

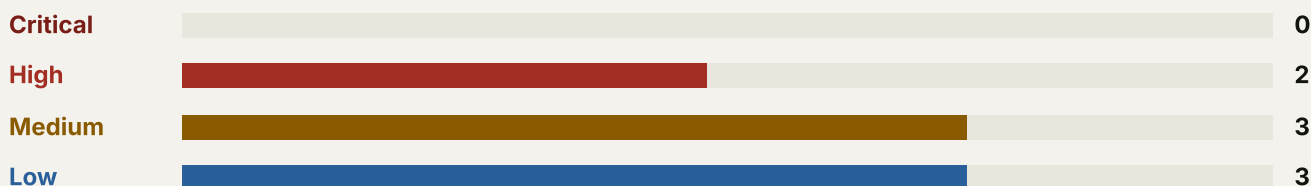


Sample report for a demo repository

SAMPLE. Illustrative sample. The repository, commit, findings and numbers below are invented to show the report format. They are not the output of a real run.

RUN ID	SAMPLE-0001
DATE	2026-10-25 14:00 UTC (sample date)
REPOSITORY	oddsequence-demo/vault-core (demo repository)
COMMIT	8f3a2c1000000000000000000000000000000000000000000000000000000000 (invented sample value)
PRESET	Deep (3 tools)
TOOLS	solidity-auditor v3, krait v8.2, plamen 2.2.4
MODEL PIN	PENDING: dated model snapshot id is written here for every real run
REPORT VERSION	sample-1
WEB VERSION	https://oddsequence.com/auto-audit/sample-report/

Findings by severity and status



8 findings, 3 discarded as false positives. Zero findings would not mean "safe": see Coverage (page 4) and Not checked (page 8).

All findings

ID	TITLE	SEVERITY	EVIDENCE	AGREEMENT	STATUS
F-1	Share price manipulation via a direct donation to the vault src/Vault.sol:214	High	poc-pass-fork	2 of 3 tools	confirmed
F-2	Stale oracle price is not checked src/oracle/PriceOracle.sol:77	High	static-confirmed	3 of 3 tools	confirmed
F-3	No slippage limit when exiting the strategy src/strategies/AaveStrategy.sol:131	Medium	not-verified	1 of 3 tools	lead
F-4	Admin can replace the strategy without a timelock src/Vault.sol:402	Medium	not-verified	2 of 3 tools	reported
F-5	Rounding down on withdrawal leaves dust src/Vault.sol:288	Medium	not-verified	1 of 3 tools	lead
F-6	No event when the fee changes src/VaultFactory.sol:66	Low	static-confirmed	3 of 3 tools	confirmed
F-7	Unused variable src/libraries/Math.sol:12	Low	static-confirmed	1 of 3 tools	confirmed
F-8	Pin the pragma to a fixed version src/Vault.sol:2	Low	static-confirmed	3 of 3 tools	confirmed

Agreement counts tools, not independent opinions: all three tools run on one model family, so agreement here is one voice. "Confirmed" means a passing proof of concept or a static check. Meaning of every field: <https://oddsequence.com/auto-audit/method/>

This report describes one commit at one point in time. It can miss issues and can be wrong. It does not replace a human audit.

Every tool, pinned

Deep preset: three tools with different methods, de-duplication by root cause, then an independent review by a different model. Tools are pinned by commit, not by tag. Model snapshot: PENDING: dated model snapshot id is written here for every real run.

TOOL	PINNED COMMIT	LICENSE	MODEL FAMILY	STATUS
solidity-auditor v3	c9ce8cf7300385eb0f02e15b3749059e4e8f6ec5	MIT	Anthropic Claude	completed (sample)
krait v8.2	76e5ac7b74ce5517409870c2974e6baaddc8f99e	MIT	Anthropic Claude	completed (sample)
plamen 2.2.4	795962b96e254f2e423a2635fe7f8cb8ea1e6d69	MIT (root)	Anthropic Claude	partial: timed out on 1 file (sample)

Risk classification

Severity combines impact and likelihood and is mapped to four levels: Critical, High, Medium, Low. Tool-specific labels are normalized and the raw label is kept in the JSON export.

Evidence levels

code-trace	The tool traced the issue in the code; nothing was executed.
static-confirmed	A static analysis check backs the finding.
poc-pass-fork	A proof of concept ran on a fork and passed.
poc-fail	A proof of concept ran and failed; the finding is kept as a lead.
not-verified	No independent check.

Third-party notices

- **solidity-auditor v3**: MIT. Copyright (c) 2024 AI Skills Contributors
- **krait v8.2**: MIT. Copyright (c) 2025-2026 Zealynx Security
- **plamen 2.2.4**: MIT (root). Copyright (c) 2025-2026 Plamen Contributors

Names belong to their owners and do not imply endorsement or affiliation. Full license texts are reproduced from each upstream repository in real reports.

What was in scope and what was read

FILE	NSLOC	COVERAGE
src/Vault.sol	612	read by 3 of 3 tools
src/VaultFactory.sol	148	read by 3 of 3 tools
src/strategies/AaveStrategy.sol	301	read by 3 of 3 tools
src/oracle/PriceOracle.sol	205	read by 2 of 3 tools; plamen timed out
Total in scope	1266	

Excluded from scope

- src/libraries/Math.sol (96 nSLOC): possible vendored copy, excluded by the customer
- src/interfaces/IVault.sol (44), test/Vault.t.sol (480), script/Deploy.s.sol (72): interfaces, tests and scripts
- lib/openzeppelin-contracts (5,400): external dependency

Tool coverage

TOOL	FILES READ	STATUS
solidity-auditor v3	4 of 4 files	completed (sample)
krait v8.2	4 of 4 files	completed (sample)
plamen 2.2.4	3 of 4 files	partial: timed out on 1 file (sample)

An empty result is not a clean result. One tool timed out on one file in this sample. A timeout looks the same as "found nothing" unless coverage is listed, which is why this page exists.

Freeze check

The audited commit is fixed at the value on the title page. Changes after that commit are not covered.

High severity

F-1 Share price manipulation via a direct donation to the vault

High · Likelihood: Medium. Impact: High.

Found by: solidity-auditor v3, krait v8.2 (2 of 3 tools, 1 model family)

Evidence: poc-pass-fork: a proof of concept ran on a fork and passed (sample).

convertToShares divides by a total that includes assets sent straight to the vault. Sending assets directly raises the share price before the next user deposits.

Attack path: 1) Attacker deposits 1 wei. 2) Attacker donates X assets directly. 3) A victim who deposits less than X receives 0 shares.

```
function convertToShares(uint256 assets) public view returns (uint256) {
    uint256 supply = totalSupply();
    return supply == 0 ? assets : assets * supply / totalAssets();
}
```

Hypothesis, verify it: use virtual shares and assets (an offset) or track total assets internally instead of reading the token balance.

F-2 Stale oracle price is not checked

High · Likelihood: Medium. Impact: High.

Found by: solidity-auditor v3, krait v8.2, plamen 2.2.4 (3 of 3 tools, 1 model family)

Evidence: static-confirmed: a static check backs the finding (sample).

latestRoundData() is read without checking updatedAt. If the feed stops, the vault keeps using the old price.

Attack path: Feed halts, the price goes stale, withdrawals use a wrong price.

```
(, int256 price,,) = feed.latestRoundData();
return uint256(price);
```

Hypothesis, verify it: check updatedAt and answeredInRound, and cap the allowed age.

Medium severity and where tools differ

F-3 No slippage limit when exiting the strategy

Medium · Likelihood: Low. Impact: Medium.

Found by: solidity-auditor v3 (1 of 3 tools)

Evidence: not-verified: no independent check. Listed as a lead because one tool reported it.

withdraw() accepts any amount returned by the pool.

Attack path: Sandwich attack on a withdrawal.

```
pool.withdraw(asset, amount, address(this));
```

Hypothesis, verify it: add a minimum-out parameter and verify the received amount.

Where the tools differ

ID	FINDING	V3	KRAIT	PLAMEN
F-1	Share price manipulation via a direct donation to the vault	✓	✓	–
F-2	Stale oracle price is not checked	✓	✓	✓
F-3	No slippage limit when exiting the strategy	✓	–	–
F-4	Admin can replace the strategy without a timelock	✓	✓	–
F-5	Rounding down on withdrawal leaves dust	–	✓	–
F-6	No event when the fee changes	✓	✓	✓
F-7	Unused variable	–	✓	–
F-8	Pin the pragma to a fixed version	✓	✓	✓

✓ reported it. – did not report it. An empty cell is not the same as "not found": plamen timed out on one file in scope, so its row may be incomplete (see page 4). Findings seen by one tool are listed as leads, not hidden.

False positives we filtered

A reviewer on a different model judged these findings to be false positives or to need a human. We keep them visible, with the reason and the tool that raised them, so you can check our call.

ID	TITLE	REASON	RAISED BY
D-1	Reentrancy in deposit()	likely_false: a nonReentrant guard is present. Reviewer: different model.	solidity-auditor v3
D-2	Overflow in Math.mulDiv	likely_false: Solidity 0.8 has checked arithmetic.	krait v8.2
D-3	tx.origin in the factory	needs_human: it is not used for authorization.	solidity-auditor v3

Leads that need verification

- **F-3** No slippage limit when exiting the strategy (1 of 3 tools, not-verified)
- **F-5** Rounding down on withdrawal leaves dust (1 of 3 tools, not-verified)

Leads are single-source or unverified items. They are worth a look but are not claimed as confirmed.

What was not checked

- Off-chain components, keys and key management
- Front end and infrastructure
- Economic model and parameter choices
- Dependency updates after the audited commit
- Integrations beyond the files in scope, and token behavior not listed in the scope

Zero findings is not "safe". A clean report can mean a clean repository or a tool that did not read the code. Read the coverage page first.

Disclaimer

1. This report is not a guarantee of security. It is limited in time and in resources and does not replace a human audit.
2. Zero findings does not prove the absence of vulnerabilities.
3. All tools are not deterministic: a repeat run can return a different set of findings.
4. Agreement between tools is not confirmation. Tools built on one model can make the same mistake. We call a finding confirmed only with a passing proof of concept or a static check.
5. The report applies to the stated commit. Later changes are not covered.
6. Recommendations were not tested unless stated.
7. Third-party tools are listed for transparency. Names belong to their owners and do not imply endorsement or affiliation.
8. This is not legal or investment advice.

The legal text of the final report is pending review. This sample carries working wording only.