HackSafe

Smart Contract Security Audit Report

Petverse

June 2022

Security Status

★★★★½

www.hacksafe.io

Audit Details

Audited project
Petverse

Deployer address
TU4whZ4vhTvtKYC2QB13fo95j1e1TA7dkP

Client contacts
Petverse

Blockchain
Tronchain

Website
Not provided

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.

Procedure

Step 1 - In-Depth Manual Review

Manual line-by-line code reviews to ensure the logic behind each function is sound and safe from various attack vectors. This is the most important and lengthy portion of the audit process (as automated tools often cannot find the nuances that lead to exploits such as flash loan attacks).

Step 2 - Automated Testing

Simulation of a variety of interactions with your Smart Contract on a test blockchain leveraging a combination of automated test tools and manual testing to determine if any security vulnerabilities exist.

Step 3 – Leadership Review

The engineers assigned to the audit will schedule meetings with our leadership team to review the contracts, any comments or findings, and ask questions to further apply adversarial thinking to discuss less common attack vectors.

Step 4 - Resolution of Issues

Consulting with the team to provide our recommendations to ensure the code's security and optimize its gas efficiency, if possible. We assist project team's in resolving any outstanding issues or implementing our recommendations.

Step 5 - Published Audit Report

Boiling down results and findings into an easy-to-read report tailored to the project. Our audit reports highlight resolved issues and any risks that exist to the project or its users, along with any remaining suggested remediation measures. Diagrams are included at the end of each report to help users understand the interactions which occur within the project.

Background

HackSafe was commissioned by Petverse Token to perform an audit of smart contracts:

- https://tronscan.org/#/contract/TMS1pqU1T4JewvWjchZDfffj6xJsnsXYe7/code

The purpose of the audit was to achieve the

- Ensutre that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contract Details

Token contract details for 13.06.2022

Token Type	: TRC20
Contract name	: Petverse
Contract address	: TMS1pqU1T4JewvWjchZDfffj6xJsnsXYe7
Compiler version	: Solidity 0.5.17
Total supply	: 100,000.000000
Token Ticker	: PET
Decimals	: 18
Token Holders	: 375
Top 100 token holder's dominance	: 97.06 %
Transactions count	: 3,855
Contract deployer address	: TU4whZ4vhTvtKYC2QB13fo95j1e1TA7dkP
owner address	: TU4whZ4vhTvtKYC2QB13fo95j1e1TA7dkP

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are “Secure”. This token contract does contain owner control, which do not make it fully decentralized as owner have control over smart contract.

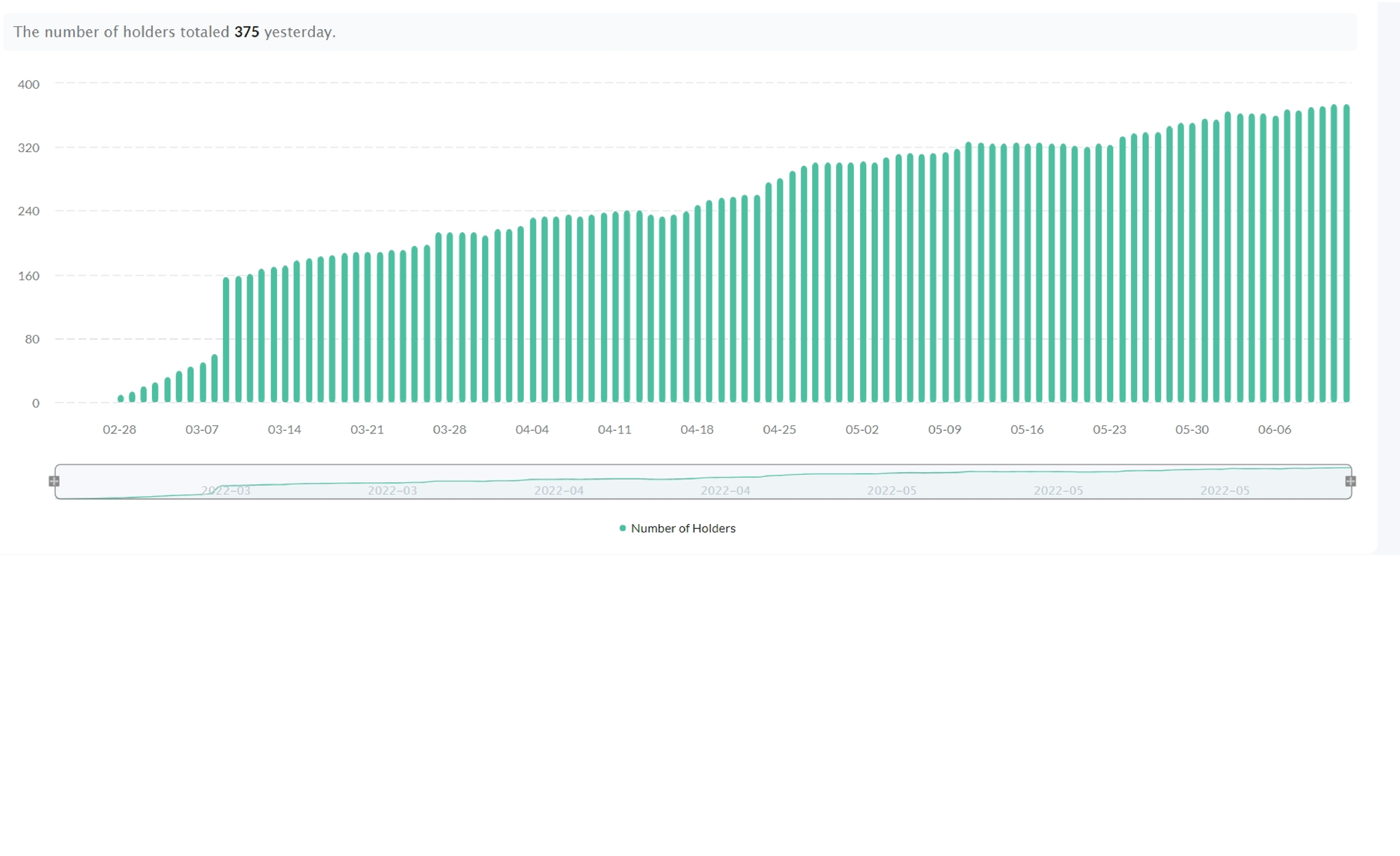
Insecure	Poor secured	Secure	Well-secured

You are here 

We used various tools like Slither, Mythril and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the Audit overview section. General overview is presented in AS-IS section and all identified issues can be found in the Audit overview section.

We found 0 critical, 0 high, 0 medium and 2 low and some very low-level issues. These issues are not critical ones.

Petverse Token Distribution



Petverse Token Distribution

Petverse Token Top 20 Token Holders

Holders' Address

The latest 10,000 records of a total of 374 addresses are shown here.

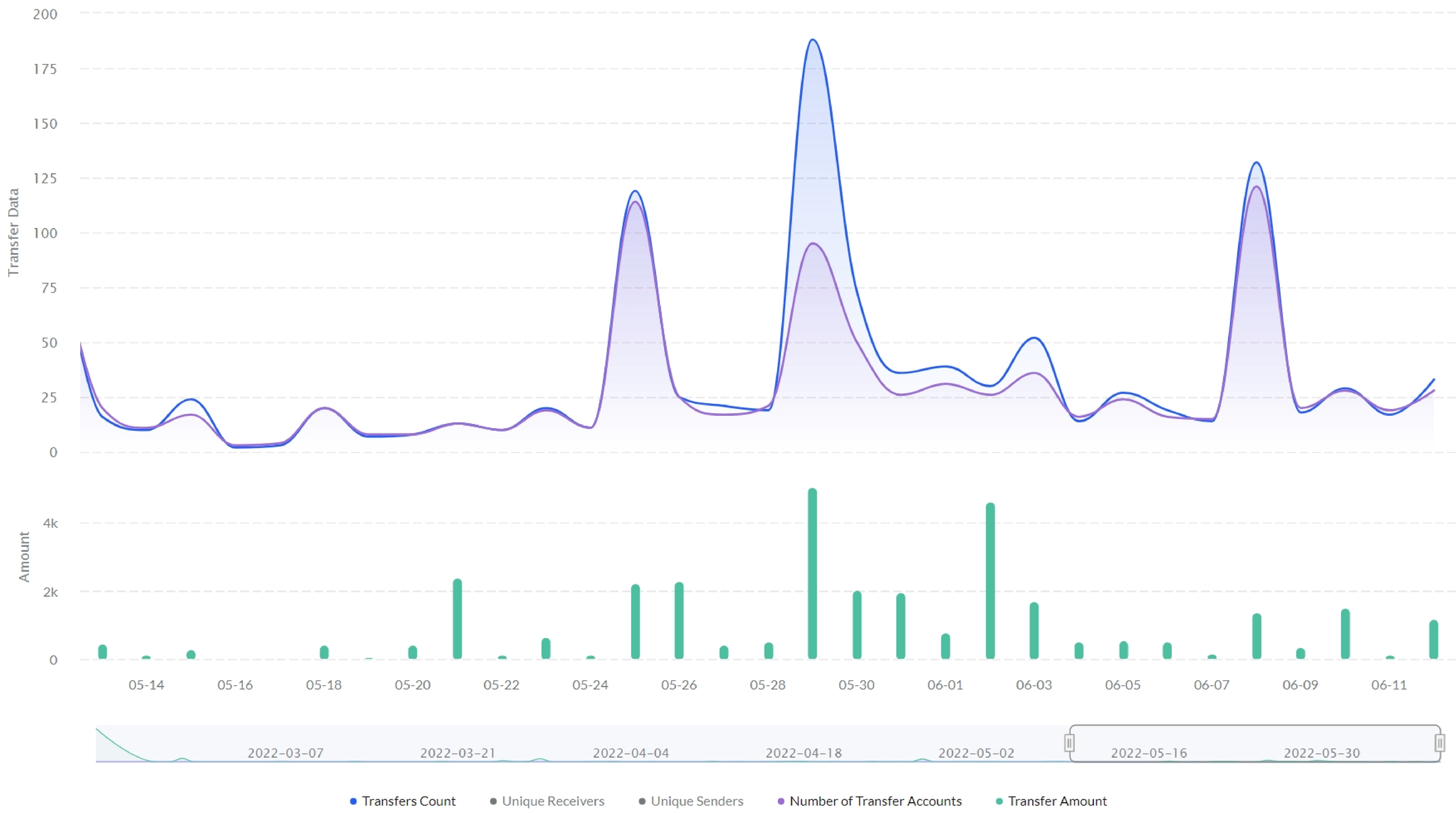
Search Address

Rank	Address	Amount	Value	Percentage
1	TU4whZ4vhTvtKYC2QB13fo95j1e1TA7dkP	66,087.800000000000000000	$1,502,756.95	66.0878%
2	SC TL22WhUUirn3FzpZKvMiUBhh2... okq9g	13,234.677691397420449730	$300,940.63	13.234678%
3	SC TWMJyK5JNVJvZnxQNKWSqnSU...jU5cs	3,666.839814701883973602	$83,379.52	3.66684%
4	SC TJKrJJNCeL3WEU8SJ88Y8sHDye...op1zJ	1,141.859626039637223191	$25,964.51	1.14186%
5	TR5w9uyQweWwzDFAReXAAdVmcB... dWEig	915.578385985531622043	$20,819.15	0.915578%
6	TRNhLMvUoDTip9NKZWFhUdv6yskRcdA5tq	904.785716148863562132	$20,573.74	0.904786%
7	TDfVWqSdBsPyXEk4UNwQTteMnXLrWhSNrq	811.250000000000000000	$18,446.85	0.81125%
8	TD4yPMfRnamoHarDGq5F6JahmwYQrAEFqW	582.379968940992597218	$13,242.62	0.58238%
9	TTXUZcPXPQr9MZnB5ErQgJxjt5XiMeq1m4	476.558795045178614866	$10,836.37	0.476559%
10	TEDP9amx6uNxEbgMN4kvjTqayJ7wCdZPNC	413.672169787570805043	$9,406.41	0.413672%
11	TBqvvAs4wB8M8yda3AxAvQUqpBAK4SKdan	412.103086733296483776	$9,370.73	0.412103%
12	TLmP9yc2NjuxGALinMPMRDMeVGrQFfoAzF	411.865958259816083969	$9,365.34	0.411866%
13	TZE3DU5zh1NUFRcV5dMKD8yikztooND4dy	373.713125302716988893	$8,497.79	0.373713%
14	TCLF6as2HgeJLLb8UBh5LT3DAuLe8PLLNb	307.412417965437769825	$6,990.19	0.307412%
15	TDj46pyRS7xUUx8dUpNowaBAwwFMyS7n77	298.700000000000000000	$6,792.08	0.2987%
16	TGa3UPaMDX663f6mCxPqmEAARHdkq9iggs	295.116252633050500322	$6,710.59	0.295116%
17	TFRibpXtxXi8sXxzPJ8BwMwcVHuHxX8njw	248.751053057547590781	$5,656.3	0.248751%
18	TASiiBCDa6N7rxs7Rc9aoJhAhwVepS58jL	213.700000000000000000	$4,859.28	0.2137%
19	TYJCs2e9mn144CTi1McL7X79NVotF2etcs	188.936114037081987453	$4,296.18	0.188936%
20	TZ9kcMUWjd4L3KGNGU9iuP4jPpTZsFBoar	166.208531140723761501	$3,779.38	0.166209%

Petverse Token Distribution

Petverse Contract overview

The transfer amount totaled **1,174.329** yesterday, with **33** transfers, **14** receivers, **18** senders, and **28** transaction accounts (accounts involved in transactions).



Contract functions details

+ [Int] IBEP20
    -[Ext] totalSupply
    -[Ext] decimals
    -[Ext] symbol
    -[Ext] name
    -[Ext] getOwner
    -[Ext] balanceOf
    -[Ext] transfer
    -[Ext] allowance
    -[Ext] approve
    -[Ext] transferFrom

+ Context
    -[Int] _msgSender
    -[Int] _msgData

+ [Lib] SafeMath
    - [Int] add
    - [Int] sub
    - [Int] sub
    - [Int] mul
    - [Int] div
    - [Int] div
    - [Int] mod
    - [Int] mod

+ Ownable (Context)
    -[Int]< constructor > #
    -[Pub] owner
    -[Pub] renounceOwnership #
      -modifiers: onlyOwner
    -[Pub] transferOwnership #
      -modifiers: onlyOwner
    -[Int] _transferOwnership #

Contract functions details

+Petverse (Context, IBEP20, Ownable)

-[Pub]<constructor> #

-[Ext] getOwner

-[Ext] decimals

-[Ext] symbol

-[Ext] name

-[Ext] totalSupply

-[Ext] balanceOf

-[Ext] transfer #

-[Ext] allowance #

-[Ext] approve #

-[Ext] transferFrom #

-[Pub] increaseAllowance #

-[Pub] decreaseAllowance #

-[Pub] mint #

-modifiers: onlyOwner

-[Pub] burn #

-[Int] _transfer #

-[Int] _mint #

-[Int] _burn #

-[Int] _approve #

-[Int] _burnFrom #

($) = payable function

= non-constant function

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Low issue
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.	Low issue
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

Two low severity issue found.

1. Unlocked Compiler Version.

- **Description**

  The contract utilizes an unlocked compiler version. An unlocked compiler version in the contract's source code permits the user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to differing compiler version numbers. This can lead to ambiguity when debugging as compiler-specific bugs may occur in the codebase that would be difficult to identify over a span of multiple compiler versions rather than a specific one.

- **Recommendation**

  It is advisable that the compiler version is alternatively locked at the lowest version possible so that the contract can be compiled. For example, for version v0.5.16 the contract should contain the following line:

  pragma solidity 0.5.16;

2. Scoping and Declarations.

Unused function.

- **Description**

  The _msgData functions do nothing.
  Library Address does nothing.

- **Location:**

  _msgData functions.

- **Recommendation:**

  We advise to remove unused code which can help you to develop clean coding style and save some computational gas too.

Centralization

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

- Petverse Contract:
    - Owner can transfer ownership.
    - Owner can renounce ownership.
    - Owner can mint new tokens.

This smart contract has some functions which can be executed by the Admin (Owner) only. If the admin wallet private key would be compromised, then it would create trouble. Following are Admin functions:

- Mint : Owner can mint new tokens.
- Transferownership : Owner can transfer ownership.
- Renounceownership : Owner can renounce ownership.

Conclusion

Smart contract contains few severity issues! The further transfer and operations with the fund raised are not related to this particular contract.

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.