Cyberscope

Audit Report

Wager

March 2025

Network	ETH
Address	0x14f87ee0b615ab2bac215ce167253c7d724e109c
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	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
●	ROF	Redundant Ownable Functionality	Acknowledged

Table of Contents

Risk Classification

The criticality of findings in Cyberscope's smart contract audits is determined by evaluating multiple variables. The two primary variables are:

1. **Likelihood of Exploitation**: This considers how easily an attack can be executed, including the economic feasibility for an attacker.
2. **Impact of Exploitation**: This assesses the potential consequences of an attack, particularly in terms of the loss of funds or disruption to the contract's functionality.

Based on these variables, findings are categorized into the following severity levels:

1. **Critical**: Indicates a vulnerability that is both highly likely to be exploited and can result in significant fund loss or severe disruption. Immediate action is required to address these issues.
2. **Medium**: Refers to vulnerabilities that are either less likely to be exploited or would have a moderate impact if exploited. These issues should be addressed in due course to ensure overall contract security.
3. **Minor**: Involves vulnerabilities that are unlikely to be exploited and would have a minor impact. These findings should still be considered for resolution to maintain best practices in security.
4. **Informative**: Points out potential improvements or informational notes that do not pose an immediate risk. Addressing these can enhance the overall quality and robustness of the contract.

Severity	Likelihood / Impact of Exploitation
Critical	Highly Likely / High Impact
Medium	Less Likely / High Impact or Highly Likely/ Lower Impact
Minor / Informative	Unlikely / Low to no Impact

Review

Contract Name	WagerToken
Compiler Version	v0.8.16+commit.07a7930e
Optimization	200 runs
Explorer	https://etherscan.io/address/0x14f87ee0b615ab2bac215ce167253c7d724e109c
Address	0x14f87ee0b615ab2bac215ce167253c7d724e109c
Network	ETH
Symbol	$WAGER
Decimals	18
Total Supply	888.000.000

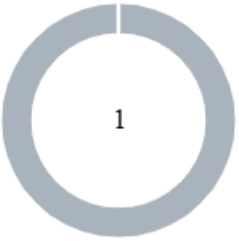
Audit Updates

Initial Audit	12 Feb 2025 https://github.com/cyberscope-io/audits/blob/main/wager/v1/audit.pdf
Corrected Phase 2	18 Feb 2025 https://github.com/cyberscope-io/audits/blob/main/wager/v2/audit.pdf
Corrected Phase 3	28 Mar 2025

Source Files

Filename	SHA256
WagerToken.sol	12e9650ade08c5771a0fe67696cd6ac826f2ce72d60487438d3d3e493e5776a9

Findings Breakdown



Critical	0
Medium	0
Minor / Informative	1

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

ROF - Redundant Ownable Functionality

Criticality	Minor / Informative
Location	WagerToken.sol#L133
Status	Acknowledged

Description

The contract inherits from the `Ownable` contract which is used to provide the address `owner` special privileges. This is done by using the `onlyOwner` modifier which can be added to any function to restrict access for anyone other than the owner. However in the current implementation of `WagerToken` there is no functionality that uses this modifier. Therefore the `Ownable` inheritance is redundant.

```
contract WagerToken is ERC20, Ownable {}
```

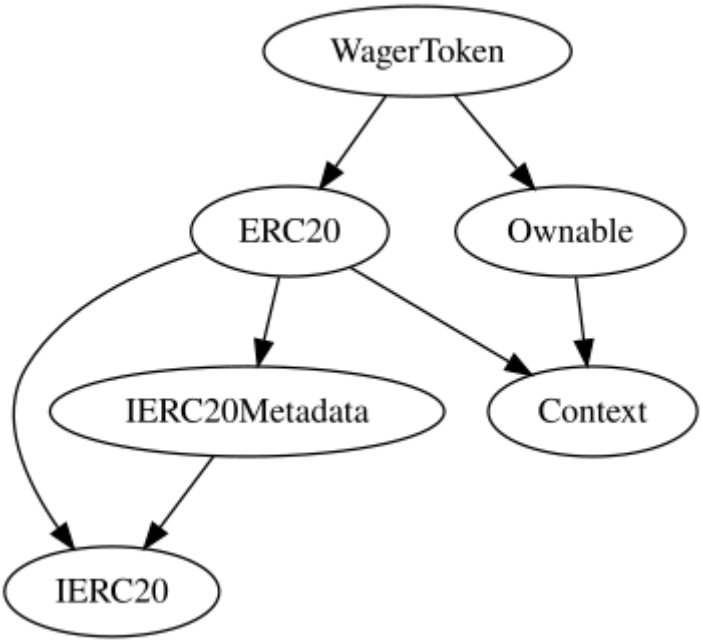
Recommendation

It is recommended to remove redundancies from the contract to enhance code optimization and increase code readability.

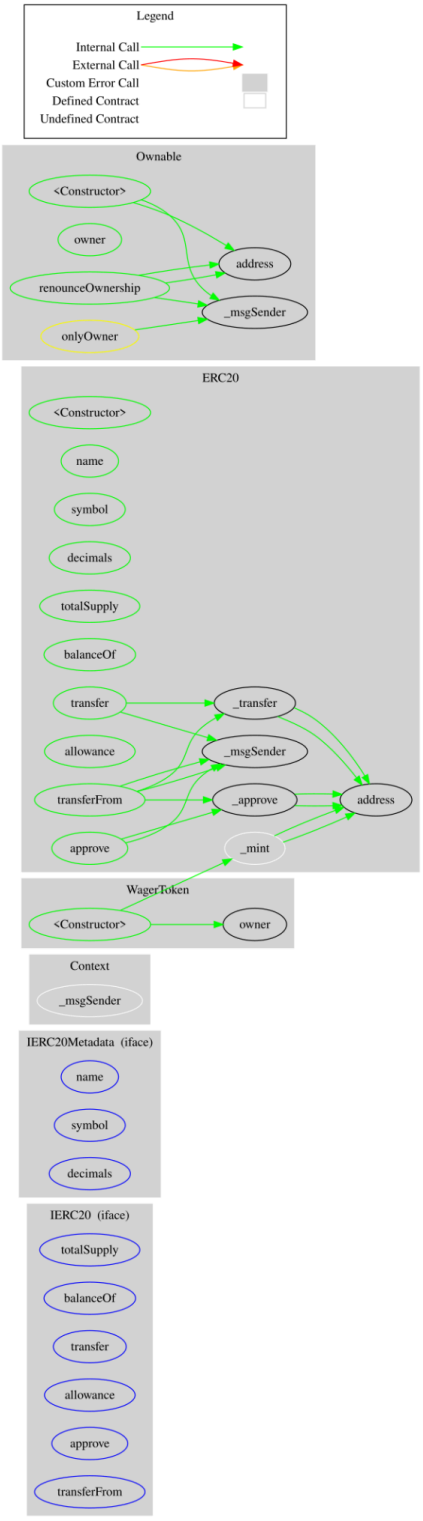
Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
WagerToken	Implementation	ERC20, Ownable		
		Public	✓	ERC20

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Custom Error Call
Defined Contract
Undefined Contract
Ownable
<Constructor>
owner
address
renounceOwnership
_msgSender
onlyOwner
ERC20
<Constructor>
name
symbol
decimals
totalSupply
balanceOf
transfer
_transfer
allowance
_msgSender
transferFrom
_approve
address
approve
_mint
WagerToken
<Constructor>
owner
Context
_msgSender
IERC20Metadata (iface)
name
symbol
decimals
IERC20 (iface)
totalSupply
balanceOf
transfer
allowance
approve
transferFrom

Summary

Wager contract implements a token mechanism. This audit investigates security issues, business logic concerns and potential improvements. Wager is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error or critical issues. The contract Owner can only access the renounce ownership function that can not be used in a malicious way to disturb the users' transactions. The contract does not implement any fees.

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

cyberscope.io