SPYWOLF

Security Audit Report

Audit prepared for

HapNeiro

Completed on

November 13, 2024

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

HapNeiro

PROJECT DESCRIPTION:

No information yet

Release Date: November 2, 2024

Launchpad: Fairlaunch

Category: Dividend token

KEY RESULTS

Cannot mint new tokens	*
Cannot pause trading (honeypot)	NOT 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	**
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 can turn into honeypot for users that supply liquidity - impossible to retrieve HapNeiro/USDT tokens back.

*New tokens can be minted based on user's dividend token holdings

** Token cannot be bought and sold in the same block

CONTRACT INFO

Token Name
HapNeiro

Symbol
HapNeiro

Contract Address
0xd63B34B48AF447f36BE3f738819446424487c397

Network
BSC

Language
Solidity

Deployment Date
Nov 02, 2024

Contract Type
Dividend

Total Supply
15,397,602

Decimals
18

TAXES

Buy Tax
3%

Sell Tax
3%

*Taxes cannot be changed

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

SMART CONTRACT STATS

Calls Count	39305
External calls	8527
Internal calls	30778
Transactions count	17565
Last transaction time	2024-11-13 14:00:32 UTC
Deployment Date	2024-11-06 00:06:50 UTC
Create TX	0xcdfa18c99aacdecd56492504fcd7957a2856ff944b43026e9046b85eb17b121f
Owner	0x0000000000000000000000000000000000000000
Deployer	0xA7a5947CAa6Cd4B73c1fC2c2F7B6B14dCd643353

TOKEN TRANSFERS STATS

Transfer Count	88634
Total Amount	98291627.42873359 HapNeiro
Median Transfer Amount	28.777417272643024 HapNeiro
Average Transfer Amount	1108.9607535340117 HapNeiro
First transfer date	2024-11-02
Last transfer date	2024-11-13
Days token transferred	12 Days

FEATURED WALLETS

Owner address	Ownership is renounced 0x0000000000000000000000000000000000000000
Marketing fee receiver	0x71F914A4907DBBEA4b4574adA8Ab33013724b509 0xfEDfc8Ac8D5106a7A942F06dde074467E32268BE 0xf75B3Da75A2272fdA1528027d35483E6917D07ca
LP address	**Pancakeswap:** 0x0dB963e6E63724AdFCD6eE2380ADCF61267aA9B1 **32.34% locked in PinkLock - unlocks at Saturday, May 10, 2025**

TOP 3 UNLOCKED WALLETS

6.10%	0x2941466238F1b8457Eab49cc1A0D8f827F31281E
0.5%	0x11BCC295F6EB83DEE5bd374F4813de58341575aA
0.19%	0xA7E8A0d3954F73A1c09CE4efb33F386aDEB65E63

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.

Code Score: 30%

FOUND THREATS

⚠ High Risk: 2

No high risk-level threats found in this contract.

⚠ Medium Risk: 1

No medium risk-level threats found in this contract.

⚠ Low Risk: 0

No low risk-level threats found in this contract.

Contract’s ownership is renounced.
Limited functionality can be used by the Dev (deployer) wallet.

FOUND THREATS

⚠ High Risk

When users adds liquidity twice, only the second time is counted and the first one is nullified. Scenario:
User adds 1000 USDT paired with HapNeiro one time
The second time user adds 100 USDT paired with HapNeiro
When user decides to quit his position he will be able to only retrieve 100 USDT with corresponding amount HapNeiro. 1000 USDT will be stuck in the liquidity pair.
When users add liquidity with order HapNeiro/USDT instead of USDT/HapNeiro no dividend tracker will be minted and t
This will renders it impossible to withdraw the liquidity which is added first

If token’s deployer alter user’s stats from initLpAmounts() function at time when user is already added liquidity, user will not be able to retrieve the liquidity back.

FOUND THREATS

⚠ High Risk

Overflow occurs in addOrRemove (_userInfo[from/to].lpAmount) and liquidity add remain undetected if the order is HapNeiro/USDT instead of USDT/HapNeiro.
This renders liquidity removal impossible if _userInfo[from/to].lpAmount is not changed manually for each individual investor by the deployer.

```
function _transfer(address from, address to, uint256 amount) internal override {
    require(from != address(0), "ERC20: transfer from the zero address");
    require(to != address(0), "ERC20: transfer to the zero address");
    require(balanceOf(from) >= amount, "error");
.............................
    (bool isAddLP, bool isRemoveLP) = addOrRemove(from, to, amount);
    processMine(from);
    processMine(to);
.............................

}

function addOrRemove(address from, address to, uint256 amount) internal returns (bool isAddLP, bool isRemoveLP) {
.............................
    uint256 addLPLiquidity;

        addLPLiquidity = _isAddLiquidity(to, addAmount);
        if (addLPLiquidity > 0) {
            isAddLP = true;
            _userInfo[from].lpAmount += addLPLiquidity;
            try
                lpTracker.setBalance(
                    payable(from),
                    _userInfo[from].lpAmount
                )
            {} catch {}
            try
                minerTracker.setBalance(
                    payable(from),
                    _userInfo[from].lpAmount
                )
            {} catch {}
        }
    }

    uint256 removeLPLiquidity;
    if (from == uniswapV2Pair) {
        removeLPLiquidity = _isRemoveLiquidity(from, amount);
    }
    if (removeLPLiquidity > 0 && !_isExcludedFromFees[to]) {
        require(_userInfo[to].lpAmount >= removeLPLiquidity, "lp min");
        isRemoveLP = true;
        _userInfo[to].lpAmount -= removeLPLiquidity;
        try
            lpTracker.setBalance(payable(to), _userInfo[to].lpAmount)
        {} catch {}
        try
            minerTracker.setBalance(payable(to), _userInfo[to].lpAmount)
        {} catch {}
    }
}
```

FOUND THREATS

⚠ High Risk

Dev wallet (deployer) can alter user's 'lp dividend tracker' and 'miner dividend tracker' holdings.
New HapNeiro tokens are minted (mined) based on user's 'miner dividend tracker' holdings.
Over time this may lead to token inflation and liquidity drain.
Up to 50,000 tokens can be minted each 24 hours.
Each 30 days mintable tokens are cut in half.

If user’s userInfo.lpAmount is set to 0 at theme when the user is currently added liquidity, user won’t be able to remove his liquidity.

```
function initLPAmounts(
    address[] memory accounts,
    uint256 lpAmounts
) public onlyDev {
    uint256 len = accounts.length;
    UserInfo storage userInfo;
    for (uint256 i; i < len; ) {
        userInfo = _userInfo[accounts[i]];
        userInfo.lpAmount = lpAmounts;
        lpTracker.setBalance(payable(accounts[i]), userInfo.lpAmount);
        minerTracker.setBalance(payable(accounts[i]), userInfo.lpAmount);
        unchecked {
            ++i;
        }
    }
}
```

FOUND THREATS

Informational: 1

Dev wallet (deployer) can withdraw any tokens from the contract. When this function is present, in cases tokens and/or BNB are sent into the contract by mistake or purposefully, contract's deployer can retrieve them.

```
function claimStuckToken(address _token, uint256 _amount) public onlyDev {
    IERC20(_token).transfer(msg.sender, _amount);
}

function claimStuckETH() public onlyDev {
    payable(msg.sender).transfer(address(this).balance);
}
```

Each 30 days after the initial launch, mintable supply will reduce in half. Current mintable supply per day is 50,000.

```
function _transfer(
    address from,
    address to,
    uint256 amount
) internal override {
.....................................
    if (block.timestamp >= halfTS) {
        mineAmountOneDay = mineAmountOneDay / 2;
        halfTS = halfTS + 30 days;
    }
.....................................
}
```

The following tokenomics are based on BSCScan:

Tokenomics:

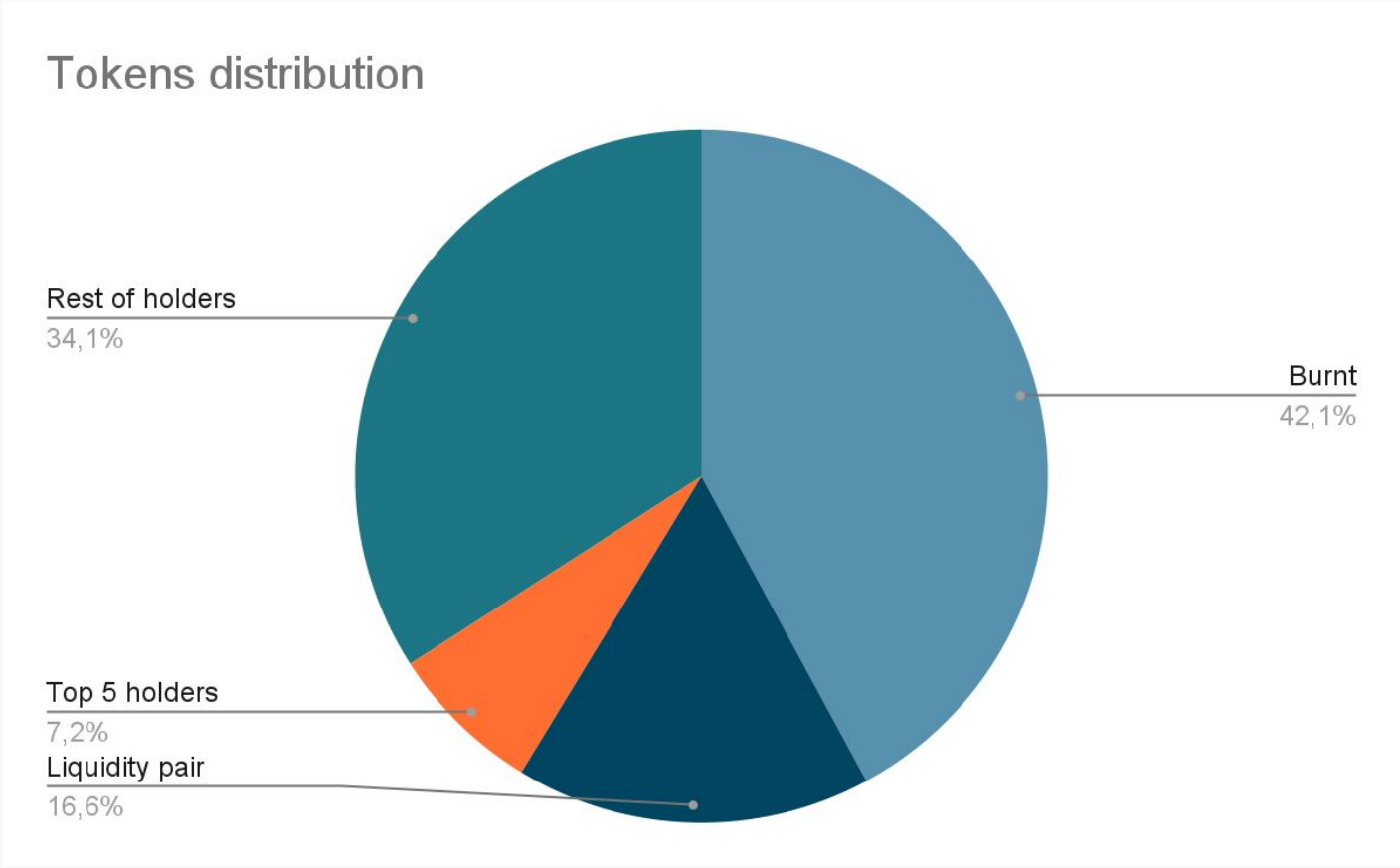
Burnt - 42.1%,

Liquidity pair - 16.6%,

Top 5 holders - 7.2%,

Rest of holders - 34,1%,

Token Distribution



TOKENOMICS

WEBSITE

Website URL:
unavailable

Domain Registry
https://www.godaddy.com

Domain Expiration
unavailable

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

Design
unavailable

Content
unavailable

Whitepaper
unavailable

Roadmap

unavailable

Mobile-friendly?

unavailable

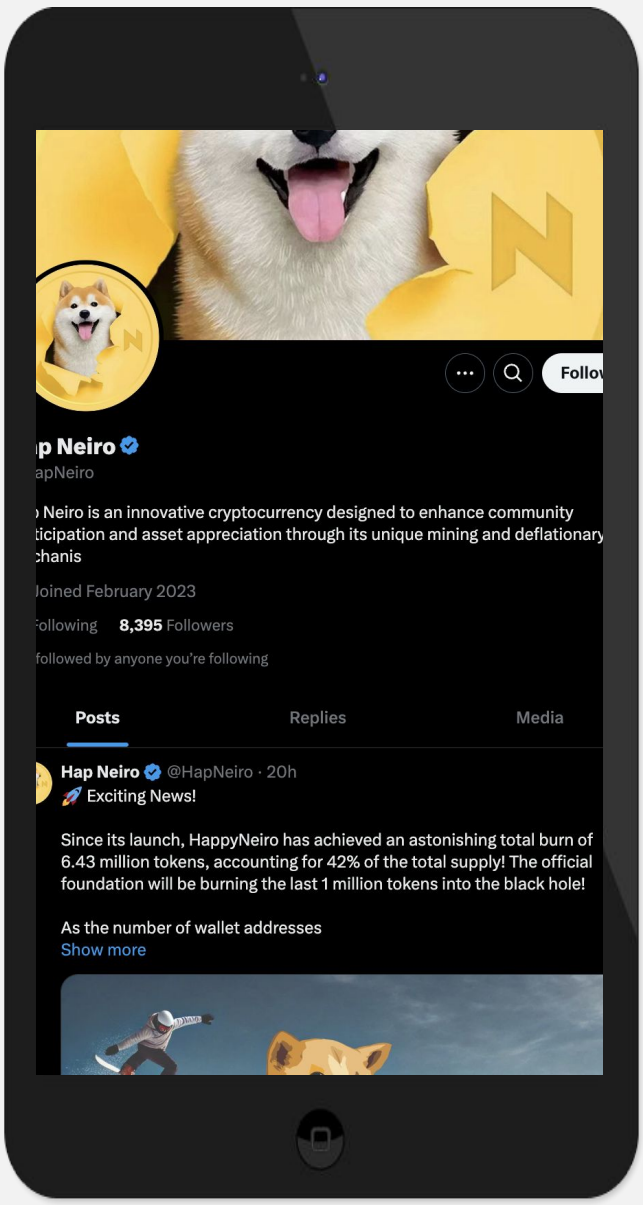
Website Score: 0%

SOCIAL MEDIA

Social Score: 100%

ANALYSIS

Project’s social media pages are active



Twitter:

@HapNeiro

- 8 194 followers
- Posts frequently
- Active

Discord

Unavailable

Telegram:

Unavailable

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.