,373 returned records, 1,100 had a nonempty repository field and 1,043 had a nonempty commit field. Both fields were present together in 1,042 records. An asset list was present in 637, an issue list in 670 and a report link in all 1,373 records.

We did not validate every URL or resolve every commit. A nonempty string can still be abbreviated, stale or invalid. An empty issue array can reflect missing export data or a clean result; it must not be interpreted as proof that no vulnerability was found. The API is an evidence-discovery aid, not a substitute for the final report.

A recent sample tests the next step

We filtered to SCA records dated no later than the check date, sorted by audit date and then audit name descending and opened the first three report links. They concern vAPI Network and two Europeum components. All three links returned readable report pages; all three API records contain a repository, a commit and a nonempty asset list.

The API records list 10, 11 and 6 findings, respectively. These counts are provider-recorded metadata, not a comparative quality score. The vAPI record includes fixed, mitigated and accepted outcomes. A buyer needs to inspect the accepted medium-severity item and its rationale rather than assume that every listed finding was eliminated.

Procurement implication

The public data makes it practical to choose reports by technology and inspect their scope, which reduces the cost of assembling an evidence packet. It does not establish reviewer skill, completeness of testing or the team that will work on a future engagement. Ask for the assigned reviewers, threat model, test evidence, final fix commits and an explanation of accepted risk.

The published preparation and methodology materials can be compared with actual report artifacts during the proposed committee review. Until two independent reviewers complete that process, this dossier supplies a research packet and no technical endorsement.

A stricter check exposes placeholder values

Of the 1,043 nonempty commit strings, 21 are placeholder values such as N/A. Exactly 963 match a single 7-to-40-character hexadecimal string. The remainder also includes multiple commits, shortened identifiers and other formats; failing this syntax check does not prove the identifier is invalid. No repository resolution is claimed. In the expanded five-client sample, vAPI, Europeum, Tangible USDR, YFSX and VIN all have readable report pages. YFSX and VIN identify deployed addresses and record accepted or mitigated findings, rather than presenting a repository commit as the scope anchor.

Limits and next verification step

This is a bounded review of public evidence. We did not rerun exploits, inspect private workpapers, interview the assigned audit team or verify current booking availability. The observations describe the cited artifacts and cannot establish the provider's overall defect-detection rate. A procurement decision still needs a scoped proposal, relevant recent work and independent technical review.

Sources and reproducibility

All source checks were made on September 5, 2026. Content hashes identify the retrieved artifacts. Data definitions and the source manifest are available from the report page and the link below.

1. Public audits API snapshot

Official source: hacken.io

SHA-256: dca20863d906d096e625de4b29d0c3cddc6f10a17c0290ed0b2b313ccdd07e35

2. Official service description

Official source: hacken.io

SHA-256: a253fd20f9ad23cc5ba4f8b5d4c22c7ef4043fefd5f24af8b0ee17a105105dd8

3. [SCA] vAPI Network / SC Audit / Jul2026

Official source: hacken.io

SHA-256: cbe796565ee8c04494d775082c518eeff653f46683953c4b3be8a363e9a1c028

4. [SCA] Europeum / TPR / Jul2026

Official source: hacken.io

SHA-256: f4c2cb2904a4432ddafcca0d29f720fc83bc0b64089dfef9c2bc606c681bdd45

5. [SCA] Europeum / Beacon Proxy / Jul2026

Official source: hacken.io

SHA-256: ec7d902ab333e408dd67303014ae8a9cda4e24cbab720f93820d830883fd29b5

6. Tangible USDR

Official source: hacken.io

SHA-256: 49a79f32c4b21dcaed50635ac63aec61044a28e1a9def678a2b7df20d4eb9415

7. YFSX Token

Official source: hacken.io

SHA-256: f8270e344e21cead593f2db5334022cf5ef994ed48d1bbeea7e76cb980957539

8. VIN Token

Official source: hacken.io

SHA-256: 18e57cfa5dcbc55987d050e3ee5e2747202c47114bb8a4713d162d2ecc12d518

Data and methodology

https://defisec.info/downloads/research/evidence-measurements-2026-09-05.json

Selection rules, HTTP results, source hashes, and original counts are recorded in the accompanying data. The research used AI assistance. No independent technical committee review is claimed.

https://defisec.info/methodology