SPYWOLF

Security Audit Report

Audit prepared for

RedditDoge

Completed on

September 12, 2024

SPYWOLF.CO
@SPYWOLFNETWORK
@SPYWOLFNETWORK

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

RedditDoge

PROJECT DESCRIPTION:

There is no description on the project's website.

Release Date:

Launchpad: Pinksale

Category: Wallet

KEY RESULTS

Cannot mint new tokens	PASSED
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	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.

N/A = Not applicable for this type of contract

*Only new deposits/reinvestments can be paused

CONTRACT INFO

Token Name
Reddit DOGE

Symbol
RDoge

Contract Address
0x3c119B26bAcE2fC64A6Cd5636f67DeeAC428d0C6

Network
BSC

Language
Solidity

Deployment Date
Sep 12, 2024

Contract Type
Reflections

Total Supply
420,690,000,000,000

Decimals
18

TAXES

Buy Tax
10%

Sell Tax
10%

*Taxes can be changed in future

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	3
External calls	3
Internal calls	0
Transactions count	3
Last transaction time	2024-09-12 13:38:17 UTC
Deployment Date	2024-09-12 13:32:50 UTC
Create TX	0xdeca8f17a95c855be151241139ee8fb8ccfab3d9e80d94edccb2e9bb32c97e46
Owner	0xd47C8b97C09008E72620488eF65f395Cc1343B6f
Deployer	0xed47c1b659dfa8871040e3b4515662d97dad4f72

TOKEN TRANSFERS STATS

Transfer Count	2
Total Amount	841380000000000 RDoge
Median Transfer Amount	420690000000000 RDoge
Average Transfer Amount	420690000000000 RDoge
First transfer date	2024-09-12
Last transfer date	2024-09-12
Days token transferred	1 Day

FEATURED WALLETS

Owner address	0xd47C8b97C09008E72620488eF65f395Cc1343B6f
Marketing fee receiver	0xBfA7cEAA16484b9915faa4f1445a75Ca19ee4Ab0
LP address	0x76927189b7998314c03A951A46Fc63be2918Ee49 Liquidity is not added yet

TOP 3 UNLOCKED WALLETS

100%	Same as owner Tokens are not distributed yet 0xd47C8b97C09008E72620488eF65f395Cc1343B6f
unavailable	
unavailable	

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: 60%

FOUND THREATS

⚠ High Risk: 0

No high risk-level threats found in this contract.

⚠ Medium Risk: 2

See the next slide for descriptions.

⚠ Low Risk: 0

No low risk-level threats found in this contract.

FOUND THREATS

⚠ Medium Risk: 2

Owner can change contract's auto swap settings.
If swapTokensAtAmount is set to 0 or very low number (fraction of a token) and swapEnabled is set to true, contract will halt on sell.

```
function _transfer(address from, address to, uint256 amount) private {
.....................
bool canSwap = balanceOf(address(this)) >= swapTokensAtAmount;
if (
    !swapping &&
    swapEnabled &&
    canSwap &&
    from != pair &&
    !_isExcludedFromFee[from] &&
    !_isExcludedFromFee[to]
) {
    if (to == pair) swapAndLiquify(swapTokensAtAmount, sellTaxes);
    else swapAndLiquify(swapTokensAtAmount, taxes);
}
.....................
}

function updateSwapEnabled(bool _enabled) external onlyOwner {
    swapEnabled = _enabled;
}

function updateSwapTokensAtAmount(uint256 amount) external onlyOwner {
    require(amount <= 1e7, "Cannot set swap threshold amount higher than 1% of tokens");
    swapTokensAtAmount = amount * 10**_decimals;
}
```

- Recommendation:
  - Ensure that swapTokensAtAmount state variable's value is also higher than 1 token (decimals considered)

FOUND THREATS

⚠ Medium Risk: 2

Owner can change dev, marketing and ops wallets.
If any of those are set to address that cannot receive BNB, contract will halt.
If BNB send value is higher than contract's balance, contract will halt.

```
function updateMarketingWallet(address newWallet) external onlyOwner {
    require(newWallet != address(0),"Fee Address cannot be zero address");
    marketingWallet = newWallet;
}

function updateDevWallet(address newWallet) external onlyOwner {
    require(newWallet != address(0),"Fee Address cannot be zero address");
    devWallet = newWallet;
}

 function updateOpsWallet(address newWallet) external onlyOwner {
        require(newWallet != address(0),"Fee Address cannot be zero address");
        opsWallet = newWallet;
    }

function swapAndLiquify(uint256 contractBalance, Taxes memory temp) private lockTheSwap {
.....................
if (marketingAmt > 0) {
        payable(marketingWallet).sendValue(marketingAmt);
    }

    uint256 devAmt = unitBalance * 2 * temp.dev;
    if (devAmt > 0) {
        payable(devWallet).sendValue(devAmt);
    }

    uint256 opsAmt = unitBalance * 2 * temp.ops;
    if (opsAmt > 0) {
        payable(opsWallet).sendValue(opsAmt);
    }
.....................
}

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

    (bool success, ) = recipient.call{ value: amount }("");
    require(success, "Address: unable to send value, recipient may have reverted");
}
```

- Recommendation:
  - Ensure addresses that receive bnb are always EOA (not a contract or contract that can receive BNB).
    Ensure to use only .call without any require() statements, this way if bnb transfer fails for any reason, tx will succeed with warning instead reverting at whole.

FOUND THREATS

Informational: 3

Owner can withdraw any tokens from the contract, except the native RDoge token.

```
function rescueBNB(uint256 weiAmount) external onlyOwner {
    require(address(this).balance >= weiAmount, "insufficient BNB balance");
    payable(msg.sender).transfer(weiAmount);
}

function rescueAnyBEP20Tokens(address _tokenAddr,address _to, uint256 _amount) public onlyOwner {
    require(_tokenAddr != address(this), "Owner can't claim contract's balance of its own tokens");
    IBEP20(_tokenAddr).transfer(_to, _amount);
}
```

Owner can exclude addresses from fees and reflections.

```
function excludeFromFee(address account) public onlyOwner {
    _isExcludedFromFee[account] = true;
}

function bulkExcludeFee(address[] memory accounts, bool state) external onlyOwner {
    for (uint256 i = 0; i < accounts.length; i++) {
        _isExcludedFromFee[accounts[i]] = state;
    }
}

function excludeFromReward(address account) public onlyOwner {
    require(!_isExcluded[account], "Account is already excluded");
    if (_rOwned[account] > 0) {
        _tOwned[account] = tokenFromReflection(_rOwned[account]);
    }
    _isExcluded[account] = true;
    _excluded.push(account);
}
```

FOUND THREATS

Informational: 3

Owner can change buy/sell taxes up to 10% each.
Combined buy+sell = 20%
When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make.
Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.

```
function setTaxes(
    uint256 _rfi, uint256 _marketing,
    uint256 _ops, uint256 _liquidity, uint256 _dev
) public onlyOwner {
    require((_rfi + _marketing + _ops +_liquidity + _dev ) <= 10, "Must keep fees at 10% or less");
    taxes = Taxes(_rfi, _marketing, _ops, _liquidity, _dev);
    emit FeesChanged();
}

function setSellTaxes(
    uint256 _rfi, uint256 _marketing,
    uint256 _ops, uint256 _liquidity, uint256 _dev
) public onlyOwner {
    require((_rfi + _marketing + _ops + _liquidity + _dev ) <= 10, "Must keep fees at 10% or less");
    sellTaxes = Taxes(_rfi, _marketing, _ops ,_liquidity, _dev);
    emit FeesChanged();
}
```

There is no information about the initial tokens distribution based on the project's whitepaper and/or website.

TOKENOMICS

WEBSITE

Website URL:
https://redditdoge.com/

Domain Registry
https://www.godaddy.com

Domain Expiration
2025-09-10

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

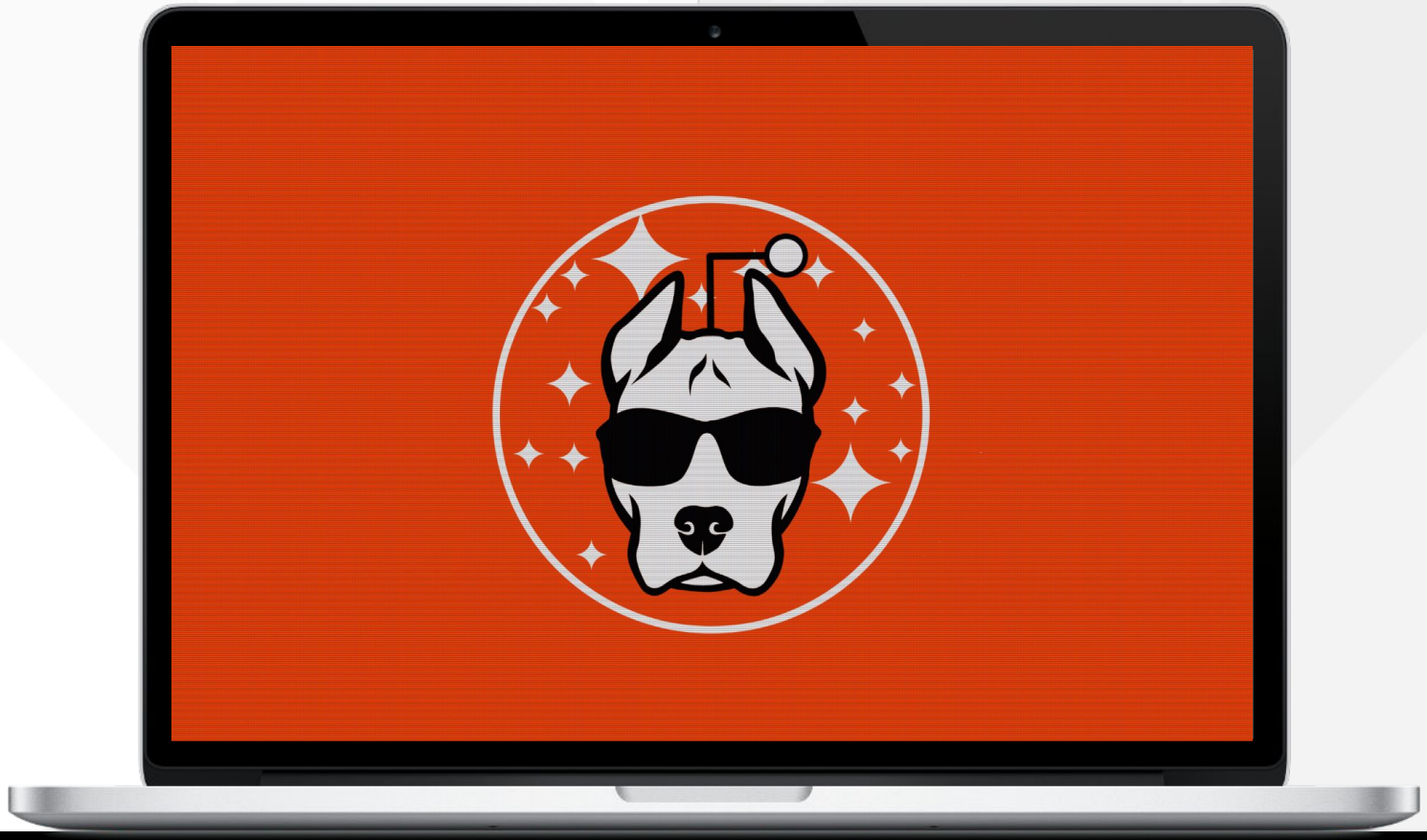
Design
Very nice overall design with appropriate color scheme and graphics.

Content
Website is under development and not finished yet.

Whitepaper
No

Roadmap
No

Mobile-friendly?
Yes



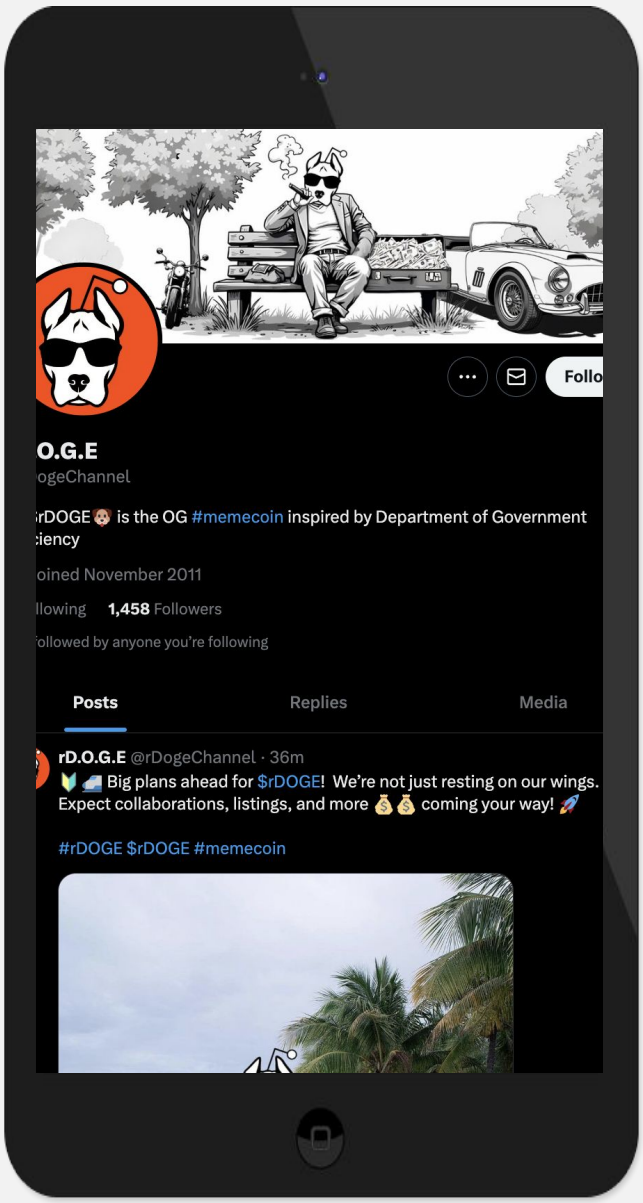
Website Score: 100%

SOCIAL MEDIA

Social Score: 100%

ANALYSIS

Project's social media pages are active



Twitter:

@rDogeChannel

- 1 487 followers
- Active
- Daily posts

Discord

unavailable

Telegram:

@RedditDogChannel

- 815 members
- Active members
- Active mods

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.