



HackenProof

SUMMARY REPORT

Reliq Audit Contest



Reliq

SMART CONTRACTS CODE LANGUAGE

Solidity

REPORT CREATED

07.01.2026

AUDIT DURATION

16.12.25-23.12.25

PREPARED BY

HackenProof Team



HackenProof Crowdsourced Audit is your solution to maximize the cybersecurity level with involvement of over 40k of the most skilled and experienced community researchers in the industry

Approved by	HackenProof team
Name	Reliq Audit Contest
Type	Smart Contracts
Technology	Solidity
Timeline	16.12.25-23.12.25
Deployed contract / GitHub	Public



Table of Contents

Overview	4
About audit	4
About Reliq	4
Scopes and targets	4
Payment statistics	5
Rewards distribution	5
Findings	6
Valid reports statistics	6
Signal-to-noise ratio	6
Findings list	7
Security researchers	8
Top hackers	8
Conclusion	9
About Reliq	9
Technical disclaimer	9



OVERVIEW

ABOUT AUDIT

BUDGET
ALLOCATED

\$5 000

TOTAL REPORT
SUBMITTED

339

SCOPE REVIEW
COUNT

10123

ABOUT RELIQ

Reliq is a DeFi protocol built on Hyperliquid. It's a reserve currency coupled with an internal loan book to let people access more liquidity through 99% LTV loans

SCOPES AND TARGETS

Target

Type

Tech

<https://github.com/hackenproof-public/reliq-protocol>



Smart contract

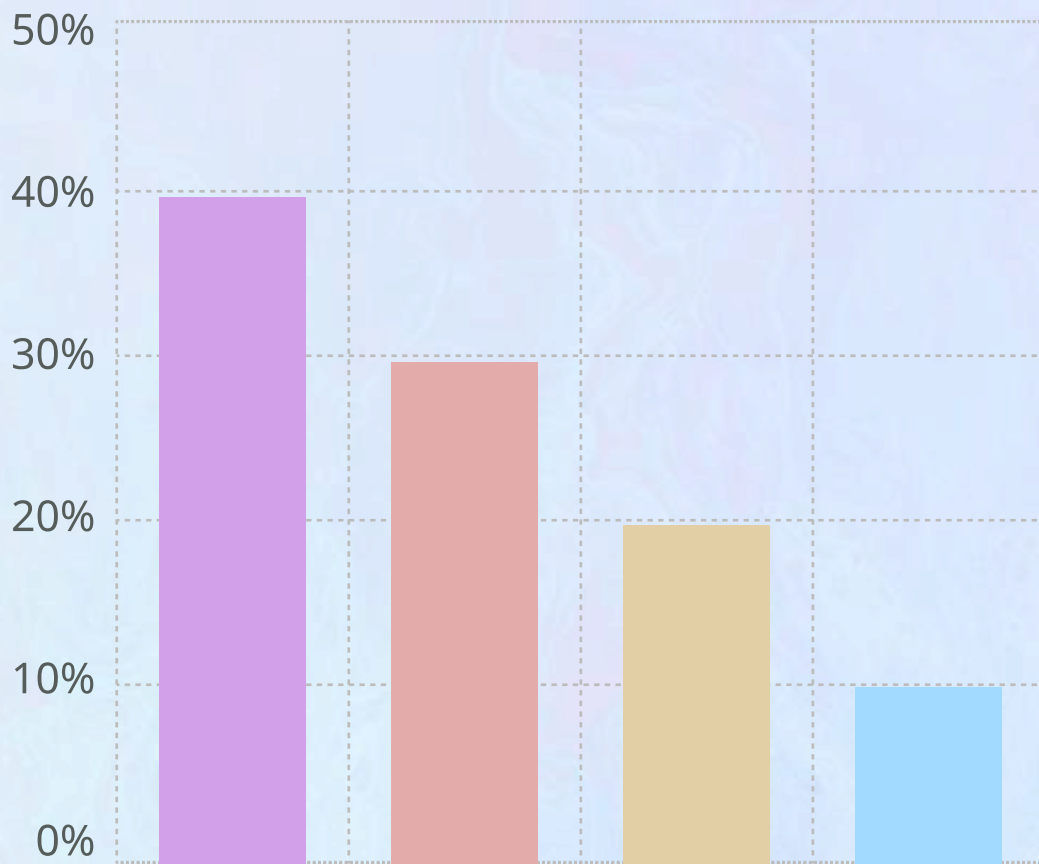


Solidity



PAYMENT STATISTICS

DISTRIBUTION OF PAID-OUT REWARDS



- 40% for critical issues
- 30% for high issues
- 20% for medium issues
- 10% for low issues

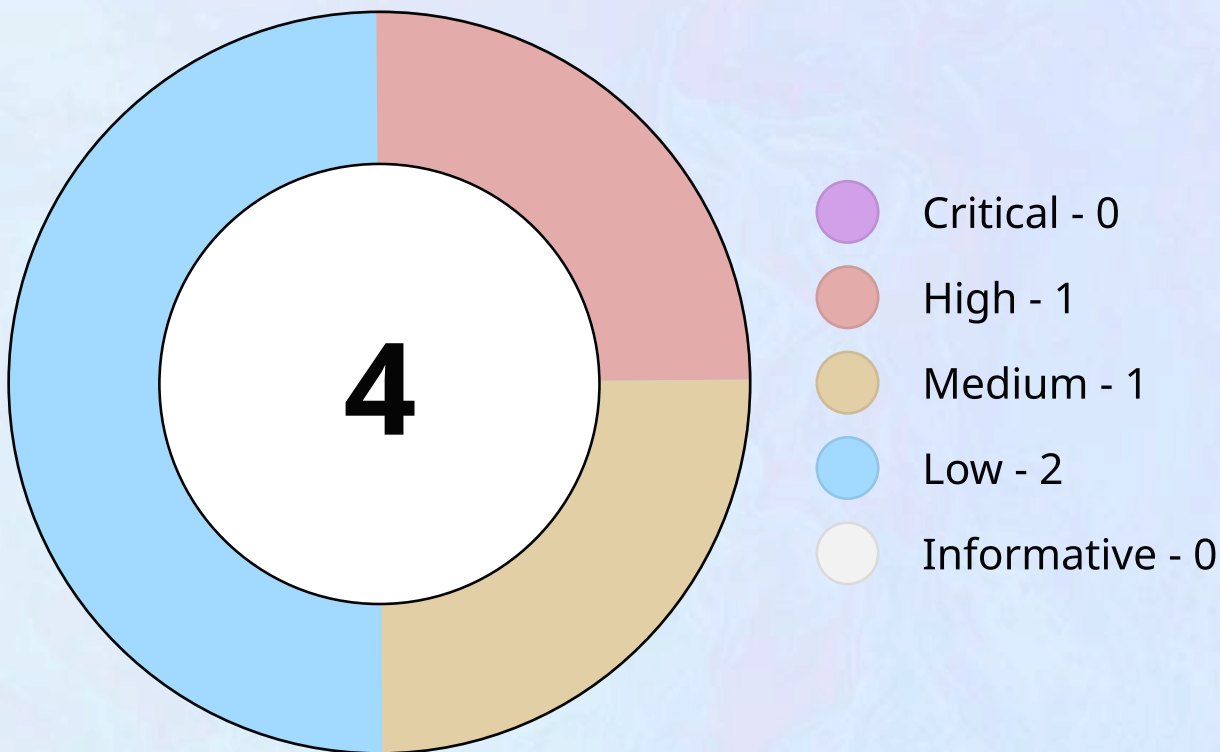
BUDGET
\$5 000

TOTAL PAID OUT
\$3 000



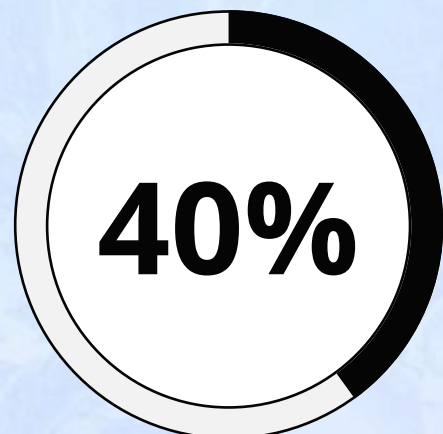
FINDINGS

VALID REPORTS STATISTICS







SIGNAL-TO-NOISE RATIO

Displays the ratio of the Valid reports and Received reports. Valid reports include Informative, Triaged, Paid, Resolved, Discosed statuses








FINDINGS LIST

	Name	Severity	Submission date
	RELIQCA-52 <u>ReliqHYPE: 'borrowMore()'</u> <u>can charge 0 interest even</u> <u>with 23 hours remaining</u> <u>until maturity</u>	• High	17.12.2025
	RELIQCA-173 <u>Users lose funds to MEV</u> <u>sandwich attacks due to</u> <u>missing slippage protection</u>	• Medium	20.12.2025
	RELIQCA-50 <u>Altar: "per-user cap" is not</u> <u>enforced - users can exceed</u> <u>'maxContribution' by</u> <u>splitting deposits and</u> <u>monopolize 'depositCap'</u>	• Low	17.12.2025
	RELIQCA-303 <u>numberOfDays Field</u> <u>Corruption in borrowMore()</u>	• Low	22.12.2025



SECURITY RESEARCHERS

TOP HACKERS

Researcher	Total findings	Payouts	Place
 @jayx	11	\$187.72	1
 @count-sum	23	\$187.72	2
 @maketer	17	\$147.82	3
 @rbd3	5	\$137.79	4
 @alical	8	\$137.79	5

CONCLUSION

ABOUT RELIQ

The audit makes no statements or warranties on security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree status or any other statements of the contract.

It is important to note that you should not rely on this report only - we recommend proceeding with several independent audits and a public bug bounty program to ensure security of smart contracts.

TECHNICAL DISCLAIMER

Smart contracts are deployed and executed on blockchain platform. The platform, its programming language, and other software related to the smart contract can have its vulnerabilities that can lead to hacks. Thus, the audit can't guarantee the explicit security of the audited smart contracts.