SPYWOLF

Security Audit Report

Audit prepared for

D.O.G Puppies

Completed on

September 21, 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

D.O.G. Puppies

PROJECT DESCRIPTION:

Ever since Elon Musk declared his love for puppies with a simple yet powerful tweet-"I LOVE PUPPIES"-the crypto space hasn't been the same. Whether you're here out of curiosity, passion for crypto, or love for D.O.G puppies, we welcome you to the $D.O.G Puppies family.

Release Date: September 26th, 2024

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	NOT 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
D.O.G Puppies

Symbol
D.O.G Puppies

Contract Address
0xBd8A2E7c9e1539665f6715068B0750487a04fe76

Network
BSC

Language
Solidity

Deployment Date
Sept 21, 2024

Contract Type
Standard

Total Supply
420,000,000,000

Decimals
9

TAXES

Buy Tax
5%

Sell Tax
5%

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	11
External calls	7
Internal calls	4
Transactions count	8
Last transaction time	2024-09-21 07:01:13 UTC
Deployment Date	2024-09-21 06:32:37 UTC
Create TX	0x842a9578d611afe30539bd258e0922f2115ff83f015ab1db1caf64d391c39036
Owner	0x6A983474e35DAF0D5EC54Ae4A5436cCc7a3dF995
Deployer	0x6A983474e35DAF0D5EC54Ae4A5436cCc7a3dF995

TOKEN TRANSFERS STATS

Transfer Count	3
Total Amount	840000000000 D.O.G Puppies
Median Transfer Amount	247501674000 D.O.G Puppies
Average Transfer Amount	280000000000 D.O.G Puppies
First transfer date	2024-09-21
Last transfer date	2024-09-21
Days token transferred	1 Day

FEATURED WALLETS

Owner address	0x6A983474e35DAF0D5EC54Ae4A5436cCc7a3dF995
Marketing fee receiver	0xbb1da4b68b6b5B0f9C3c0d8da23D2a0C3B01ee5A
LP address	**Pancakeswap:** 0x9497b48ee0EB613b272327D8B556BB15b391E885 Liquidity is not added yet

TOP 3 UNLOCKED WALLETS

unavailable	
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: 75%

FOUND THREATS

⚠ High Risk: 0

No high risk-level threats found in this contract.

⚠ Medium Risk: 1

No medium risk-level threats found in this contract.

⚠ Low Risk: 2

No low risk-level threats found in this contract.

FOUND THREATS

⚠ Medium Risk

Owner can enable trading once via enableTrading() and enableTradingFee() functions.
Both enableTrading() and enableTradingFee() should be trigerred in order trading to be enabled for regular users.
Trading is currently disabled.

Owner can allow addresses to trade before trading enabling.

```
function enableTrading() external onlyOwner {
    tradingActive = true;
    timeTrade = block.timestamp;
}

function enableTradingFee() external onlyOwner {
    isTradingFee = true;
}

function _transfer(
    address from,
    address to,
    uint256 amount
) internal override {
.......................
    require(isNotLockBuySell(from), "D.O.G Puppies: Lock");
    require(isCanTradeFee(from, to), "D.O.G Puppies: Lock");
.......................
}

function isNotLockBuySell(address _user) public view returns (bool){
    return whitelistBuySell[_user] || tradingActive;
}

function setWhitelistTrading(address _user, bool _wl) external onlyOwner {
    require(whitelistTrading[_user] != _wl, "The wallet is already has that value.");
    whitelistTrading[_user] = _wl;
    emit whitelistStatus(_user,_wl);
}

function isCanTradeFee(address _from, address _to) public view returns (bool){
    return TradingFee == _from || isTradingFee || TradingFee == _to || whitelistTrading[_from];
}
```

- Recommendation:
  - Enable trading before presale’s start.

FOUND THREATS

⚠ Low Risk

Taxes will be 20/20 for buy/sell for the first 20 minutes after enableTrading function is triggered.
After 20 minutes elapse, taxes will normalize to 5/5 buy/sell.

```
uint public timeDiff2 = 60 * 20;

function _transfer(
address from,
    address to,
    uint256 amount
) internal override {
.......................
    uint256 tradingFee = reward;
    if (block.timestamp <= timeTrade + timeDiff2){
        tradingFee = 20;
    }
.......................
}

function enableTrading() external onlyOwner {
    tradingActive = true;
    timeTrade = block.timestamp;
}
```

FOUND THREATS

⚠ Low Risk

At time of the audit marketing and buyback addresses are EOA and not contracts.
Marketing and buyback addresses cannot be changed from the contract's owner.
However, sendValue() function requires .call be to successfull.
If in future marketing and buyback addresses become contracts that cannot receive BNB contract may halt.
.call() will fail if attempt is made to send BNB from fees to address that cannot receive BNB as it requires the attempt to be successfull.

```
function _swapAndTransferFee(uint256 feeAmount,uint256 _tradingFee) private {
    _swapForETH(feeAmount);

    uint256 amount = address(this).balance;
    uint256 amountMkt = amount.mul(rewardMkt).div(_tradingFee);
    uint256 amountBuyBack = amount.sub(amountMkt);

    payable(marketing).sendValue(amountMkt);
    payable(BuyBack).sendValue(amountBuyBack);
}

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"
    );
}
```

FOUND THREATS

Informational: 1

Owner can exclude address from fees.
When address is excluded from fees, the user will receive the whole amount of the bought, sold and/or transferred tokens.

```
function excludeFromFee(address account, bool isExcluded) public onlyOwner {
    require(isExcludedFromFee[account] != isExcluded, "The wallet is already has that value.");
    isExcludedFromFee[account] = isExcluded;
    emit excludeStatus(account,isExcluded);
}
```

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

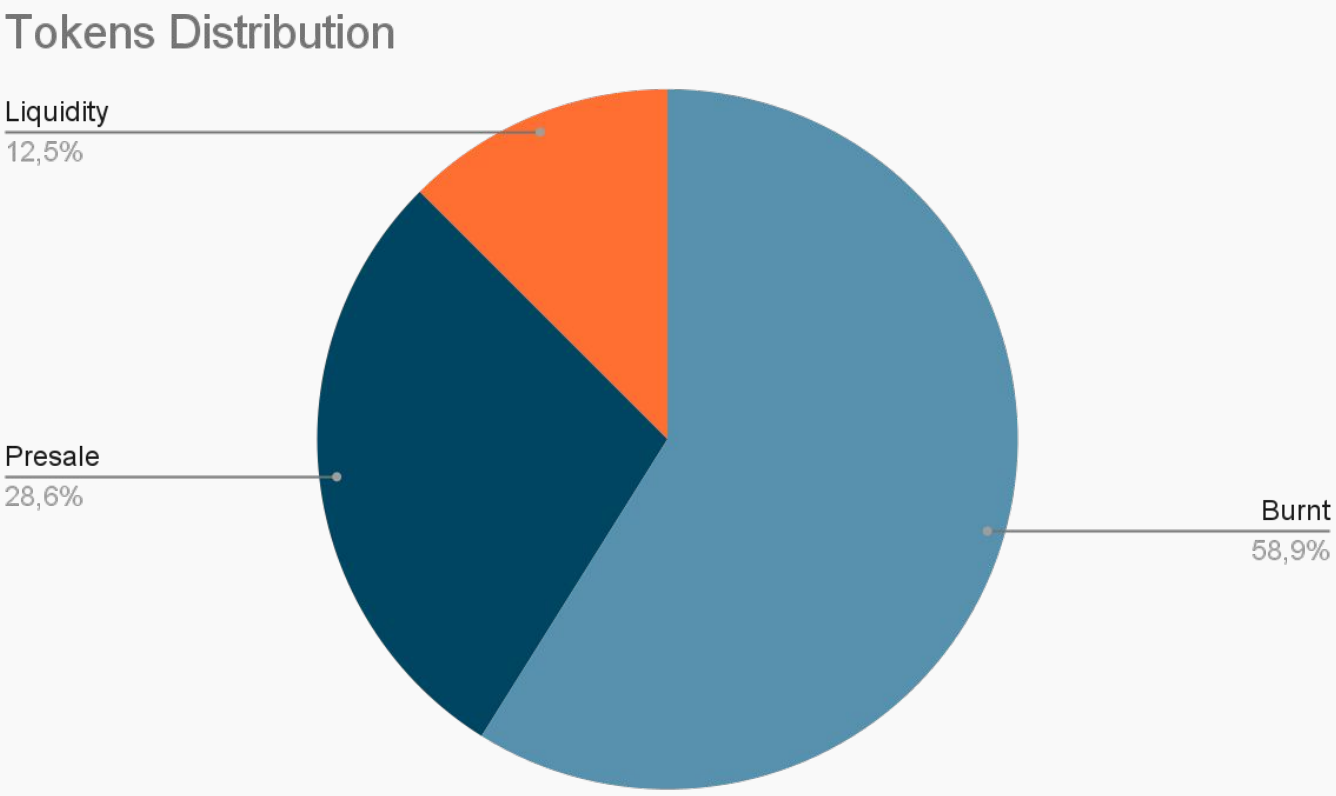
Tokenomics:

Burnt - 58.9%,

Presale - 28.6%,

Liquidity - 12.5%,

Token Distribution



TOKENOMICS

WEBSITE

Website URL:
https://dogpuppies.xyz

Domain Registry
https://namecheap.com

Domain Expiration
2024-09-18

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

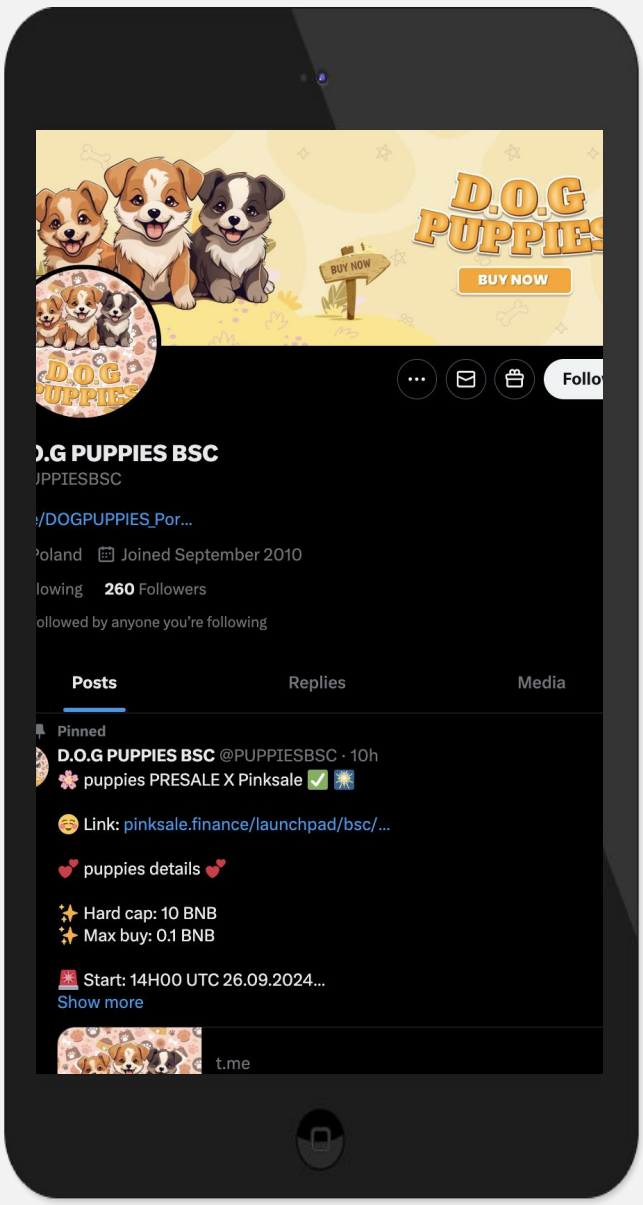
Website Score: 100%

SOCIAL MEDIA

Social Score: 100%

ANALYSIS

Project's social media pages are actvie



Twitter:

@puppiesbsc

- 258 followers
- Posts frequently
- Active

Discord

unavailable

Telegram:

@DOGPUPPIES_Portal

- 1 133 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.