



Smart Contract Security Audit Report

PancakeSwap

May 2022

Security Status



www.hacksafe.io



Audit Details



Audited project

PancakeSwap



Deployer address

0x0F9399FC81DaC77908A2Dde54Bb87Ee2D17a3373



Client contacts

PancakeSwap team



Blockchain

Binance smart chain



Website

<https://pancakeswap.finance/>

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the 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 below 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 TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (HackSafe) owe no duty of care towards you or any other person, nor does HackSafe 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 HackSafe 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, HackSafe hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against HackSafe, 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 alone. No applications or operations were reviewed for security. No product code has been reviewed.

Background

HeckSafe was commissioned by PancakeSwap to perform an audit of smart contracts:

- <https://bscscan.com/address/0x0e09fabb73bd3ade0a17ecc321fd13a19e81ce82#code>

Contract Details

Token contract details for 11.05.2022

Contract name	: CakeToken
Contract address	: 0x0E09FaBB73Bd3Ade0a17ECC321fD13a19e81cE82
Total supply	: 747,381,431.751051
Token Ticker	: Cake
Decimals	: 18
Network	: Bscscan
Token Holders	: 1,189,800
Transactions count	: 169,624,079
Contract deployer address	: 0x0F9399FC81DaC77908A2Dde54Bb87Ee2D17a3373
Owner address	: 0x73feaa1eE314F8c655E354234017bE2193C9E24E

PancakeSwap Token Distribution

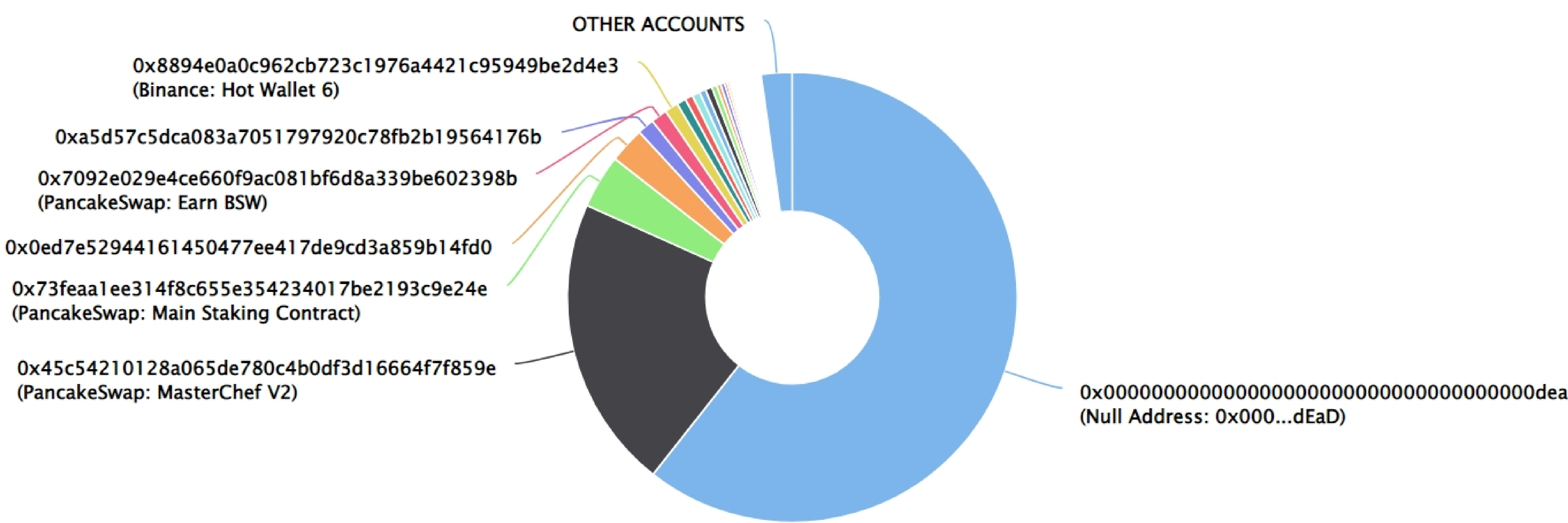
The top 100 holders collectively own 97.78% (730,772,757.77 Tokens) of PancakeSwap Token

Token Total Supply: 747,381,431.75 Token














Total Token Holders: 1,189,896

PancakeSwap Token Top 100 Token Holders

Source: BscScan.com



PancakeSwap Top 20 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Null Address: 0x000...dEaD	453,055,054.030574251783365812	60.6190%
2	 PancakeSwap: MasterChef V2	157,555,410.679752435938448604	21.0810%
3	 PancakeSwap: Main Staking Contract	28,895,280.425572966943469992	3.8662%
4	 0x0ed7e52944161450477ee417de9cd3a859b14fd0	19,048,028.585925903551116852	2.5486%
5	 0xa5d57c5dca083a7051797920c78fb2b19564176b	9,129,169.753230389393328635	1.2215%
6	 PancakeSwap: Earn BSW	8,677,305.502714618252513581	1.1610%
7	Binance: Hot Wallet 6	7,220,123.652759738725657449	0.9661%
8	0xf977814e90da44bfa03b6295a0616a897441acec	5,000,000	0.6690%
9	Binance: Hot Wallet 7	4,180,783.47257720108804869	0.5594%
10	Binance: Hot Wallet 8	4,098,561.079968245896018387	0.5484%
11	 PancakeSwap: Earn RPG	3,536,801.61545737216151761	0.4732%
12	Binance: Hot Wallet 9	3,499,984.680169582257372293	0.4683%
13	 PancakeSwap: Earn GMT	2,700,056.974652092173321319	0.3613%
14	 PancakeSwap: Earn ANKR	2,255,845.350730982763022778	0.3018%
15	 PancakeSwap: Earn CEEK	2,108,448.492215935587277565	0.2821%
16	 0x804678fa97d91b974ec2af3c843270886528a9e6	1,352,574.171008276931322165	0.1810%
17	 PancakeSwap: Earn FROYO	1,350,486.496391870593781299	0.1807%
18	 0xa39af17ce4a8eb807e076805da1e2b8ea7d0755b	1,067,125.128100055110301024	0.1428%
19	0x4fd4266f1434d3929cc9fc12538adb2c318177cc	1,003,730.032265918597521528	0.1343%
20	 Venus: vCAKE Token	941,524.86957179175830238	0.1260%

Contract functions details

+Context

- [Int] constructor
- [Int] _msgSender
- [Int] _msgData

+ Ownable (Context)

- [Int] constructor #
- [Pub] owner #
- [Pub] renounceOwnership#
 - modifiers: onylOwner
- [Pub] transferOwnership#
 - modifiers: onlyOwner
- [Int] _transferOwnership#

+ [Int] IBEP20

- [Ext] totalSupply
- [Ext] decimals
- [Ext] symbol
- [Ext] name
- [Ext] getOwner
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Ext] transferFrom #

+ [Lib] SafeMath

- [Int] add
- [Int] sub
- [Int] sub
- [Int] mul
- [Int] div
- [Int] div
- [Int] mod
- [Int] mod

Contract functions details

+ [Lib] Address

- [Int] isContract
- [Int] sendValue
- [Int] functionCall
- [Int] functionCall
- [Int] functionCallWithValue
- [Int] functionCallWithValue
- [Pvt] _functionCallWithValue

+ BEP20 (Context, IBEP20, Ownable)

- [pub] <constructor> #
- [Ext] getOwner #
- [Pub] name
- [Pub] decimals
- [Pub] symbol
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Pub] mint #
 - modifiers: onlyOwner
- [Int] _transfer #
- [Int] _mint #
- [Int] _burn #
- [Int] _approve
- [Int] _burnFrom

+ CakeToken (BEP20)

- [Pub] mint #
 - modifiers: onlyOwner
- [Ext] delegates
- [Ext] delegate
- [Ext] delegateBySig

Contract functions details

- [Ext] getCurrentVotes
- [Ext] getPriorVotes
- [Int] _delegate
- [Int] _moveDelegates#
- [Int] _writeCheckpoint#
- [Int] safe32
- [Int] getChainId

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Passed
2.	Missing Input Validation	Passed
3.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
4.	Possible delays in data delivery	Passed
5.	Oracle calls.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Passed
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	Private use data leaks.	Passed
13.	Malicious Event log.	Passed
14.	Scoping and Declarations.	Passed
15.	Uninitialized storage pointers.	Passed
16.	Arithmetic accuracy.	Passed
17.	Design Logic.	Passed
18.	Safe Open Zeppelin contracts implementation and usage.	Passed
19.	Incorrect Naming State Variable	Passed

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution.

Security Issues

✔ Critical Severity Issues

No critical severity issue found.

✔ High Severity Issues

No high severity issue found.

✔ Medium Severity Issues

No medium severity issues found.

✔ Low Severity Issues

No low severity issues found.

Owner Privileges

Owner Privileges (in the period when the owner is not renounced) :

- PancakeSwap Contract:
 - Owner can renounce ownership
 - Owner can transfer ownership.
 - Owner can mint tokens

Conclusion

Smart contract contains no severity issues!

HackSafe note: Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.