SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

SPYWOLF

Security Audit Report

Audit prepared for

KEKIUS

Completed on

January 6, 2025

OVERVIEW

This goal of this report is to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

> *The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal*
>
> \- SPYWOLF Team -

TABLE OF CONTENTS

KEKIUS

PROJECT DESCRIPTION:

Kekius Maximus, also known as “Pepe the frog Emperor,” is the sovereign ruler of the mythical Kekistani Empire, a realm that exists primarily in the digital universe of memes. Picture this: Pepe the Frog, that once innocent cartoon character, has evolved into a majestic emperor,crowned with the might of internet humor, reigning over a land where memes dictate law and laughter is the currency. His chariot? Golden, of course, pulled by fellow Pepe frogs because why not?

Release Date: January 8, 2025

Launchpad: Pinksale

Category: Meme token

KEY RESULTS

Cannot mint new tokens	PASSED
Cannot pause trading (honeypot)	PASSED
Cannot blacklist an address	PASSED
Cannot raise taxes over 25%?	PASSED
No proxy contract detected	PASSED
Not required to enable trading	PASSED
No hidden ownership	PASSED
Cannot change the router	PASSED
No cooldown feature found	PASSED
Bot protection delay is lower than 5 blocks	PASSED
Cannot set max tx amount below 0.05% of total supply	PASSED
The contract cannot be self-destructed by owner	PASSED

For a more detailed and thorough examination of the heightened risks, refer to the subsequent parts of the report.

CONTRACT INFO

Token Name
KEKIUS

Symbol
KEKIUS

Contract Address
0x7522f9ddC0f8e17A15421081c0aDe03d42E8Cf04

Network
BSC

Language
Solidity

Deployment Date
December 28, 2024

Contract Type
Standard

Total Supply
10,000,000,000 KEKIUS

Decimals
18

TAXES

Buy Tax
2%

Sell Tax
2%

Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

VULNERABILITY ANALYSIS

ID	Title	
SWC-100	Function Default Visibility	Passed
SWC-101	Integer Overflow and Underflow	Passed
SWC-102	Outdated Compiler Version	Passed
SWC-103	Floating Pragma	Passed
SWC-104	Unchecked Call Return Value	Passed
SWC-105	Unprotected Ether Withdrawal	Passed
SWC-106	Unprotected SELFDESTRUCT Instruction	Passed
SWC-107	Reentrancy	Passed
SWC-108	State Variable Default Visibility	Passed
SWC-109	Uninitialized Storage Pointer	Passed
SWC-110	Assert Violation	Passed
SWC-111	Use of Deprecated Solidity Functions	Passed
SWC-112	Delegatecall to Untrusted Callee	Passed
SWC-113	DoS with Failed Call	Passed
SWC-114	Transaction Order Dependence	Passed
SWC-115	Authorization through tx.origin	Passed
SWC-116	Block values as a proxy for time	Passed
SWC-117	Signature Malleability	Passed
SWC-118	Incorrect Constructor Name	Passed

VULNERABILITY ANALYSIS

ID	Title	
SWC-119	Shadowing State Variables	Passed
SWC-120	Weak Sources of Randomness from Chain Attributes	Passed
SWC-121	Missing Protection against Signature Replay Attacks	Passed
SWC-122	Lack of Proper Signature Verification	Passed
SWC-123	Requirement Violation	Passed
SWC-124	Write to Arbitrary Storage Location	Passed
SWC-125	Incorrect Inheritance Order	Passed
SWC-126	Insufficient Gas Griefing	Passed
SWC-127	Arbitrary Jump with Function Type Variable	Passed
SWC-128	DoS With Block Gas Limit	Passed
SWC-129	Typographical Error	Passed
SWC-130	Right-To-Left-Override control character (U+202E)	Passed
SWC-131	Presence of unused variables	Passed
SWC-132	Unexpected Ether balance	Passed
SWC-133	Hash Collisions With Multiple Variable Length Arguments	Passed
SWC-134	Message call with hardcoded gas amount	Passed
SWC-135	Code With No Effects	Passed
SWC-136	Unencrypted Private Data On-Chain	Passed

VULNERABILITY ANALYSIS

NO ERRORS FOUND

MANUAL CODE REVIEW

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time.

We categorize these vulnerabilities by 4 different threat levels.

THREAT LEVELS

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance, functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

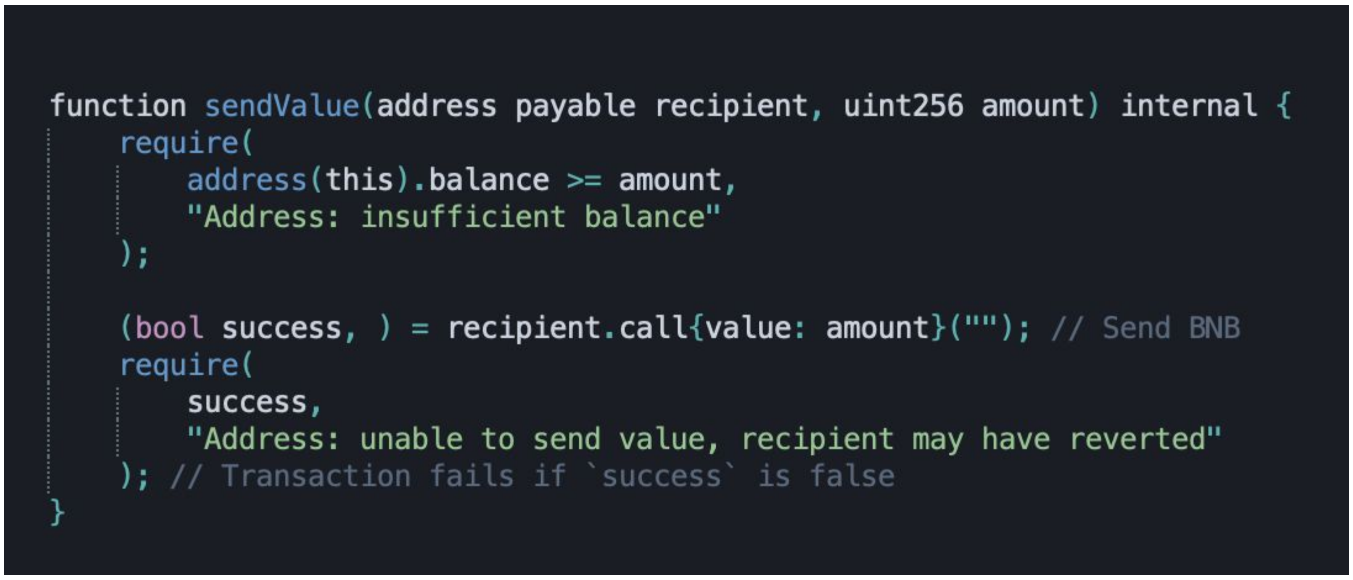
Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ Low Risk

At time of the audit, the marketing address is EOA and not contract. The marketing address currently uses a low-level .call() to send BNB via the sendValue() function. This call will fail and revert the transaction if the address cannot receive BNB (e.g., becomes a contract with restrictive logic). This could halt the contract's ability to distribute marketing fees, potentially leading to functionality issues if the address is not managed properly.



```
function sendValue(address payable recipient, uint256 amount) internal {
    require(
        address(this).balance >= amount,
        "Address: insufficient balance"
    );

    (bool success, ) = recipient.call{value: amount}(""); // Send BNB
    require(
        success,
        "Address: unable to send value, recipient may have reverted"
    ); // Transaction fails if `success` is false
}
```

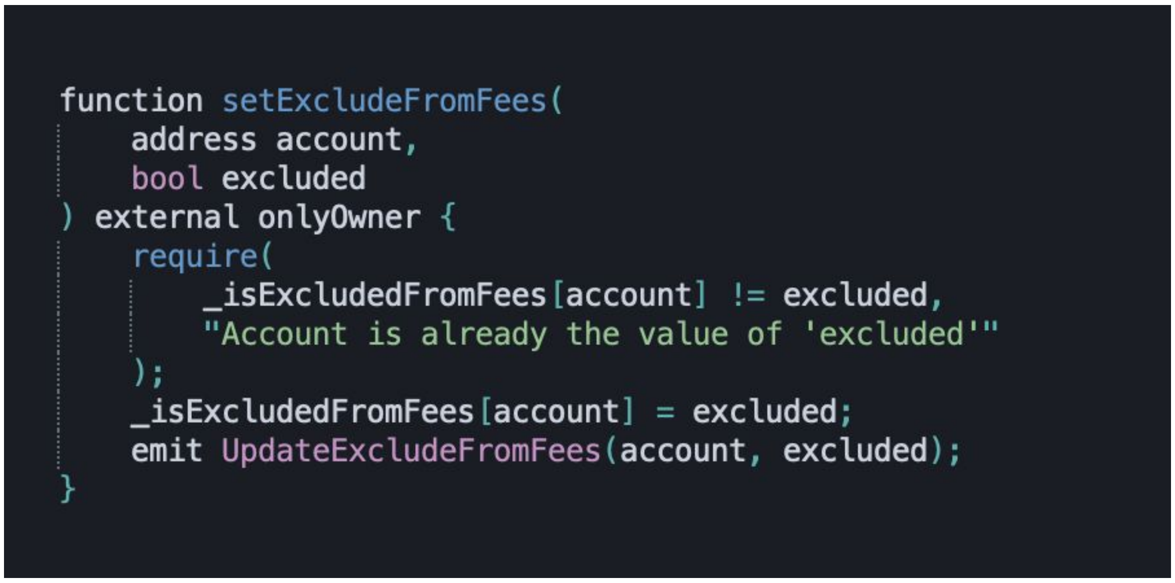
- Recommendation:
  - ○ Update the setMarketingWallet() function to remove the restriction preventing contract addresses. This allows using smart contracts capable of managing BNB programmatically.

FOUND THREATS

Informational

The owner can exclude an address from fees using the `setExcludeFromFees` function.

When an address is excluded, it will receive or transfer the full amount of tokens during buy, sell, or transfer transactions without any deductions for fees.



```
function setExcludeFromFees(
    address account,
    bool excluded
) external onlyOwner {
    require(
        _isExcludedFromFees[account] != excluded,
        "Account is already the value of 'excluded'"
    );
    _isExcludedFromFees[account] = excluded;
    emit UpdateExcludeFromFees(account, excluded);
}
```

ADDITIONAL INFO

Ownership and Access Control: The contract employs an Ownable pattern, granting the owner exclusive rights to execute specific administrative functions.

Maximum Fee Limit: The combined total of liquidity and marketing fees for both buy and sell transactions is capped at 10% (i.e., 1000 basis points out of a 10,000 basis point denominator).

Fee Exclusion: The owner can exclude specific addresses from fees using the setExcludeFromFees function. Excluded addresses will not incur any fees during transactions.

Trading Control: The contract includes a isTradingFee flag that, when set to false, restricts trading activities. This flag can be managed by the owner to control the commencement of trading.

Liquidity Management: The contract integrates with the PancakeSwap (Uniswap V2) router to facilitate automatic liquidity additions. Collected liquidity fees are converted to BNB and paired with KEKIUS tokens to add liquidity to the pool.

Marketing Wallet: A designated marketing wallet (marketingWallet) receives funds collected from marketing taxes. The owner can update this wallet address using the setMarketingWallet function, provided the new address is not a contract.

Swap and Liquify Mechanism: The contract includes a swapBack function that swaps accumulated tokens for BNB when a certain threshold is reached. This BNB is then allocated for liquidity and marketing purposes.

Anti-Bot Measures: The contract does not implement specific anti-bot measures such as cooldown periods or maximum transaction limits. However, the owner has control over trading activation and fee structures to mitigate potential bot activity.

TOKENOMICS

The following tokenomics are based on the project's whitepaper and/or website:

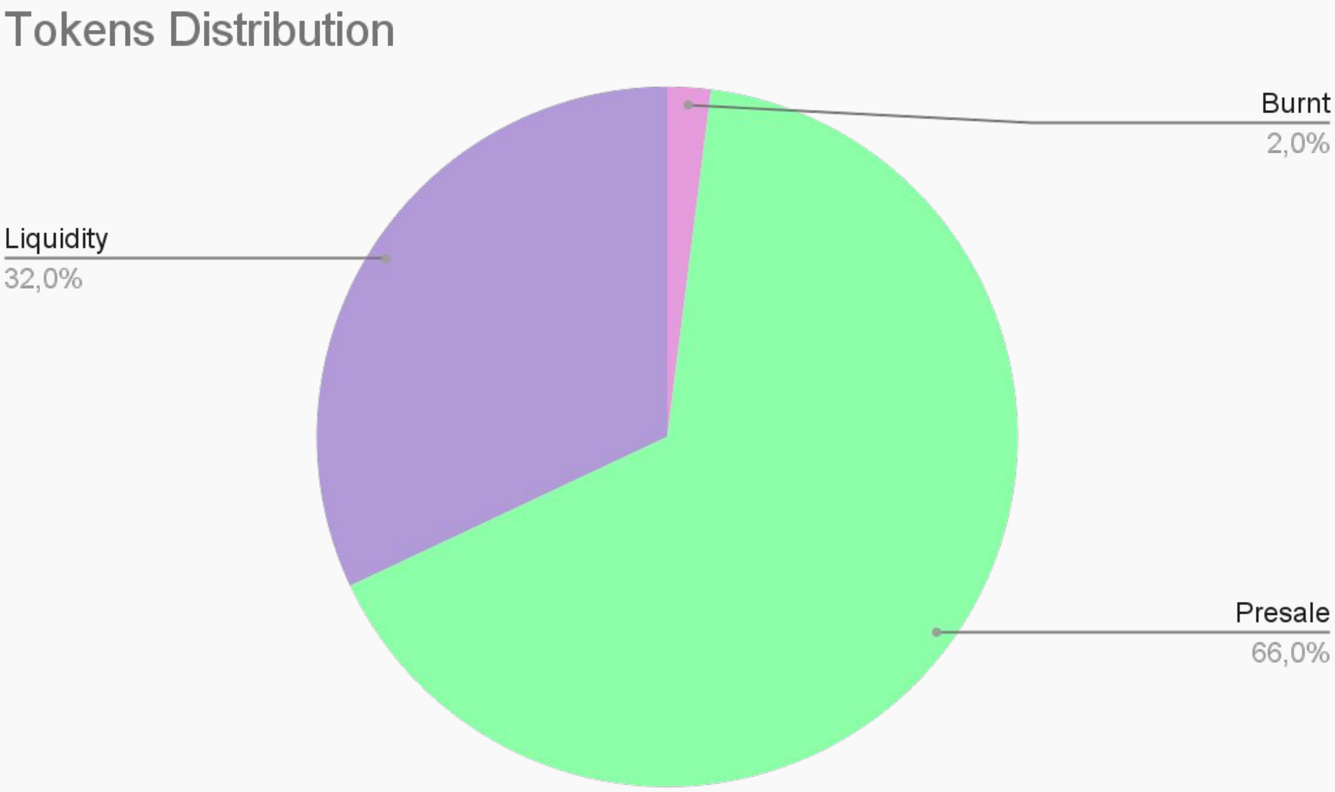
Tokenomics:

Burnt - 2%,

Presale - 66%,

Liquidity - 32%,

Token Distribution



WEBSITE

Website URL:
https://kekiusmeme.xyz/

Domain Registry
https://namecheap.com

Domain Expiration
2026-01-05

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

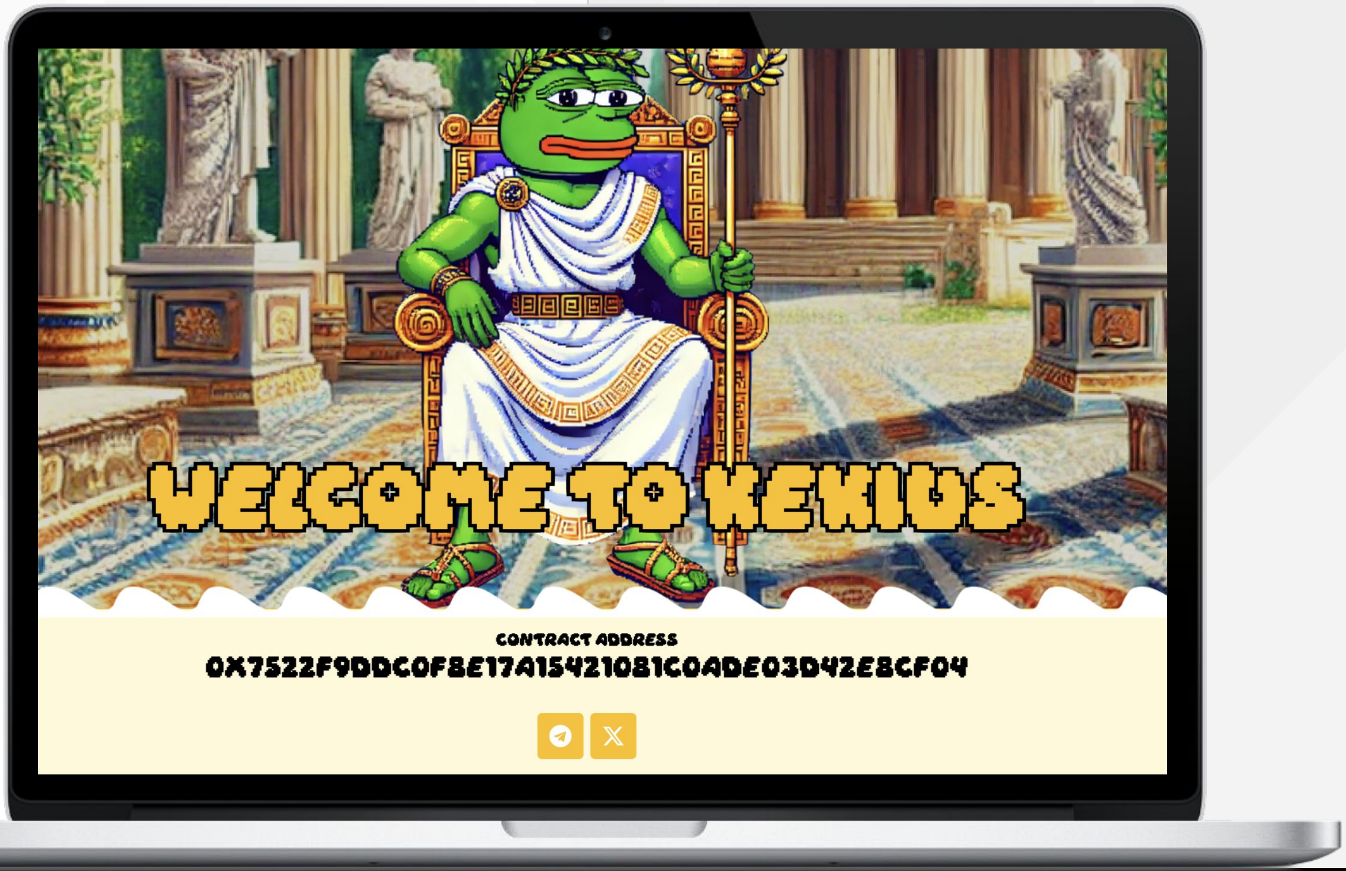
Design
Single page design with appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found. .

Whitepaper
No

Roadmap
Yes, goals set without time frames

Mobile-friendly?
Yes



WELCOME TO KEKIUS

CONTRACT ADDRESS

0X7522F9DDC0F8E17A15421081C0ADE03D42E8CF04

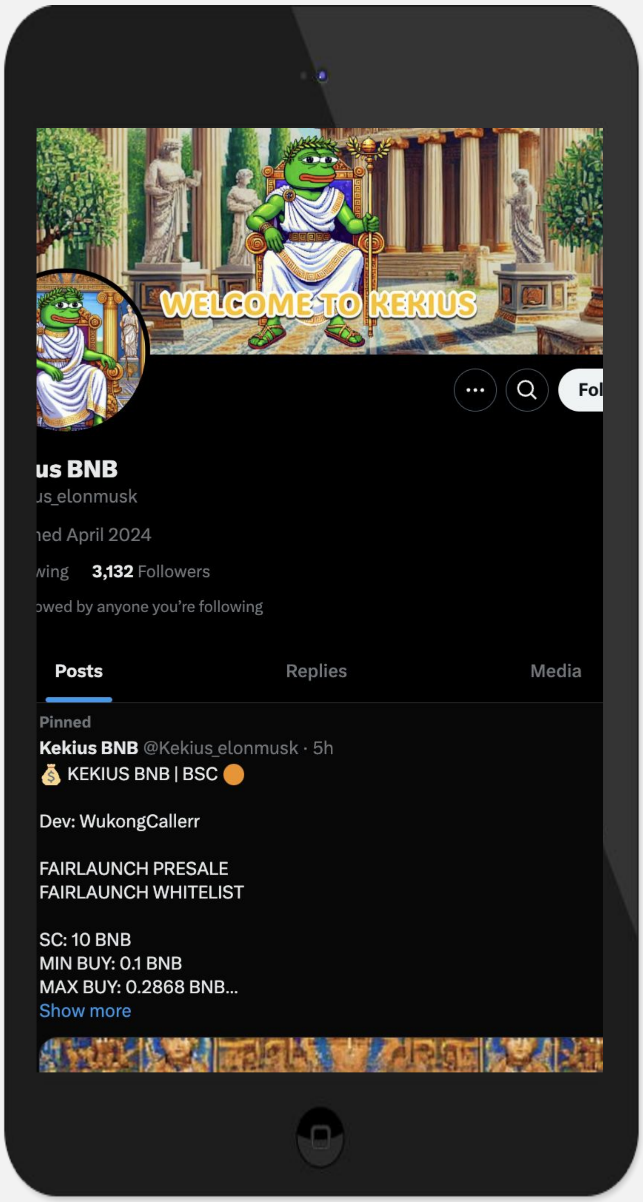
kekiusmeme.xyz

SOCIAL MEDIA

Social Score: 100%

ANALYSIS

Project's social media pages are active with daily posts.



us BNB
us_elonmusk
ned April 2024
wing 3,132 Followers
owed by anyone you're following

Pinned
Kekius BNB @Kekius_elonmusk · 5h
💰 KEKIUS BNB | BSC 🟠

Dev: WukongCallerr

FAIRLAUNCH PRESALE
FAIRLAUNCH WHITELIST

SC: 10 BNB
MIN BUY: 0.1 BNB
MAX BUY: 0.2868 BNB...
Show more

Twitter:

@Kekius_elonmusk

- 3,133 Followers
- Posts frequently
- Active

Discord

unavailable

Telegram:

@kekiusbnblv80

- 1 581 members
- Active mods
- Active members

Medium

unavailable

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 700 SUCCESSFUL CLIENTS
- ✓ MORE THAN 1000 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.