



Smart Contract Security Audit Report

ParmaFanToken

March 2023

Security Status



www.hacksafe.io



Audit Details



Audited project

ParmaFanToken



Deployer address

0x304a91c189f020b64b1a39b2bf97063a21fb3af1



Client contacts

ParmaFanToken team



Blockchain

Binance Smart Chain



Website

<https://www.unitos.io/parma-fantoken>

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 ParmaFanToken to perform an audit of smart contracts:

- <https://bscscan.com/address/0xf7f0dc9fd88e436847580d883319137ec2aa6b94#code>

The purpose of the audit was to achieve the following:

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

The information in this report should be understood to 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 03.03.2023

Token Type	: DEFI
Contract name	: ParmaFanToken
Contract address	: 0xf7F0dc9fD88e436847580D883319137Ec2aA6b94
Total supply	: 20,000,000
Token ticker	: PARMA
Decimals	: 18
Token Holders	: 955
Top 100 token holder's dominance	: 99.81 %
Transactions count	: 8,658
Compiler version	: v0.8.10+commit.fc410830
Contract deployer address	: 0x304a91c189f020b64b1a39b2bf97063a21fb3af1
Owner address	: 0xe6736c2d1e1ae51f2b2cbbbbccc1c485b48e1b263

Social profiles

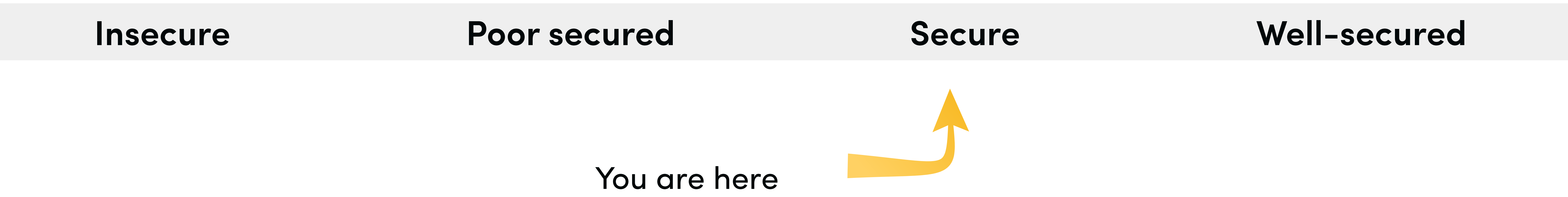
Twitter Profile	: https://twitter.com/unitos_io
Telegram Profile	: https://t.me/parmafantoken_int
Github Profile	: https://github.com/unitos-international-holding/contracts-Parma-FanToken
Medium Profile	: https://unitos.medium.com/
Whitepaper Link	: https://docsend.com/view/x7r2zi6zdb5chtaj
LinkedIn Profile	: https://www.linkedin.com/company/unitos
Coinmarketcap Profile	: https://coinmarketcap.com/currencies/parma-fan-token/
Coingecko Profile	: https://www.coingecko.com/en/coins/parma-calcio-1913-fan-token

Claimed Smart Contract Features

Claimed Feature Detail	Our Observation
<p>Tokenomics :</p> <ul style="list-style-type: none">• Name : ParmaFanToken• Symbol : PARMA• Decimals : 18• Protocol : DEFI• Total supply : 20,000,000• Contract address 0xf7F0dc9fD88e436847580D883319137Ec2aA6b94	<p>YES, this is valid.</p>

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 does have control over smart contract.



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 issues checking status.

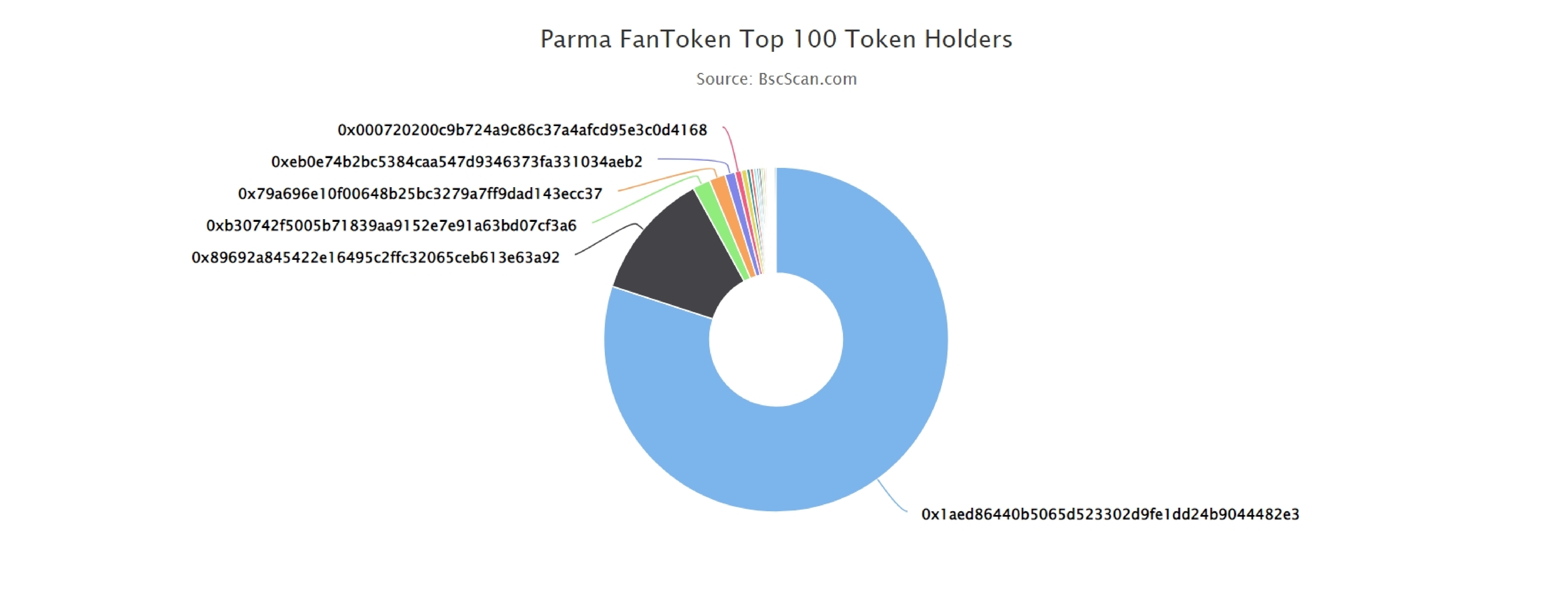
We found 0 critical, 0 high, 1 medium and 0 low and some very low-level issues. These issues are not critical ones.

ParmaFanToken TOKEN Distribution

 The top 100 holders collectively own 99.82% (19,963,602.76 Tokens) of Parma FanToken












Token Total Supply: 20,000,000.00 Token | Total Token Holders: 949



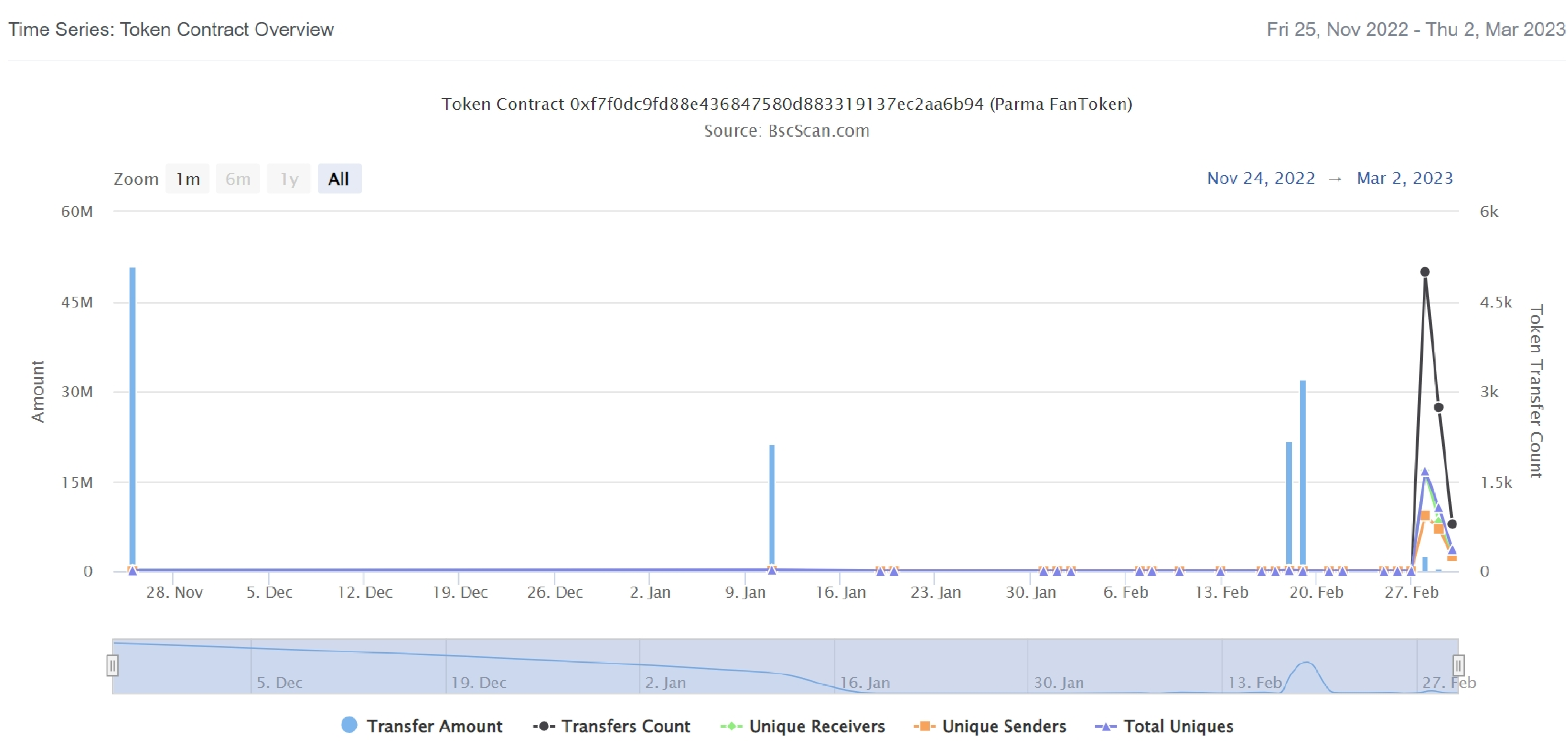
ParmaFanToken Top 20 Token Holders

(A total of 19,963,602.76 tokens held by the top 100 accounts from the total supply of 20,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	 0x1aed86440b5065d523302d9fe1dd24b9044482e3	16,000,000	80.0000%
2	 0x89692a845422e16495c2ffc32065ceb613e63a92	2,406,610	12.0331%
3	0xb30742f5005b71839aa9152e7e91a63bd07cf3a6	333,087	1.6654%
4	 0x79a696e10f00648b25bc3279a7ff9dad143ecc37	300,000	1.5000%
5	 0xeb0e74b2bc5384caa547d9346373fa331034aeb2	193,357.239137543958357807	0.9668%
6	0x000720200c9b724a9c86c37a4afcd95e3c0d4168	116,331.149827858964565472	0.5817%
7	0x481c3f22470a7af27d78790c198876bbd67e0efd	100,718.08163265306122449	0.5036%
8	mexc.com	69,487.6683	0.3474%
9	0xf724a35c71eae68d4df686e95054f7f6ba53136a	60,154.55852734693877551	0.3008%
10	PancakeSwap V2: PARMA 18	52,718.911228713709871582	0.2636%
11	 0x20f1dd414fb78545aa531ced5ec7cb4b950d1699	44,511.047027142009079724	0.2226%
12	 0x436ce2ce8d8d2ccc062f6e92faf410db4d397905	42,865	0.2143%
13	0x58ebef154702add20eb925fe85d7abb750b18d33	40,000	0.2000%
14	 0x7a20bf387c0f4dc4c4e5824c0d6a03b338c9d2e0	39,793.9335	0.1990%
15	 0x389b56da67ebb5342a74e3c48e1cd6ec7c614261	29,881.00434	0.1494%
16	0x898fce2414a1347c0e12bde6b28b75843fd9bbad	22,600	0.1130%
17	 Unitos: PARMA Token	10,000	0.0500%
18	0x1f8d421573156d6dc2d628d40244ca65f63a0ffe	10,000	0.0500%
19	0xb94a7c31946a32b1bb3ae6c2099812d0d023a649	8,633.1	0.0432%
20	0x405f3a35b7a304f79157e6c9206ffb6bb6afd2c2	7,308.527431	0.0365%

ParmaFanToken TOKEN Distribution

ParmaFanToken Contract Overview



Contract functions details

Context.sol

+Context

-[Int] _msgSender

-[Int] _msgData

IERC20Metadata.sol

+ [Int] IERC20Metadata (IERC20)

-[Ext] name

-[Ext] symbol

-[Ext] decimals

IERC20.sol

+ [Int] IERC20

-[Ext] totalSupply

-[Ext] balanceOf

-[Ext] transfer #

-[Ext] allowance

-[Ext] approve #

-[Ext] transferFrom #

Ownable.sol

+Ownable (Context)

-[Pub] <Constructor> #

-[Pub] owner

-[Pub] renounceOwnership #

- modifiers: onlyOwner

-[Pub] transferOwnership #

- modifiers: onlyOwner

-[Prv] _setOwner #

ERC20.sol

+ERC20 (Context, IERC20, IERC20Metadata)

-[Pub] <Constructor> #

-[Pub] name

-[Pub] symbol

-[Pub] decimals

-[Pub] totalSupply

-[Pub] balanceOf

-[Pub] transfer #

-[Pub] allowance

Contract functions details

- [Pub] approve #
- [Pub] transferFrom #
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Int] _transfer #
- [Int] _mint #
- [Int] _burn #
- [Int] _approve #
- [Int] _beforeTokenTransfer #
- [Int] _afterTokenTransfer #

ParmaFanToken.sol

+ParmaFanToken (ERC20, Ownable)

- [Pub] <Constructor> #
 - modifiers: ERC20
- [Ext] addAddressToBlacklist #
 - modifiers: onlyOwner
- [Ext] removeAddressFromBlacklist #
 - modifiers: onlyOwner
- [Pub] isBlacklisted
- [Int] _beforeTokenTransfer #

(\$) = payable function

= non-constant function

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.	Medium issue
19.	Incorrect Naming State Variable	Passed
20.	Too old version	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

One Medium severity issues found.

1.Safe Open Zeppelin contracts implementation and usage.

- **Issue:**

contract ParmaFanToken.sol has direct imported open zeppelin file as any changes in that repository can affect this contract too.

- **Recommendation**

It is advisable to not import any repository direct from any sources.

✔ Low Severity Issues

No Low severity issue found.

Notes:

Blacklisted address can transfer approved tokens using transferFrom() function.

Centralization

Owner Privileges (In the period when the owner is not renounced)

- ParmaFanToken Contract:
 - Owner can add/remove blacklisted addresses.

Conclusion

Smart contract contains medium 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.