Pinksale

$PINKSALE | BSC | defi

Contract: 0x602b.....824689

Issues	Found	Fixed
Critical	0	0
Medium	0	0
Minor	0	0
Informational	1	0

9.9/10

AUDIT PASSED



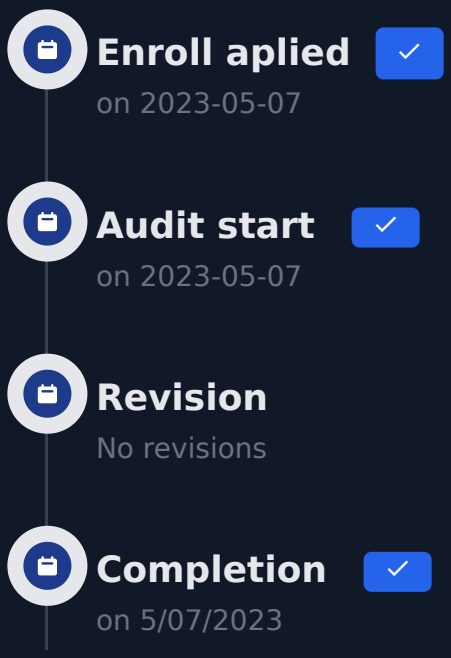
Project Description

PinkSale is a protocol aiming to provide users with the capabilities to launch their own token and create their own initial token sale. No code is required, simply navigate through our terminal and design your own token and token launch with just a few clic

Enroll

PinkSale offers multiple other features to help you with the overall token launch, such as: helping with the listing of your token on PancakeSwap, PinkSwap, UniSwap, ShibaSwap, SushiSwap, KuSwap and QuickSwap with locking your LP and with adding a vesting period for your tokens.

Project details



Language: **Solidity**

Contract address: **0x60...4689**

Owner: **0x00...0000**

SHA-256:
52d...cab

Supply: **100,000**

Decimals: **18**

Deployer: **0x3D...a79A**

Chain: **Binance Smart Chain**

Compiler: **v0.7.6+commit.7338295f**

Optimization: **Yes with 200 runs**

License: **SPDX-License-Identifier: MIT**

Verified: **Yes**

Contract type: **ERC20**

Contract Name: **PinkSaleToken**

Enroll

Deploy date: **07-24-2021**

Overview

Minting

Can't mint new tokens

Blacklist

Can't blacklist - Ownership Renounced

Enable Trading

N/A

Ownership

Ownership is renounced

Honeypot

No

Buy fees

There are no buy fees

Sell fees

There are no sell fees

Proxy

There is no proxy contract

Max tx amount

Can't set maxTx - Ownership Renounced

Trading Cooldown

Can't set cooldown period - Ownership Renounced

Anti Bot

No antibot

Pause

No pause function detected

Hidden Owner

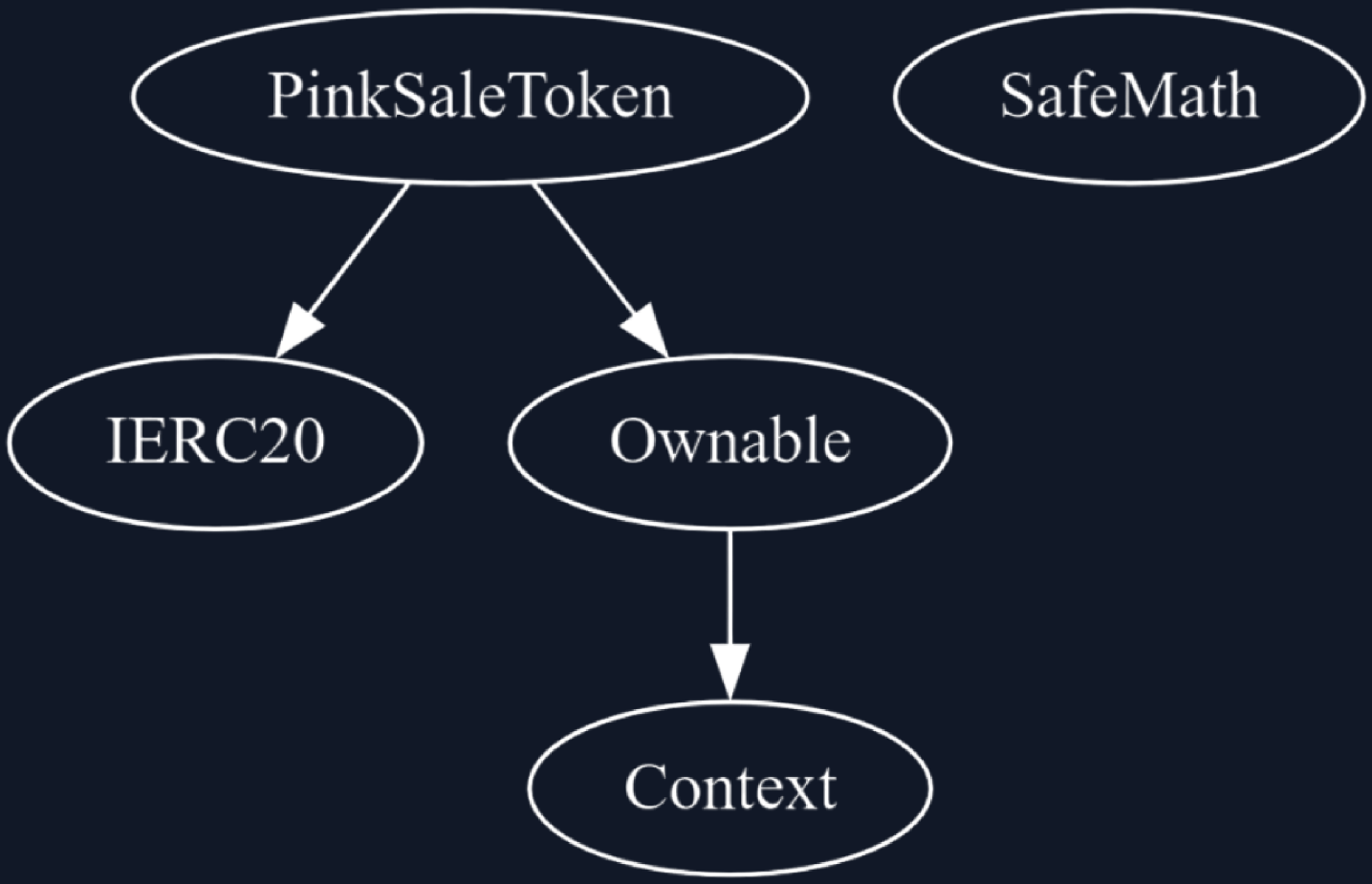
No

Safe

Enroll

- Caution advised
- Be careful
- Extreme caution

Inheritance



Contract details 0x60...4689

Contracts and libraries collapse

Contract	Type	Bases			
└	**Function Name**	**Visibility**	**Mutability**	*	
IERC20	Interface				
SafeMath	Library				
Context	Implementation				
Ownable	Implementation	Context			

Enroll

```
| **PinkSaleToken** | Implementation | Ownable, IERC20 |||
```

Modifiers collapse

```
Contract SafeMath
+----------+-----------+
| Function | Modifiers |
+----------+-----------+
|  tryAdd  |     []    |
|  trySub  |     []    |
|  tryMul  |     []    |
|  tryDiv  |     []    |
|  tryMod  |     []    |
|   add    |     []    |
|   sub    |     []    |
|   mul    |     []    |
|   div    |     []    |
|   mod    |     []    |
|   sub    |     []    |
```

Constructor calls collapse

```
############################
####### PinkSaleToken #######
############################

## Constructor Call Sequence
        - Ownable
        - PinkSaleToken

## Constructor Definitions

### Ownable

    constructor() {
       address msgSender = _msgSender();
       _owner = msgSender;
```

Requires collapse

```
Contract SafeMath
+----------+-------------------------------------------------------------
| Function |                          require or assert
```

Enroll

```
+----------+-------------------------------------------------------------
|  tryAdd  |
|  trySub  |
|  tryMul  |
|  tryDiv  |
|  tryMod  |
|   add    |      require(bool,string)(c >= a,SafeMath: addition overflow)
|   sub    |    require(bool,string)(b <= a,SafeMath: subtraction overflow)
|   mul    | require(bool,string)(c / a == b,SafeMath: multiplication overflo
|   div    |       require(bool,string)(b > 0,SafeMath: division by zero)
|   mod    |        require(bool,string)(b > 0,SafeMath: modulo by zero)
|   sub    |             require(bool,string)(b <= a,errorMessage)
```

Findings

High Severity

No high severity issues found

Medium Severity

No medium severity issues found

Low Severity

No low severity issues found

Informational

Dead Code

Lines: multiple lines

Description: The following functions are not used in the contract, making the code's review more difficult:
_burn() lines(#749-760)
_setupDecimals() lines(#794-796)
div() lines(#248-251)
div() lines(#307-314)
mod() lines(#265-268)
mod() lines(#331-338)
mul() lines(#229-234)
sub() lines(#214-217)
tryAdd() lines(#122-129)
tryDiv() lines(#167-173)
tryMod() lines(#180-186)
tryMul() lines(#149-160)
trySub() lines(#136-142)

Enroll

Possible remediation: Remove unused functions.

SWC Vulnerabilities

36/37 tests passed collapse

Code #	Name	Result	Severity
SWC-100	Function Default Visibility	Passed	n/a
SWC-101	Integer Overflow and Underflow	Passed	n/a
SWC-102	Outdated Compiler Version	Passed	n/a
SWC-103	Floating Pragma	Failed	Informational
SWC-104	Unchecked Call Return Value	Passed	n/a
SWC-105	Unprotected Ether Withdrawal	Passed	n/a
SWC-106	Unprotected SELF-DESTRUCT Instruction	Passed	n/a
SWC-107	Reentrancy	Passed	n/a
SWC-108	State Variable Default Visibility	Passed	n/a
SWC-109	Uninitialized Storage Pointer	Passed	n/a
SWC-110	Assert Violation	Passed	n/a
SWC-111	Use of Deprecated Solidity Functions	Passed	n/a
SWC-112	Delegatecall to Untrusted Callee	Passed	n/a
SWC-113	DoS with Failed Call	Passed	n/a
SWC-114	Transaction Order Dependence	Passed	n/a
SWC-115	Authorization through tx.origin	Passed	n/a
SWC-116	Block values as a proxy for time	Passed	n/a
SWC-117	Signature Malleability	Passed	n/a
SWC-118	Incorrect Constructor Name	Passed	n/a
SWC-119	Shadowing State Variables	Passed	n/a
SWC-120	Weak Sources of Randomness from Chain Attributes	Passed	n/a
SWC-121	Missing Protection against Signature Replay Attacks	Passed	n/a
SWC-122	Lack of Proper Signature Verification	Passed	n/a
SWC-123	Requirement Violation	Passed	n/a
SWC-124	Write to Arbitrary Storage Location	Passed	n/a
SWC-125	Incorrect Inheritance Order	Passed	n/a
SWC-126	Insufficient Gas Griefing	Passed	n/a
SWC-127	Arbitrary Jump with Function Type Variable	Passed	n/a
SWC-128	DoS With Block Gas Limit	Passed	n/a
SWC-129	Typographical Error	Passed	n/a
SWC-130	Right-To-Left-Override control character (U+202E)	Passed	n/a
SWC-131	Presence of unused variables	Passed	n/a
SWC-132	Unexpected Ether balance	Passed	

Enroll

SWC-133	Hash Collisions With Multiple Variable Length Arguments	Passed	n/a
SWC-134	Message call with the hardcoded gas amount	Passed	n/a
SWC-135	Code With No Effects	Passed	n/a
SWC-136	Unencrypted Private Data On-Chain	Passed	n/a

Other findings

Missing events access control

The following functions can modify critical parameters, but have no event emitted, making it difficult to track off-chain changes: function setLockTimeBetweenSwap(uint256 seconds_) external onlyOwner { lockedTimeBetweenSwap = seconds_; } function setPairAddress(address pair_) external onlyOwner { pair = pair_; } function setMaxTxAmount(uint256 maxTxAmount_) external onlyOwner { maxTxAmount = maxTxAmount_; }

- There should be an event emitted for critical parameter changes.

Additional information: link

Holders stats (top 10)

0x3d...a79a		79.21%
0x00...dead	locked	6.33%
0x53...89ec	PancakeV2	4.83%
0xf8...cc84		1.13%
0xe6...836e		0.94%
0x49...89cb		0.80%
0xfd...66ac		0.77%
0x78...0e0c		0.75%
0x46...41a5		0.75%
0x69...30a6		0.68%

KYC & DOXX

Enroll

- **KYC**

No information

- **DOXX**

No information

Website audit https://www.pinksale.finance/

- **Domain Registry**

http://porkbun.com

- **Domain Expiry Date**

2031-05-17

- **Response Code**

200

- **SSL Check and HTTPS test**

Cloudflare, Inc.

- **HTTP2**

Yes, passed

- **Safe Browsing Test**

Yes, passed

Disclaimer

GuardGate is not a financial institution and the information provided on this website does not constitute investment advice, financial advice, trading advice, or any other sort of advice. You should not treat any of the website's content as such. Investing in crypto assets carries a high level of risk and does not hold guarantees for not sustaining financial loss due to their volatility. Accuracy of Information GuardGate will strive to ensure the accuracy of the information listed on this website although it will not hold any responsibility for any missing or wrong information. GuardGate provides all information as is. You understand that you are using any and all information available here at your own risk. Any use or reliance on our content and services is solely at your own risk and discretion. The purpose of the audit is to analyze the on-chain smart contract source

Enroll

code and to provide a basic overview of the project. While we have used all the information available to us for this straightforward investigation, you should not rely on this report only - we recommend proceeding with several independent audits Be aware that smart contracts deployed on a blockchain aren’t secured enough against external vulnerability or a hack. Be aware that active smart contract owner privileges constitute an elevated impact on the smart contract safety and security. Therefore, GuardGate does not guarantee the explicit security of the audited smart contract. The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

© 2023 GuardGate Co. All rights reserved.