freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Ai Puppy

$PUPPY

10/04/2024

TOKEN OVERVIEW

Fees

• Buy fees: 3.5%

• Sell fees: 3.5%

Fees privileges

• The transferFeeConfigAuthority has been renounced and as a result the fees configuration cannot change

Ownership

• N/A

Minting

• N/A

Max Tx Amount / Max Wallet Amount

• N/A

Blacklist

• N/A

Other privileges

• LP has to be added manually by the team

TABLE OF CONTENTS

DISCLAIMER

The information provided on this analysis document is only
for general information and should not be used as a reason to invest.

FreshCoins Team will take no payment for manipulating the results
of this audit.

The score and the result will stay on this project page information
on our website https://freshcoins.io
FreshCoins Team does not guarantees that a project will not sell off
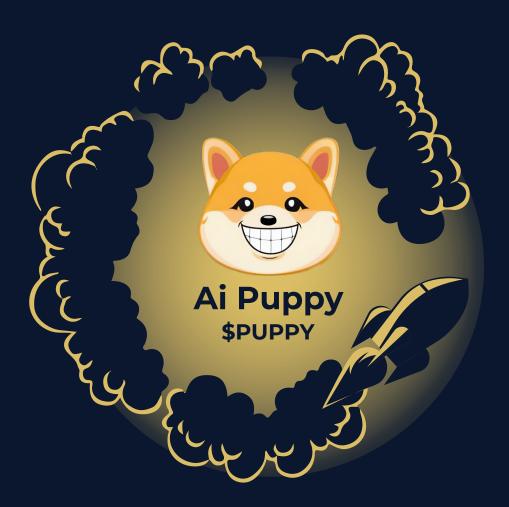team supply, or any other scam strategy (RUG or Honeypot etc)

INTRODUCTION

FreshCoins (Consultant) was contracted by
Ai Puppy (Customer) to conduct a Smart Contract Code Review and Security
Analysis.

6H2UtTiQ9VwwWcGsCZUcUqi5Uus9jYnQVTAiXqGcM1rC

Network: Solana (SOL)

This report presents the findings of the security assessment of
Customer's smart contract and its code review conducted on 10/04/2024

WEBSITE DIAGNOSTIC

https://aipuppy.org/

0-49

50-89

90-100

96
Performance

94
Accessibility

95
Best
Practices

92
SEO

NA
Progressive
Web App

Socials

Twitter

Telegram

https://twitter.com/aipuppyorg

https://t.me/aipuppyorg

AUDIT OVERVIEW

88

Security Score

🚀 **Auditing Request**
07.04.2024

🚀 **Onboarding Process**
07.04.2024

🚀 **Audit Preview**
09.04.2024

🚀 **Audit Release**
10.04.2024

1 High

1 Medium

0 Low

0 Optimizations

0 Informational

TOKEN SUMMARY

Address:	6H2UtTiQ9VwwWcGsCZUcUqi5Uus9jYnQVTAiXqGcM1rC
Name:	Ai Puppy
Symbol:	PUPPY
Decimals:	6
Supply:	100,000,000.00
Platform:	Solana
Contract Name:	PUPPY
Optimization:	Yes
License Type:	Unlicensed
Language:	Rust

PROJECT OVERVIEW

METADATA RESULTS

mint: 6H2UtTiQ9VwwWcGsCZUcUqi5Uus9jYnQVTAiXqGcM1rC

updateAuthority: bLPT1NVhHVosppAsy3r8EBh2H6pSZPb9ST3BZ2j7Won

URI METADATA

Solana URI Metadata pertains to the information linked with a token, which is fetched from its Uniform Resource Identifier (URI)

https://bafkreieixkioqqaoktg25qkn25jtjl3clogwwtphzgop6obbjfa6k4eixa.ipfs.nftstorage.link

```
▼ { 3 items
    mint : "6H2UtTiQ9VwwWcGsCZUcUqi5Uus9jYnQVTAiXqGcM1rC"
    updateAuthority : "bLPT1NVhHVosppAsy3r8EBh2H6pSZPb9ST3BZ2j7Won"
  ▼ data : { 3 items
      name : "Ai Puppy"
      symbol : "PUPPY"
      uri : "https://bafkreieixkioqqaoktg25qkn25jtjl3clogwwtphzgop6obbjfa6k4eixa.ipfs.nftstor ..."
    }
}
```

PROJECT OVERVIEW

METADATA RESULTS

key: This is an integer value that signifies the key linked to the root object

updateAuthority: This is a string value that denotes the update authority for the program

mint: This is a string value that signifies the mint address associated with the program

sellerFeeBasisPoints: This is an integer value that represents the seller fee basis points

primarySaleHappened: This is an integer value that indicates whether the primary sale of the token has occurred

isMutable: This is an integer value that indicates the mutability of the token. A value of 1 suggests that the token is mutable, while a value of 0 indicates that the token is not mutable

editionNonce: This is an integer value that denotes the edition nonce for the token

tokenStandard: This is an integer value that signifies the token standard for the program

PROJECT OVERVIEW

METAPLEX METADATA

Solana metadata encompasses supplementary information linked to a digital asset or NFT on the Solana blockchain. This information comprises details such as the asset's name, description, image, attributes, and other pertinent data

In the Solana context, metadata is usually stored in JSON format and associated with the unique identifier or token ID of assets. This metadata offers crucial information about the asset, enabling users and applications to comprehend and engage with it effectively.

```
▼ { 4 items
    name : "Ai Puppy"
    symbol : "PUPPY"
    description : "aipuppy.org promoting 'absolute fair play' launch on Solana memes"
    image : "https://bafybeiekbewgb3knnpjaiafwya5ukqijgevg6434i6p3p5edtenxru4c6u.ipfs.nftstor ..."
}
```

PROJECT OVERVIEW

EXTENSIONS RESULTS

transferFeeConfigAuthority: null

withdrawWithheldAuthority: bLPT1NVhHVosppAsy3r8EBh2H6pSZPb9ST3BZ2j7Won

updateAuthority: null

In addition to Metaplex Metadata, the token comes with additional features. To be specific, there's a 3.5% transfer fee imposed on the asset, which is calculated based on 350 basis points (transferFeeBasisPoints: 350).
Moreover, there's a maximum fee per transfer set at 100,000,000,000,000.

The authority to configure transfer fees has been revoked, meaning that the fee settings cannot be altered.

```
▼ [ 3 items
  ▼ 0 : { 2 items
    extension : "transferFeeConfig"
    ▼ state : { 5 items
      ▼ newerTransferFee : { 3 items
        epoch : 599
        maximumFee : 100000000000000
        transferFeeBasisPoints : 350
      }
      ▼ olderTransferFee : { 3 items
        epoch : 599
        maximumFee : 100000000000000
        transferFeeBasisPoints : 350
      }
      transferFeeConfigAuthority : NULL
      withdrawWithheldAuthority : "bLPT1NVhHVosppAsy3r8EBh2H6pSZPb9ST3BZ2j7Won"
      withheldAmount : 0
    }
  }
  ▼ 1 : { 2 items
    extension : "metadataPointer"
    ▼ state : { 2 items
      authority : "bLPT1NVhHVosppAsy3r8EBh2H6pSZPb9ST3BZ2j7Won"
      metadataAddress : "6H2UtTiQ9VwwWcGsCZUcUqi5Uus9jYnQVTAiXqGcM1rC"
    }
  }
  ▼ 2 : { 2 items
    extension : "tokenMetadata"
    ▼ state : { 6 items
      ▶ additionalMetadata : [] 0 items
      mint : "6H2UtTiQ9VwwWcGsCZUcUqi5Uus9jYnQVTAiXqGcM1rC"
      name : "Ai Puppy"
      symbol : "PUPPY"
      updateAuthority : NULL
      uri : "https://bafkreieixkioqqaoktg25qkn25jtjl3clogwwtphzgop6obbjfa6k4eixa.ipfs.nftstor ..."
    }
  }
]
```

TECHNICAL FINDINGS

● **Centralization / Privilege**

During the contract deployment, all tokens are allocated to the contract deployer, presenting a potential risk of centralization. This is concerning because the deployer possesses the ability to distribute tokens without seeking consensus from the community

Recommendation

We advise the team to maintain transparency regarding the initial token distribution process

● **transferFeeConfig extension enabled**

The TransferFeeConfig extension is intended to manage fee collection, where a fee is charged for every token transfer. The transferFeeConfigAuthority has been revoked, indicating that the fee setup cannot be modified.

```
transferFeeConfigAuthority: NULL
```

● **LP has to be added manually by the team**

The team utilizing Pinksale Launchpad on the Solana blockchain needs to manually add the liquidity pool (LP)

The project team must manually contribute liquidity to Fluxbeam's liquidity pool in order to utilize it effectively. This involves adding their own assets to the pool, ensuring sufficient liquidity for trading and transactions within the Fluxbeam ecosystem.

Recommendation:

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. The risk can be prevented by temporarily locking the contract or renouncing ownership.

CONCLUSION AND ANALYSIS

Smart Contracts within the scope were manually reviewed and analyzed with static tools.

Audit report overview contains all found security vulnerabilities and other issues in the reviewed code.

Found 1 HIGH issues during the first review.

TOKEN DETAILS

Details

Buy fees:	3.5%
Sell fees:	3.5%
Max TX:	N/A
Max Sell:	N/A

Honeypot Risk

Ownership:	N/A
Blacklist:	Not detected
Modify Max TX:	Not detected
Modify Max Sell:	Not detected
Disable Trading:	Not detected

Rug Pull Risk

Liquidity:	N/A
Holders:	100% unlocked tokens

PUPPY TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

#	Account	Token Account	Quantity	Percentage
1		7JEjNq...6jvxRY	100,000,000.00	100.00%

TECHNICAL DISCLAIMER

Smart contracts are deployed and executed on the blockchain platform. The platform, its programming language, and other software related to the smart contract can have its vulnerabilities that can lead to hacks. The audit can't guarantee the explicit security of the audited project / smart contract.