SPYWOLF

Security Audit Report

Audit prepared for

Husky Inu

Completed on

May 30, 2025

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.

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

HUSKY INU

PROJECT DESCRIPTION

Based on the Pinksale link:

"HUSKY INU isn’t the next DOGE, SHIBA, or FLOKI — it’s the cold-blooded alpha of a new era.

100B supply. LP locked. 5% tax for marketing & buybacks — no tax during presale, and reduced to 0% before renounce and CG/CMC listing. No unlocked tokens. Just pure meme energy and a pack built to dominate.

Run with us — or freeze outside.

Release Date: Presale starts 2025.05.30 15:00 (UTC)

Category: Token

CONTRACT INFO

Token Name
SLOTH

Symbol
S

Contract Address
0xE644Ce61cC26a4Eb5FBaeb4567b2f23FAD65F1aa

Network
Binance Smart Chain

Language
Solidity

Deployment Date
May 25, 2025

Contract Type
ERC20 Token

Total Supply
1,000,000,000

Status
Presale

TAXES

Buy Tax
0%

Sell Tax
0%

*owner can set buy/sell fees up to 10%

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

FEATURED WALLETS

Owner address	0x8C1C03B9bDbc0194aA3EDdf3e2a29c028b1347FB
Marketing fee receiver	0xd807b657C20830883023d57322f22B1E5df42A56
LP address	**Pool address:** 0x670aF5a281fd7866ae7722C151788d25E79CAea2 **PancakeSwap Address:** To be confirmed after LP creation on PancakeSwap and updated in the token contract by the owner. **Lock Details:** Based on the Pinksale information, the liquidity is expected to be locked via PinkLock (Pinksale's locker) for 365 days. The exact percentage locked and specific unlock date will be available once the lock transaction is completed. For example, if locked on May 27, 2025, it would unlock around May 27, 2026.

TOP 3 UNLOCKED WALLETS

-	Not Launched Yet
-	Not Launched Yet
-	Not Launched Yet

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

⚠ High Risk

Owner's Control Over HUSKY Tax Rates (Up to 20% Total)
The owner of the HUSKY contract has the unilateral ability to set and change the reflectionTax and treasuryTax at any time. The contract limits the *combined* total of these two taxes to a maximum of 20%. While the project claims a "5% tax... reduced to 0% later," the owner can technically implement any tax structure up to this 20% cap in the meantime. This could be used to make trading highly unprofitable or to extract excessive value from transactions.

```
uint16 public reflectionTax;
uint16 public treasuryTax;

function setFee(
    uint16 reflectionTax_,
    uint16 treasuryTax_
) public onlyOwner { // Only owner can call
    validateFees(reflectionTax_, treasuryTax_); // Checks sum <= 20%
    reflectionTax = reflectionTax_;
    treasuryTax = treasuryTax_;
    emit ChangedFees(reflectionTax_, treasuryTax_);
}

function validateFees(
    uint16 reflectionTax_,
    uint16 treasuryTax_
) internal pure {
    require(
        reflectionTax_ + treasuryTax_ <= 20, // Max 20%
        "Fees cannot be greater than 20%"
    );
}
```

Recommendation

- The community should push for the owner to set the tax to the claimed rate (or 0%) as soon as possible after launch.
- Ultimately, the owner should **renounce ownership** after setting the final tax rate (ideally 0%, as promised) to make it immutable.
- Monitor on-chain transactions for any calls to the setFee() function.

FOUND THREATS

⚠ High Risk

Owner's Control Over HUSKY Treasury Address
The treasuryTax portion of the transaction fees is converted to BNB and sent to a treasuryAddress. The owner of the HUSKY contract can change this treasuryAddress at any time to any wallet they control. This means that any BNB accumulated from the treasuryTax can be diverted by the owner.

```
address payable public treasuryAddress;

function setTreasuryAddress(address payable account) external onlyOwner { // Only owner
    require(account != address(0x0), "treasury address cannot be zero");
    treasuryAddress = account;
    _isExcludedFromFee[account] = true; // New treasury also excluded
    emit UpdatedTreasuryWallet(account);
}

// BNB from treasury tax swaps is sent to 'treasuryAddress' in the
// swapExactTokensForETHSupportingFeeOnTransferTokens (or equivalent) function calls.
```

Recommendation

- The project should use a multi-signature wallet for the treasuryAddress for better security and accountability before renouncing ownership.
- The owner should **renounce ownership** after the treasury system is stable and the tax is set to its final state (ideally 0%).
- Monitor on-chain transactions for any calls to setTreasuryAddress().

FOUND THREATS

⚠ High Risk

Owner's Liquid 2% HUSKY Token Holding (2 Billion HUSKY)
The owner's wallet (0xBc15315C...4BA0fa98a) holds 2 Billion HUSKY tokens (2% of the total supply) that are not locked and not part of the Pinksale Fair Launch allocation. These tokens can be sold on the market at any time by the owner.

Impact: A sudden sale of these 2 Billion tokens, especially into a new and potentially thin liquidity pool, can cause a significant price drop ("dump"), harming investors. This also contradicts the Pinksale claim of "No unlocked tokens," raising transparency concerns.

Recommendation

- The project team must clarify the purpose of these 2 Billion liquid tokens and address the "No unlocked tokens" discrepancy.
- Ideally, these tokens should also be subject to a transparent locking or vesting schedule if they are intended for team/project use.
- Investors should monitor the owner's wallet for movements of these tokens.

FOUND THREATS

⚠ Medium Risk

uniswapV2Pair Variable Verification & Potential Tax Collection Issues
The HUSKY contract (assuming it uses the Redis code verbatim) will attempt to create its own LP pair in its constructor and store this pair's address in its internal uniswapV2Pair variable. Transaction taxes are only applied if sender == uniswapV2Pair || recipient == uniswapV2Pair. However, the *main* HUSKY trading liquidity pool will be created by the Pinksale Fair Launch contract.

Risk: If the HUSKY contract's internal uniswapV2Pair variable does not correctly reference the main Pinksale-generated trading pair, the tax mechanism might not trigger for buys/sells on that main pair. This could mean no taxes are collected, or they are collected incorrectly/unexpectedly.

```
uniswapV2Pair = IUniswapV2Factory(uniswapV2Router.factory()).createPair(
    address(this),
    getNativeCurrency()
);

// In _transferStandard function of Redis (assumed HUSKY)
bool takeFee = !_isExcludedFromFee[sender] &&
               !_isExcludedFromFee[recipient] &&
               (sender == uniswapV2Pair || recipient == uniswapV2Pair) && // Critical check
               !inSwap;
```

Recommendation

- After HUSKY is deployed and the Pinksale LP is created, check the address stored in the HUSKY contract's public uniswapV2Pair variable (via BscScan's "Read Contract" tab).
- Confirm if this address matches the main HUSKY/BNB (or other pairing) liquidity pool address created by Pinksale.
- If the HUSKY contract was intended to use the Pinksale LP for its tax logic, its constructor should have been modified to accept the Pinksale LP address post-creation or another mechanism to set it correctly, rather than creating its own.

FOUND THREATS

⚠ Medium Risk

Reliance on Future Promises (0% Tax, Renouncement)
The project claims that taxes will be reduced to 0% and ownership of the HUSKY contract will be renounced "before CG/CMC listing." These are positive long-term goals for decentralization and investor confidence.

Risk: These are currently promises, not guaranteed actions hardcoded to occur automatically. Until these actions are verifiably completed on-chain (calling setFee(0,0) and renounceOwnership() on the HUSKY contract), the owner retains all the high-risk privileges mentioned above. There's a risk of delays or the team not following through.

Recommendation

- The community should seek a clear, committed timeline from the project for these actions.
- Monitor the HUSKY contract on BscScan for these transactions. Renouncement is a permanent action.

FOUND THREATS

Informational

Fixed Total Supply

The HUSKY token contract is designed with a fixed total supply (100 Billion HUSKY) set at the time of deployment. The code does not contain any functions that would allow the owner or anyone else to mint new HUSKY tokens after the initial creation. This prevents an unexpected increase in the total supply, which can devalue existing tokens.

Standard Trading Functions (No Pause/Blacklist)

The contract code does not include common potentially problematic functions like pauseTrading() (which would allow the owner to halt all trading) or blacklistAddress() (which would allow the owner to prevent specific wallets from trading). This means once trading is live on a DEX, it cannot be arbitrarily stopped or censored at the contract level by these specific common functions.

Pinksale Launch & LP Lock

The project launched via Pinksale, which typically includes a mechanism to lock the initial liquidity pool.

https://www.pinksale.finance/launchpad/bsc/0x2D8dD9E152Bd52ff7a29BcCE1eC513990Fe5Cd43

FOUND THREATS

Informational

Renounceable Ownership

The contract includes a standard renounceOwnership() function. If the owner calls this function, they will permanently give up all special owner privileges over the contract (like changing fees, treasury address, etc.). The project has claimed they will do this after setting taxes to 0%.

No selfdestruct Function

The contract code does not contain a selfdestruct function, meaning the owner cannot destroy the contract and remove its code and balance from the blockchain.

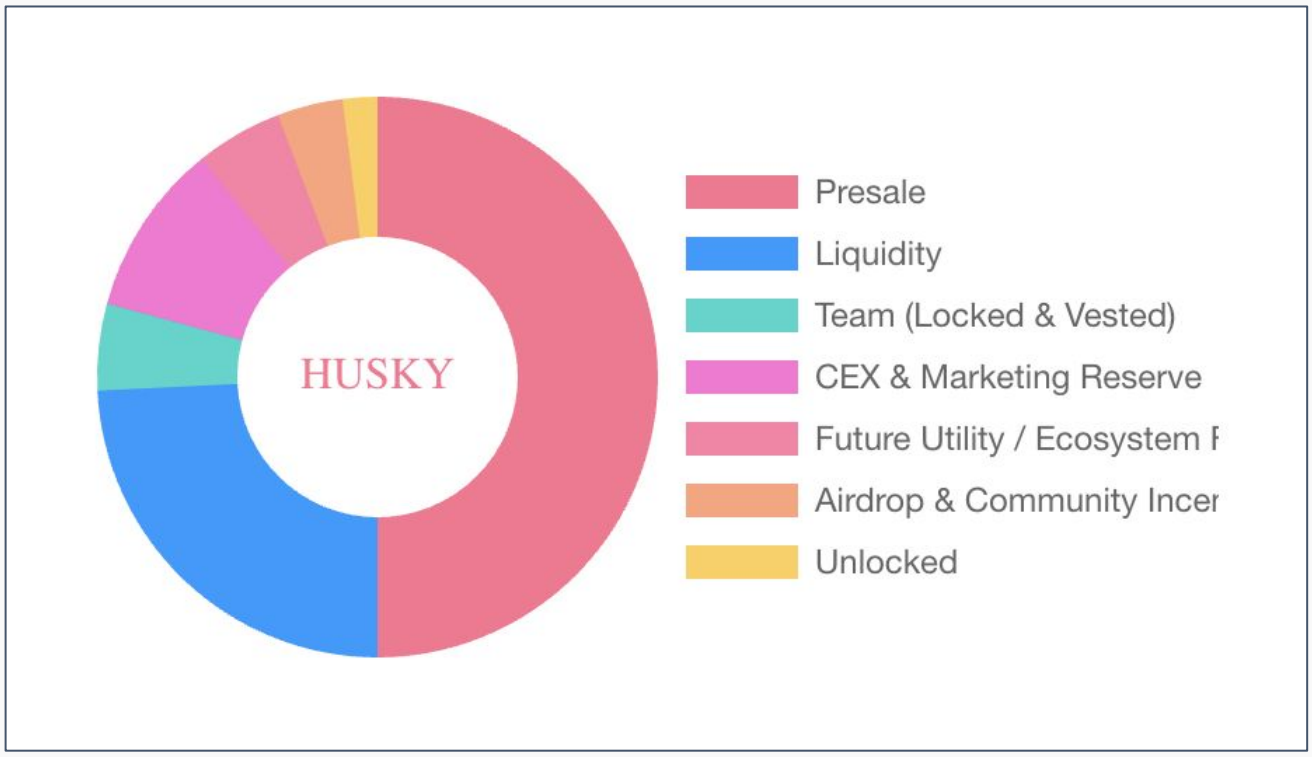
Significant Portion of Tokens Allocated for Liquidity & Locked

- A very large portion of the total HUSKY supply (74.225% or 74.225 Billion tokens) was sent to the Pinksale Fair Launch contract, which is intended for the public sale and subsequent automatic creation and locking of the main Liquidity Pool (LP).
- Additionally, the owner proactively locked another 23.775 Billion HUSKY tokens (23.775% of supply) via Pinksale's PinkLock V2 service, with unlocks starting July 1, 2025, or later. These likely cover team, ecosystem, or marketing allocations.
- These actions demonstrate an intent to secure a large part of the token supply against immediate sell-offs by the project or team.

TOKENOMICS

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

- 50% Presale
- 24.22% Liquidity
- 5% Team
- 3.77% Airdrop
- 10% CEX/Marketing
- 5% Marketing Reserve
- 5% Future Utility
- 2% Unlocked



WEBSITE

Website URL
https://huskyinucoin.com/

Domain Registry
http://www.spaceship.com

Domain Expiration
5/26/2026

Technical SEO Test
Passed

Security Test
Passed

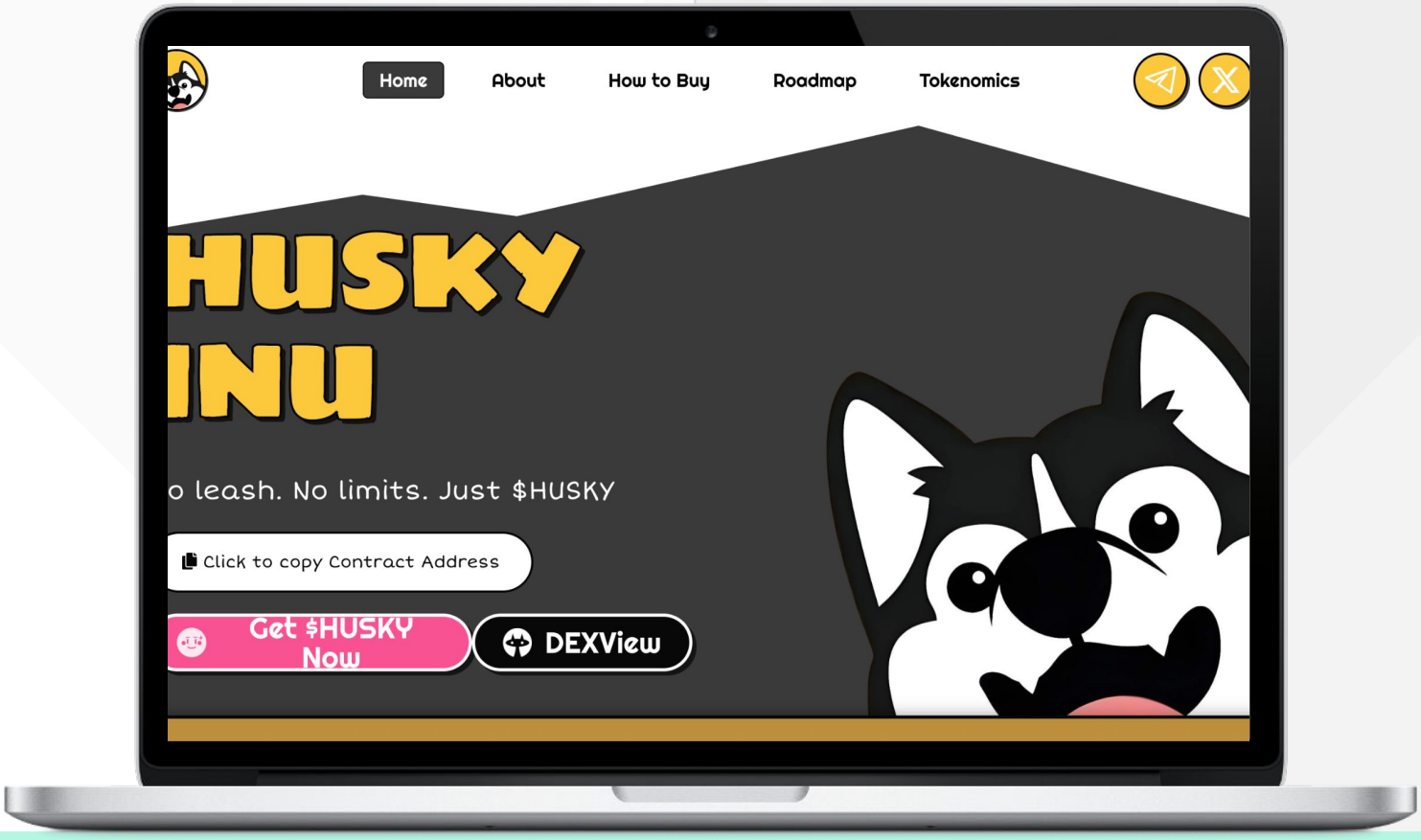
Design
Very nice design style and overall composition of colors to match the memecoin industry.

Content
The information is clear and easy to read for potential investors.

Whitepaper
No

Roadmap
Yes (Without dates)

Mobile-friendly?
Yes



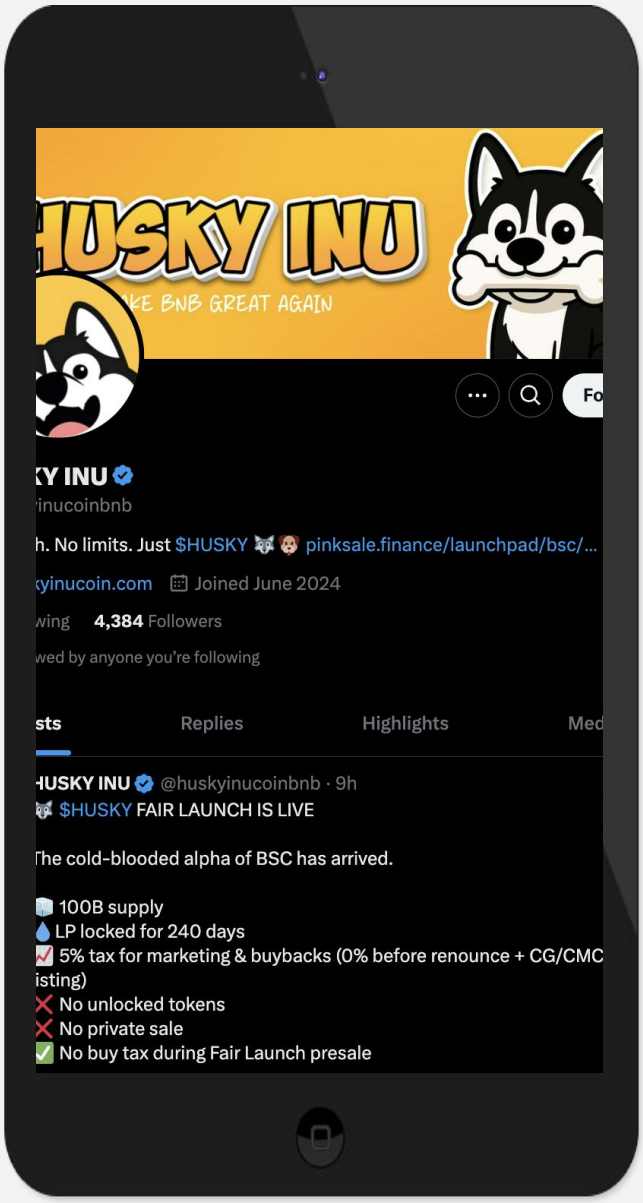
huskyinucoin.com

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

The project's social media pages are new.



Twitter's X

@huskyinucoinbnb

- 4,384 Followers
- 1 post

Discord

- Not available

Telegram

@huskyinuportal

- 47 subscribers
- 1 post
- New account

Medium

- Not available

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.