SPYWOLF

Security Audit Report

Audit prepared for

SLOTH

Completed on

May 25, 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

SLOTH

PROJECT DESCRIPTION

Based on the Pinksale link:

"Hi, I'm $SLOTH! Built on the BSC, S combines the energy of memes with the power of AI, creating a platform that's fun, engaging, and smart.

Why Choose SLOTH?

💡 Computer desktop pet

💡 AI-Powered Utility

🔥 PinkSale Exclusive

🌍 Community First"

Release Date: Presale starts 2025.05.25 11:00 (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

withdrawTokens() Function Callable by Anyone
This function allows any external address to trigger the withdrawal of any tokens (including collected SLOTH fees or BNB from swaps) held by the contract to the marketingWalletAddress. This is highly unorthodox.

```
function withdrawTokens(address[] memory tokens) external {
    for (uint256 index = 0; index < tokens.length; index++) {
        uint256 amount;
        if (TransferHelper.isETH(tokens[index])) {
            amount = address(this).balance;
            // ETH is sent to marketingWalletAddress
            TransferHelper.safeTransferETH(marketingWalletAddress, amount);
        } else {
            amount = IERC20(tokens[index]).balanceOf(address(this));
            // Other tokens are sent to marketingWalletAddress
            TransferHelper.safeTransferWithoutRequire(tokens[index], marketingWalletAddress, amount);
        }
        emit Withdraw(tokens[index], msg.sender, marketingWalletAddress, amount);
    }
}
```

Recommendation

- Modify the function visibility from external to external onlyOwner. This will restrict the ability to trigger these withdrawals to the contract owner, which is standard practice for such administrative functions.

FOUND THREATS

⚠ Medium Risk

Owner's Control Over Transaction Fees
The owner can change buy, sell, and wallet-to-wallet transfer fees (up to 10% each) at any time.

```
function setBuyFee(uint256 _buyFee) external onlyOwner {
    require(_buyFee <= 10, "Buy Fee cannot be more than 10%");
    buyFee = _buyFee;
    emit BuyFeeUpdated(buyFee);
}

function setSellFee(uint256 _sellFee) external onlyOwner {
    require(_sellFee <= 10, "Sell Fee cannot be more than 10%");
    sellFee = _sellFee;
    emit SellFeeUpdated(sellFee);
}
// Similar function: setWalletToWalletTransferFee
```

Recommendation

- The team should maintain clear communication with the community regarding any fee adjustments. For enhanced trust, consider implementing a timelock mechanism for fee changes or, if feasible, placing fee control under a multi-signature wallet if ownership is not renounced.

FOUND THREATS

Informational

Trading is Enabled

The owner has called the `enableTrading()` function, so the token is actively tradable.

Fees Initialized at 0%

The `buyFee` and `sellFee` are initialized to 0% in the contract. The owner can raise these fees up to 10% each at any time.

Pinksale Launch & LP Lock

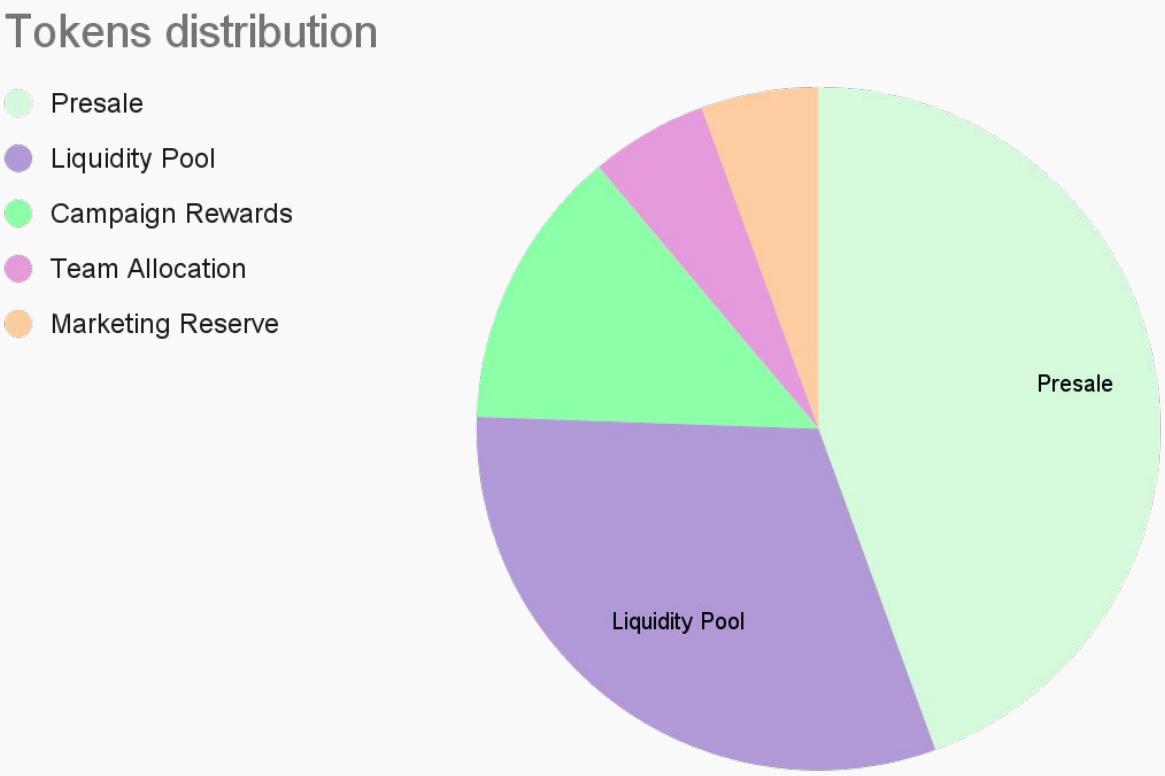
The project launched via Pinksale, which typically includes a mechanism to lock the initial liquidity pool. The stated lockup period is 365 days, which is a positive factor against immediate LP removal by the team.

https://www.pinksale.finance/launchpad/bsc/0x670aF5a281fd7866ae7722C151788d25E79CAea2

TOKENOMICS

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

- 40% Presale
- 38% Liquidity Pool
- 12% Campaign Rewards
- 5% Team Allocation
- 5% Marketing Reserve



WEBSITE

Website URL
Not Available Yet

Domain Registry
Not Available Yet

Domain Expiration
Not Available Yet

Technical SEO Test
Not Available Yet

Security Test
Not Available Yet

Design
Not Available Yet

Content
Not Available Yet

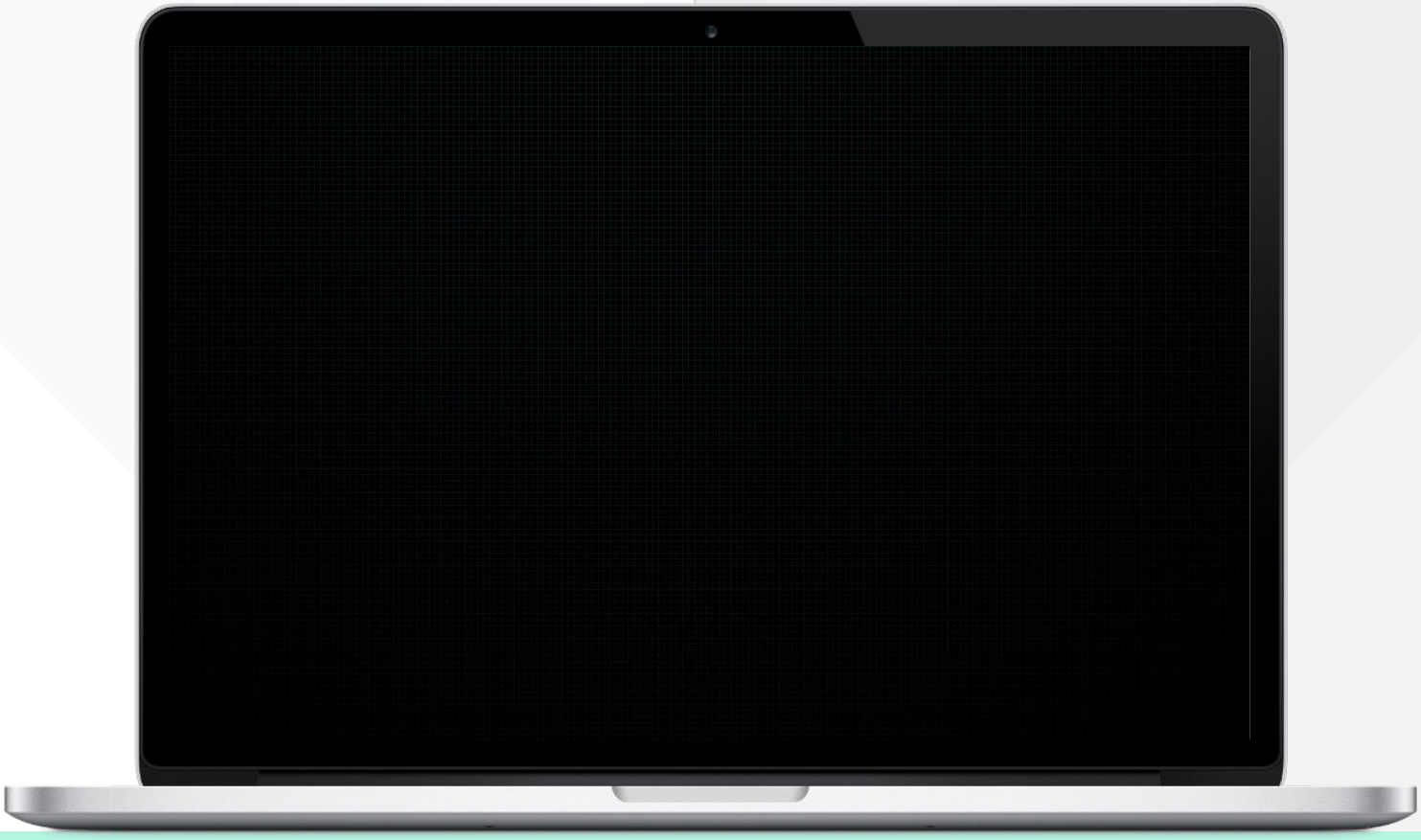
Whitepaper
Not Available Yet

Roadmap

Not Available Yet

Mobile-friendly?

Not Available Yet



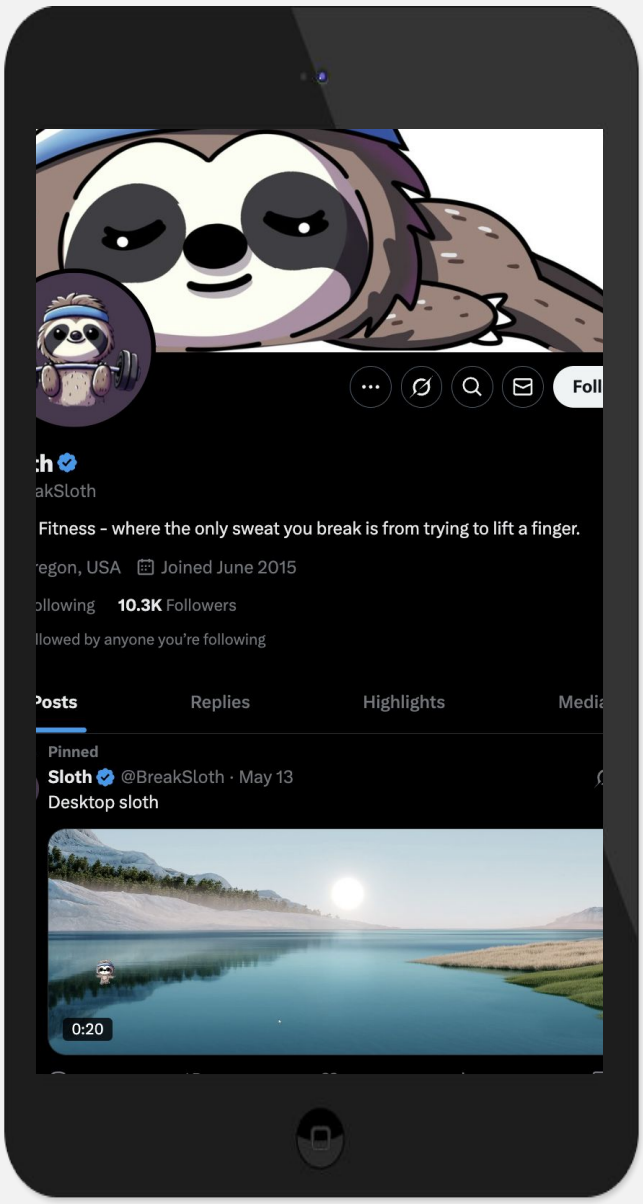
Not Available Yet

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

The project's social media pages are new but active.



Twitter's X

@BreakSloth

- 10.3K Followers
- Responds to comments
- Daily posts

Discord

- Not available

Telegram

@BreakSloth

- 7 subscribers

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.