



# Cyberscope

## Audit Report

# **PARMY**

November 2023

SHA256      ebe25db0284aa8157641e3e9dda5238b5896fcadce88dfd055958d850a3cb3a3

Audited by   © cyberscope

# Analysis

● Critical   ● Medium   ● Minor / Informative   ● Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	MT	Mints Tokens	Unresolved
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

# Table of Contents

<b>Analysis</b>	<b>1</b>
<b>Table of Contents</b>	<b>2</b>
<b>Review</b>	<b>3</b>
Audit Updates	3
Source Files	3
<b>Findings Breakdown</b>	<b>4</b>
MT - Mints Tokens	5
Description	5
Recommendation	5
<b>Functions Analysis</b>	<b>6</b>
<b>Inheritance Graph</b>	<b>9</b>
<b>Flow Graph</b>	<b>10</b>
<b>Summary</b>	<b>11</b>
<b>Disclaimer</b>	<b>12</b>
<b>About Cyberscope</b>	<b>13</b>

## Review

Testing Deploy	<a href="https://testnet.bscscan.com/address/0xd79dc2febb24de16bb67da552bbcc0a372adb9db">https://testnet.bscscan.com/address/0xd79dc2febb24de16bb67da552bbcc0a372adb9db</a>
----------------	---

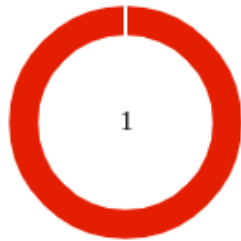
## Audit Updates

Initial Audit	09 Nov 2023
---------------	-------------

## Source Files

Filename	SHA256
contracts/ParmyToken.sol	ebe25db0284aa8157641e3e9dda5238b5896fcadce88dfd055958d850a3cb3a3

## Findings Breakdown



● Critical	1
● Medium	0
● Minor / Informative	0

Severity	Unresolved	Acknowledged	Resolved	Other
● Critical	1	0	0	0
● Medium	0	0	0	0
● Minor / Informative	0	0	0	0

## MT - Mints Tokens

Criticality	Critical
Location	contracts/ParmyToken.sol#L252
Status	Unresolved

### Description

The contract owner has the authority to mint tokens. The owner may take advantage of it by calling the `mint` function. As a result, the contract tokens will be highly inflated.

```
function mint(address to, uint256 amount) public onlyOwner {  
    _mint(to, amount);  
}
```

### Recommendation

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions.

#### Temporary Solutions:

These measurements do not decrease the severity of the finding

- Introduce a time-locker mechanism with a reasonable delay.
- Introduce a multi-signature wallet so that many addresses will confirm the action.
- Introduce a governance model where users will vote about the actions.

#### Permanent Solution:

- Renouncing the ownership, which will eliminate the threats but it is non-reversible.

## Functions Analysis

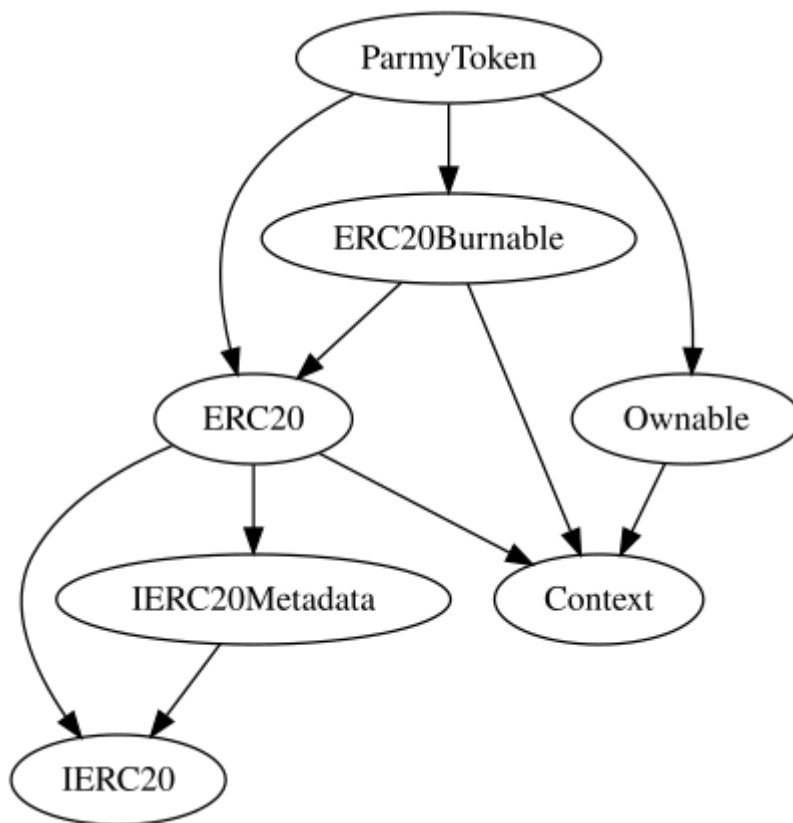
Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
<b>IERC20</b>	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
<b>IERC20Metadata</b>	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
<b>Context</b>	Implementation			
	_msgSender	Internal		
	_msgData	Internal		

<b>ERC20</b>	Implementation	Context, IERC20, IERC20Meta data		
		Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_spendAllowance	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
<b>ERC20Burnable</b>	Implementation	Context, ERC20		

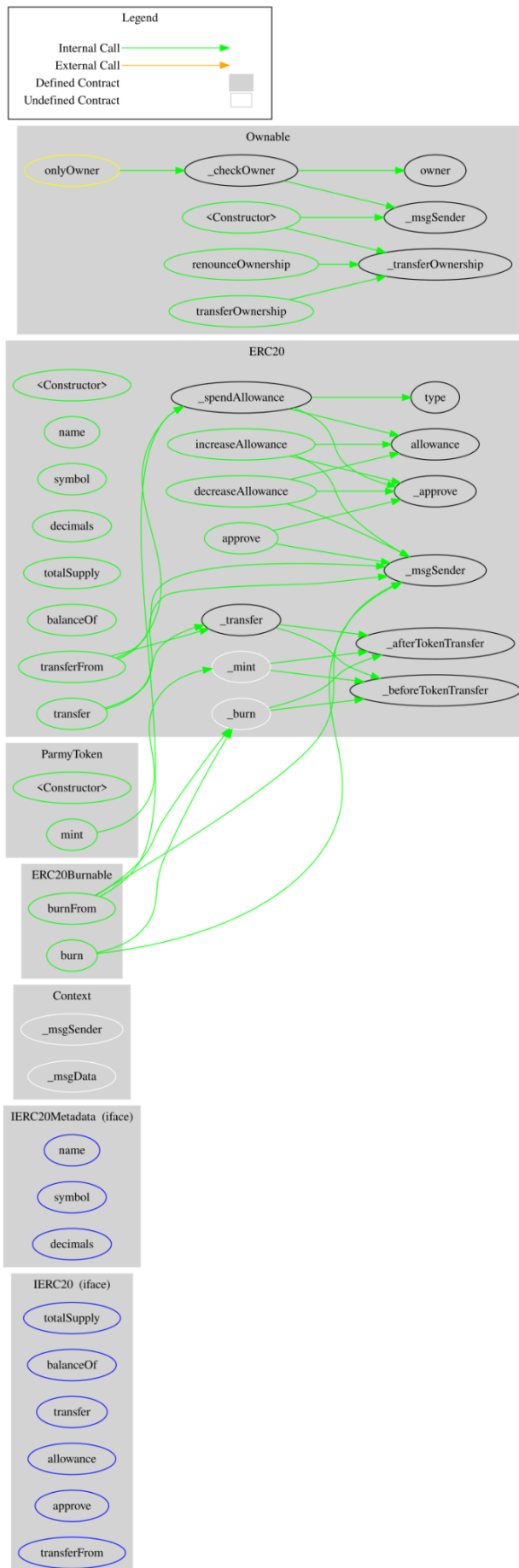


	burn	Public	✓	-
	burnFrom	Public	✓	-
<b>Ownable</b>	Implementation	Context		
		Public	✓	-
	owner	Public		-
	_checkOwner	Internal		
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
<b>ParmyToken</b>	Implementation	ERC20, ERC20Burnable, Ownable		
		Public	✓	ERC20
	mint	Public	✓	onlyOwner

## Inheritance Graph



# Flow Graph



## Summary

PARMY Token contract implements a token mechanism. This audit investigates security issues, business logic concerns and potential improvements. There are some functions that can be abused by the owner like mint tokens. If the contract owner abuses the mint functionality, then the contract will be highly inflated. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats.

## Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. This report is not nor should be considered an "endorsement" or "disapproval" of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security. Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

# About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.



**The Cyberscope team**

<https://www.cyberscope.io>