



HackenProof

# SUMMARY REPORT

## Kinetic Audit Contest



SMART CONTRACTS CODE LANGUAGE

**Solidity**

REPORT CREATED

**11.04.2025**

AUDIT DURATION

**20.01.2025 - 20.02.2025**

PREPARED BY

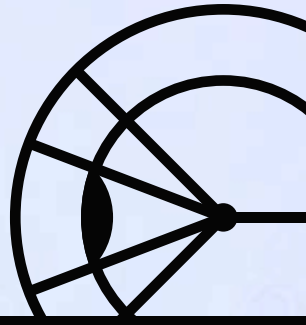
**HackenProof team**

HackenProof Crowdsourced Audit is your solution to maximize the cybersecurity level with involvement of over 30k of the most skilled and experienced community researchers in the industry

Approved by	HackenProof team
Name	Kinetic Audit Contest
Type	Smart Contracts
Technology	Solidity
Timeline	20.01.2025 - 20.02.2025
Deployed contract / GitHub	Public

# Table of Contents

<b>Overview</b>	4
About audit	4
About Kinetic	4
Scopes and targets	5
<b>Payment statistics</b>	6
Rewards distribution	6
<b>Findings</b>	7
Valid reports statistics	7
Signal-to-noise ratio	7
Findings list	8-11
<b>Security researchers</b>	12
Top hackers	12
<b>Conclusion</b>	13
About Kinetic	13
Technical disclaimer	13



# OVERVIEW

## ABOUT AUDIT

BUDGET  
ALLOCATED

**\$40 000**

TOTAL REPORT  
SUBMITTED

**175**

SCOPE REVIEW  
COUNT

**4700**

---



## ABOUT KINETIC

Kinetic is here to kickstart De-Fi and guide the Flare ecosystem into its next stage of explosive growth. We want to inspire you to activate your assets, whether they are traditional (ERC20) or non-traditional (FAssets), and turn their latent potential into progress. Through the tooling provided by Kinetic, you can develop and employ advanced financial strategies with long-term benefits. We are an ecosystem-tailored money market enhanced with an optional work-to-earn element through Kii Stake.



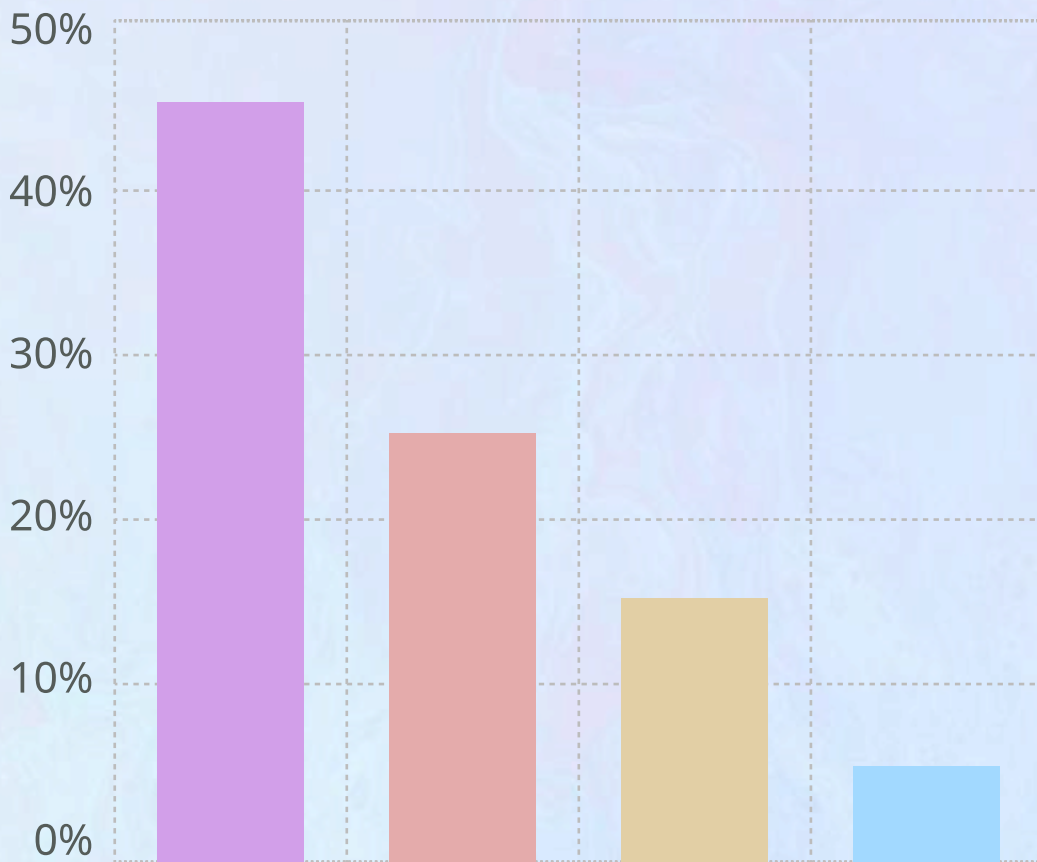
---

# SCOPES AND TARGETS

Target	Type	Tech
<a href="https://github.com/kinetic-market/public-money-market-contracts">https://github.com/kinetic-market/public-money-market-contracts</a>	 Smart contract	 Solidity

# PAYMENT STATISTICS

## REWARDS DISTRIBUTION



- 45% for critical issues
- 25% for high issues
- 15% for medium issues
- 5% gas optimization issues, best practices

BUDGET

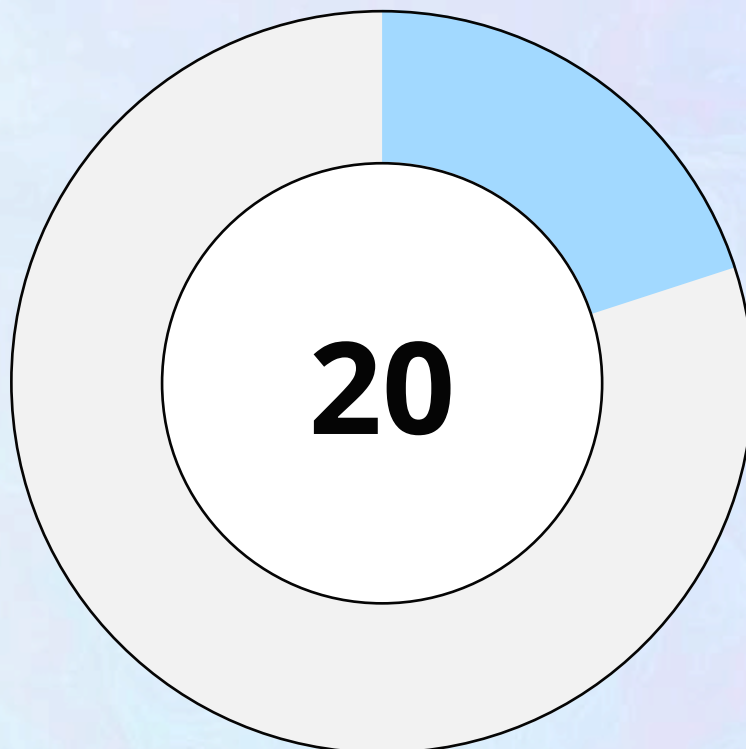
**\$40 000**

TOTAL PAID OUT

**\$2 000**

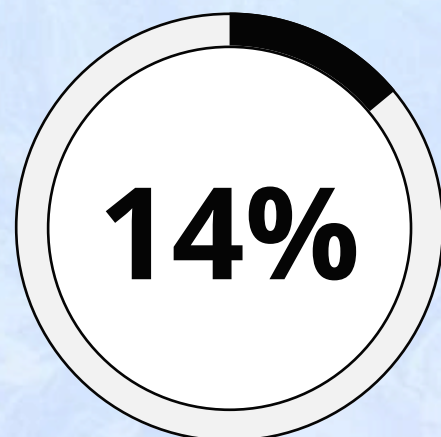
# FINDINGS

## 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	State
<div>KINETIAC-166</div> <div> <u>Borrowing donated tokens to grief and then steal all the tokens in the protocol</u></div>	<ul style="list-style-type: none"><li>• Informative</li></ul>	18.02.2025	Disclosed
<div>KINETIAC-161</div> <div> <u>Reward Distribution Precision Loss Could Lead to Zero Rewards</u></div>	<ul style="list-style-type: none"><li>• Informative</li></ul>	18.02.2025	Disclosed
<div>KINETIAC-158</div> <div> <u>The protocol allows borrowing small positions that can create bad debt</u></div>	<ul style="list-style-type: none"><li>• Informative</li></ul>	18.02.2025	Disclosed
<div>KINETIAC-149</div> <div> <u>Borrow Rate Exceeding borrowRateMaxMantissa Can Cause Protocol Failure</u></div>	<ul style="list-style-type: none"><li>• Informative</li></ul>	17.02.2025	Disclosed
<div>KINETIAC-148</div> <div> <u>Wrong `DOMAIN_TYPEHASH` definition</u></div>	<ul style="list-style-type: none"><li>• Low</li></ul>	17.02.2025	Disclosed
<div>KINETIAC-145</div> <div> <u>`depositTokens` May Lead to Sending Excessive Tokens</u></div>	<ul style="list-style-type: none"><li>• Informative</li></ul>	17.02.2025	Disclosed



	Name	Severity	Submission date	State
	KINETIAC-144 <u>`useOraclePrice` Cannot Be Modified</u>	• Informative	17.02.2025	Disclosed
	KINETIAC-138 <u>Borrow Rate Max Mantissa Not Optimized for Flare Network's Block Time</u>	• Informative	16.02.2025	Disclosed
	KINETIAC-137 <u>Interest rate manipulation in cToken markets where `borrowCap = 0` (i.e unlimited borrowing).</u>	• Informative	16.02.2025	Disclosed
	KINETIAC-120 <u>Zero-Address Allocation Burns Ether</u>	• Informative	14.02.2025	Disclosed
	KINETIAC-106 <u>Borrow rate calculation can cause `accrueInterest()` to revert, causing DoS in all major functionality</u>	• Informative	14.02.2025	Disclosed
	KINETIAC-105 <u>borrowRateMaxMantissa was not adjusted after switching from block.number to block.timestamp.</u>	• Informative	14.02.2025	Disclosed

Name

Severity

Submission  
date

State

KINETIAC-103



Inappropriate Maximum  
Borrow Rate for Fast Block  
Times on the Flare  
Network

• Informative

14.02.2025

Disclosed

KINETIAC-93



Validate Implementation  
Address in Proxy Upgrade

• Informative

13.02.2025

Disclosed

KINETIAC-80



Risk of Exchange Rate  
Manipulation Caused by  
Multiple Entry Point  
Tokens

• Informative

11.02.2025

Disclosed

KINETIAC-78



Hardcoded gas limit

• Informative

11.02.2025

Disclosed

KINETIAC-77



Consider overrides  
'renounceOwnership'  
function in  
'esProtocol.sol'.

• Informative

11.02.2025

Disclosed

KINETIAC-72



Division by Zero in APR  
Calculation in 'Lens.sol'.

• Low

11.02.2025

Disclosed

Name

Severity

Submission  
date

State

KINETIAC-64



Price Validation and  
Arithmetic Vulnerabilities  
in  
RedeemBurnRateCalculato  
rV3

• Informative

09.02.2025

Disclosed

KINETIAC-22



`Comptroller` expecting  
`getUnderlyingPrice` to  
return `0` for errors




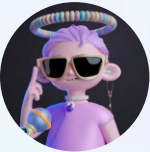

• Informative

21.01.2025

Disclosed

# SECURITY RESEARCHERS

## TOP HACKERS

Researcher	Total findings	Payouts	Place
 <u>@polaristow</u> Polaristow	13	\$547.58	1
 <u>@Bauer</u> Bauer	19	\$416.63	2
 <u>@0xiehnkta</u> Heavenly Demon	15	\$285.7	3
 <u>@erictee</u> erictee	12	\$285.7	4
 <u>@JakeFromStateFarm</u> JakeFromStateFarm	25	\$285.7	5



# CONCLUSION

---

## ABOUT KINETIC

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.