

Source Code Security Assessment Sample report

WHE-SAMPLE-07 | Version 1.0 | 11 September 2026

Fictional demonstration. No real assessment was performed.

All assets, evidence, findings, and severity ratings in this document are synthetic. This report is not a client deliverable, certification, or statement about the security of any real organization.

Executive summary

This example demonstrates how WheInfosec can present an assessment scope, a finding, and a remediation plan. It contains one illustrative high-severity finding: missing authorization check in export handler.

An authenticated user may export another account data if the illustrated path is reachable and no upstream control exists. Runtime exploitability requires validation.

Recommended next step

Invoke a centralized authorization policy before querying or exporting account data. Bind identity to allowed resources and add negative authorization tests at the route and service boundaries.

Scope and methodology

Illustrative scope

One fictional export module and its authorization data flow. Full repository and runtime testing excluded.

Engagement inputs

Read-only repository snapshot, commit identifier, build context, trust boundaries, and role model.

Example assessment process

- 1. Confirm written authorization, assets, access, and testing boundaries.
- 2. Review the scoped controls and validate observations with controlled test data.
- 3. Document evidence, prerequisites, impact, and practical remediation.
- 4. Agree a retest plan and report unresolved limitations.

Severity model

Qualitative severity combines plausible impact and required access. High means material impact with realistic prerequisites; Medium means narrower impact or stronger prerequisites; Low means limited impact. Ratings are illustrative, not CVSS scores.

Framework context

OWASP Top 10:2025. Scope determines category coverage; no OWASP certification is implied.

Coverage and limitations

Only the example workflow described here is represented. No tool scans, customer interviews, exploit attempts, or retests actually occurred. Absence of other findings does not imply that other controls passed.

ID	Finding	Severity
WHE-SAMPLE-07-01	Missing authorization check in export handler	High

Missing authorization check in export handler

Observation

The fictional export handler checks authentication but does not verify authorization for the requested account.

Illustrative evidence

```
Synthetic review location: src/routes/export.ts:42. Data flow: request.accountId ->
exportService.create(accountId), without an ownership or role policy check. This is
not a reference to customer code.
```

Potential impact and prerequisites

An authenticated user may export another account data if the illustrated path is reachable and no upstream control exists. Runtime exploitability requires validation.

Validation boundary

The evidence above illustrates reporting style only. An actual assessment must confirm affected assets, access conditions, scope, and reproducibility before assigning a final severity.

Recommended remediation

Invoke a centralized authorization policy before querying or exporting account data. Bind identity to allowed resources and add negative authorization tests at the route and service boundaries.

Remediation and retesting

Suggested owner

The application or infrastructure owner responsible for the affected control, supported by the security team.

Retest acceptance criteria

Review the corrected data flow and tests. Verify permitted exports succeed and cross-account requests fail without creating export files or background jobs.

Tracking field	Sample value
Status	Illustrative finding - no actual remediation tracked
Target date	To be agreed by the asset owner
Retest result	Not performed
Residual risk	Requires validation in a real assessment

Technical reference

https://cheatsheetseries.owasp.org/cheatsheets/Secure_Code_Review_Cheat_Sheet.html

Reference material supports assessment concepts; the fictional finding is authored for this sample and does not imply endorsement by the reference publisher.

Discuss your scope

contact@wheinfosec.com
wheinfosec.com/contact.html

Public sample. Do not use this document as evidence of a completed security assessment.