



Smart Contract Security Audit Report

Polywolf

October 2022

Security Status



www.hacksafe.io



Audit Details



Audited project

Polywolf



Deployer address

0x9FE5EE3C6d60496063bCdF9859aba446DA18195c



Client contacts

Polywolf Team



Blockchain

Polygon



Website

<https://moonwolf.io/>

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 Polywolf to perform an audit of smart contracts:

- <https://polygonscan.com/address/0xc56d17dd519e5eb43a19c9759b5d5372115220bd#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 07.10.2022

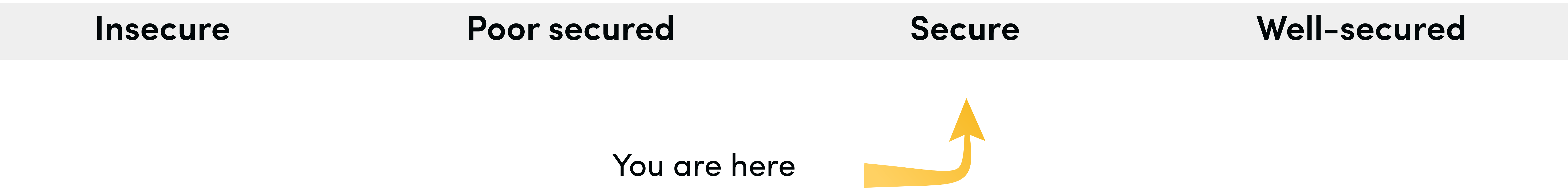
Token Type	: ERC20
Contract name	: Moon
Contract address	: 0xc56d17dD519e5eB43a19C9759b5D5372115220BD
Total supply	: 1,000,170.245158
Token ticker	: MOON
Decimals	: 18
Token holders	: 1,226
Transactions count	: 290,122
Compiler version	: v0.7.4+commit.3f05b770
Contract deployer address	: 0x9FE5EE3C6d60496063bCdF9859aba446DA18195c
Owner address	: 0xb0a8e90ff02d2918ef74c46c2defe7405126239f

Social profiles

Telegram profile	: https://t.me/moonwolf_io
Twitter profile	: https://twitter.com/moonwolf_io
Coingecko profile	: https://www.coingecko.com/en/coins/polywolf/

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 the 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, 0 medium and 1 low and some very low-level issues.

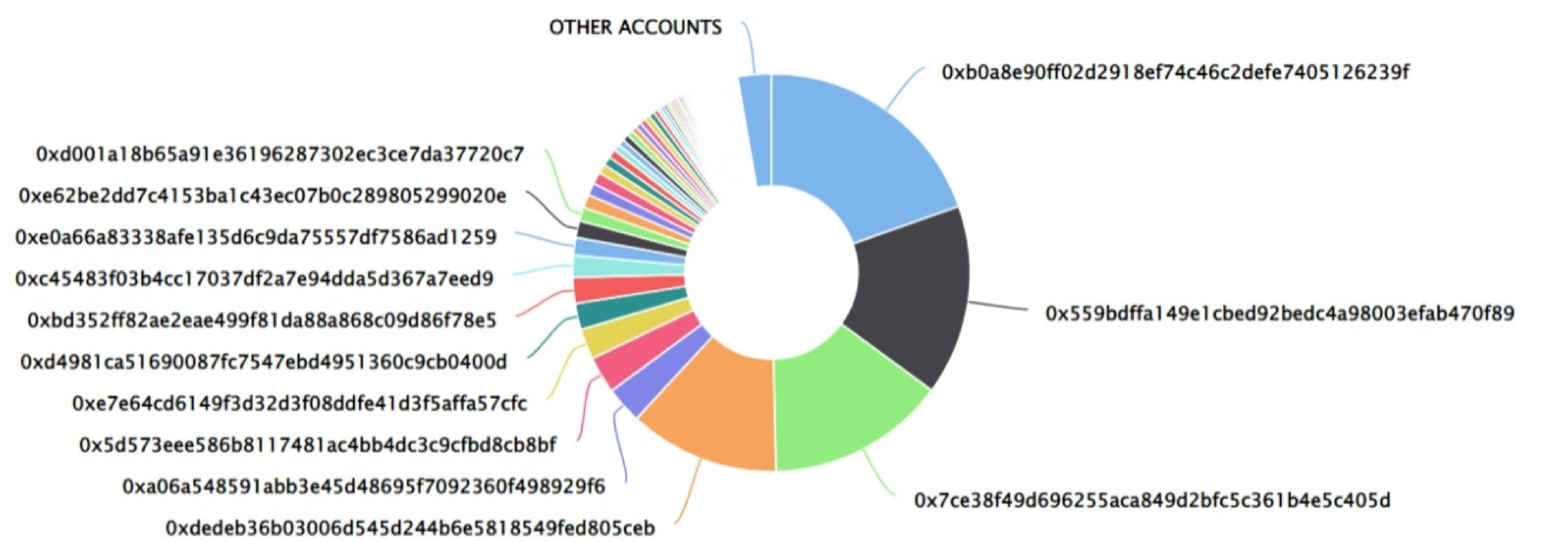
Polywolf Token Distribution

💡 The top 100 holders collectively own 97.27% (972,899.63 Tokens) of Polywolf

💡 Token Total Supply: 1,000,170.25 Token | Total Token Holders: 1,226






Polywolf Top 100 Token Holders

Source: polygonscan.com



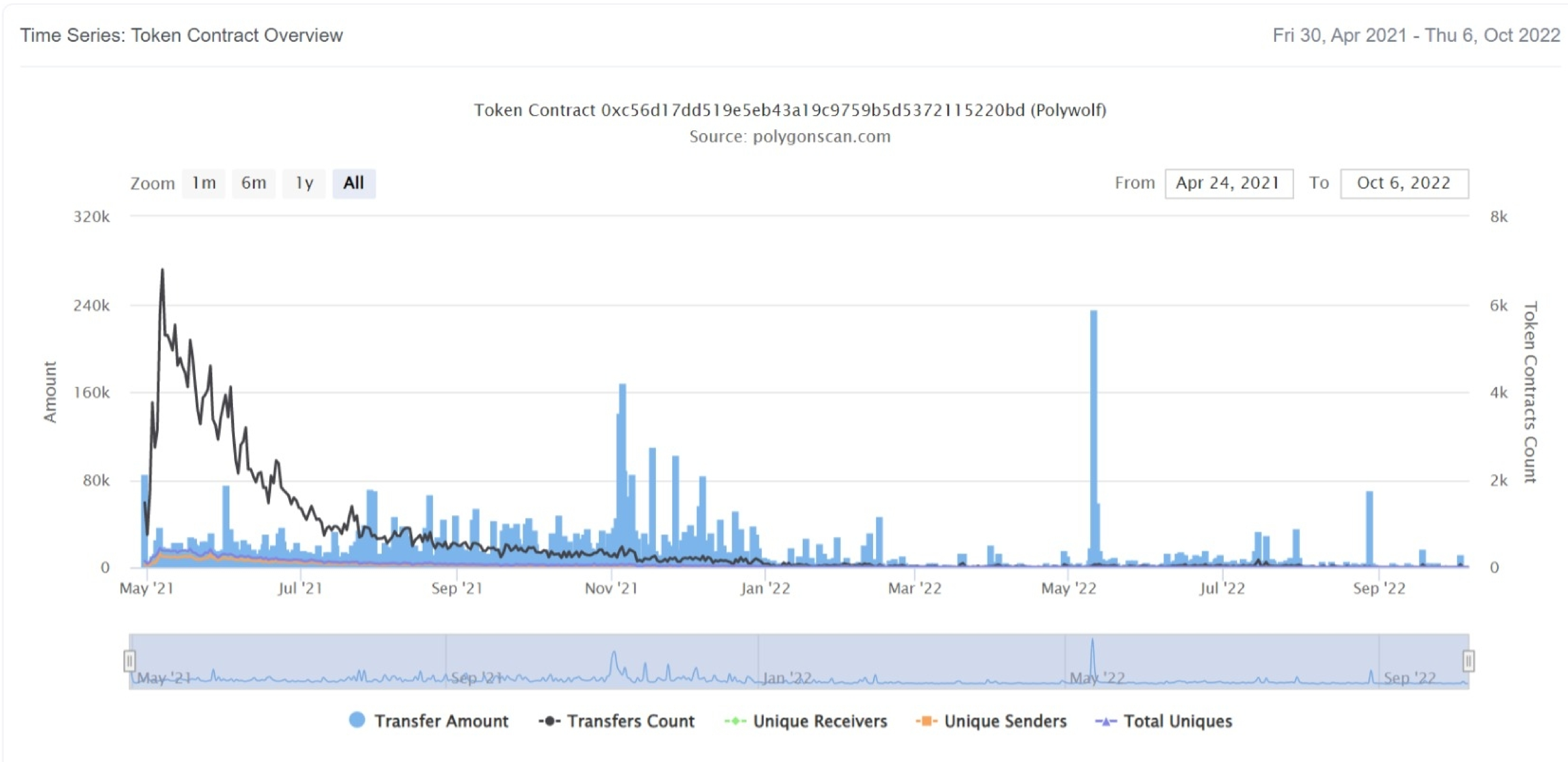
Polywolf Top 20 Token Holders

(A total of 972,899.63 tokens held by the top 100 accounts from the total supply of 1,000,170.25 token)

Rank	Address	Quantity (Token)	Percentage
1	 0xb0a8e90ff02d2918ef74c46c2defe7405126239f	196,060.893762346758407456	19.6028%
2	 0x559bdffa149e1cbcd92bedc4a98003efab470f89	154,720.034432974480577206	15.4694%
3	 0x7ce38f49d696255aca849d2bfc5c361b4e5c405d	145,650.462933563294771296	14.5626%
4	 0xdedeb36b03006d545d244b6e5818549fed805ceb	122,555.243850790336144388	12.2534%
5	0xa06a548591abb3e45d48695f7092360f498929f6	30,039.390190919493835665	3.0034%
6	 0x5d573eee586b8117481ac4bb4dc3c9cfbd8cb8bf	30,031.854306155322027605	3.0027%
7	0xe7e64cd6149f3d32d3f08ddfe41d3f5affa57cfc	25,030.860289950441953247	2.5027%
8	0xd4981ca51690087fc7547ebd4951360c9cb0400d	21,249.1587157587029757	2.1246%
9	0xbd352ff82ae2eae499f81da88a868c09d86f78e5	20,974.934284181681458535	2.0971%
10	0xc45483f03b4cc17037df2a7e94dda5d367a7eed9	17,960.266545658075623917	1.7957%
11	0xe0a66a83338afe135d6c9da75557df7586ad1259	14,421.25	1.4419%
12	0xe62be2dd7c4153ba1c43ec07b0c289805299020e	13,533.499055042835246754	1.3531%
13	0xd001a18b65a91e36196287302ec3ce7da37720c7	11,206.91709619686800851	1.1205%
14	0xf9a7abb40dd35f72cfa77f2e7df5fe43938cf6f7	10,739.268816930951786206	1.0737%
15	0x4aa6907fa9f1bc2be15158897e0138e947c86956	10,000	0.9998%
16	0x35f7731360cf94a47057927c52dd044c9b708ec3	9,817.406534481884431755	0.9816%
17	0x515bf7c9906b0cbca529a3ae5d0bdf0602c6bc23	7,481.787299465007820127	0.7481%
18	0x7b1229b4cc05d28d1ae8eba3d0bdecce674839ea	7,273.480572958010045087	0.7272%
19	0x4b7beda8494a55365e4fb6195b7b4cb03718dd1b	7,000	0.6999%
20	0xe6bbbb32cc886f1a8a608914d01e3fbd0edcfecb	5,396.810982899349393046	0.5396%

Polywolf Token Distribution

Polywolf Contract Overview



Contract functions details

+ Context

- [Int] _msgSender
- [Int] _msgData

+ [Int] IERC20

- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer
- [Ext] allowance
- [Ext] approve
- [Ext] transferFrom

+ [Lib] SafeMath

- [Int] tryAdd
- [Int] trySub
- [Int] tryMul
- [Int] tryDiv
- [Int] tryMod
- [Int] add
- [Int] sub
- [Int] mul
- [Int] div
- [Int] mod
- [Int] sub
- [Int] div
- [Int] mod

+ ERC20 (Context, IERC20)

- [Pub] <constructor>
- [Pub] name
- [Pub] symbol
- [Pub] decimals
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #

Contract functions details

- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Int] _transfer #
- [Int] _mint #
- [Int] _burn #
- [Int] _approve #
- [Int] _setupDecimals #
- [Int] _beforeTokenTransfer

+ Ownable (Context)

- [Int] <constructor>
- [Pub] owner
- [Pub] renounceOwnership #
 - modifiers: onlyOwner
- [Pub] transferOwnership #
 - modifiers: onlyOwner

+Moon (ERC20, Ownable)

- [Pub] mint #
 - modifiers: onlyOwner

(\$) = 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.	Passed
19.	Incorrect Naming State Variable	Passed
20.	Too old version	Low issue

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 issues found.

✔ Medium Severity Issues

No medium severity issue found.

✔ Low Severity Issues

One low severity issue found.

1. Old compiler version

- **Description**

Contract has been deployed using too old solidity version.

- **Recommendation**

It is advisable to deploy contract using any of the latest version of solidity.

Centralization

Owner Privileges :

- Polywolf Contract:
 - Owner can mint tokens.
 - Owner can transfer and renounce 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 as smart contract ownership has not been renounced. Following are Admin functions:

- Mint
- Renounceownership
- Transferownership

Conclusion

Smart contract contains low 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.