Cyberscope

Audit Report

DoGood Giveaways

November 2024

SHA256 1067a74250288b45689ef8071a404e8dc40a15b9ddc317f62f6c041aeb18946b

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
●	OCTD	Transfers Contract's Tokens	Unresolved
●	MEM	Missing Error Messages	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved
●	L17	Usage of Solidity Assembly	Unresolved

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

Testing Deploy	https://testnet.bscscan.com/address/0x41be52243b86b64a89a1147b29e0e89f6d2f409e
Badge Eligibility	Yes

Audit Updates

Initial Audit	25 Nov 2024 https://github.com/cyberscope-io/audits/blob/main/1-dogood/v1/audit.pdf
Corrected Phase 2	29 Nov 2024

Source Files

Filename	SHA256
DOGOOD.sol	1067a74250288b45689ef8071a404e8dc40a15b9ddc317f62f6c041aeb18946b

Findings Breakdown

Critical	0
Medium	0
Minor / Informative	4

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	0	0	0	0
Medium	0	0	0	0
Minor / Informative	4	0	0	0

OCTD - Transfers Contract's Tokens

Criticality	Minor / Informative
Location	DOGOOD.sol#L222
Status	Unresolved

Description

The `marketingWallet` has the authority to claim all the balance of the contract. The `marketingWallet` may take advantage of it by calling the `manualsend20` function.

```
    function manualsend20(address token) external onlyMarketing {
        IERC20 _token = IERC20(token);
        require(_token.transfer(marketingWallet,
_token.balanceOf(address(this))));
    }
```

Recommendation

The team should carefully manage the private keys of the `marketingWallet'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.

MEM - Missing Error Messages

Criticality	Minor / Informative
Location	DOGOOD.sol#L224
Status	Unresolved

Description

The contract is missing error messages. Specifically, there are no error messages to accurately reflect the problem, making it difficult to identify and fix the issue. As a result, the users will not be able to find the root cause of the error.

```
require(_token.transfer(marketingWallet,
_token.balanceOf(address(this))))
```

Recommendation

The team is suggested to provide a descriptive message to the errors. This message can be used to provide additional context about the error that occurred or to explain why the contract execution was halted. This can be useful for debugging and for providing more information to users that interact with the contract.

L04 - Conformance to Solidity Naming Conventions

Criticality	Minor / Informative
Location	DOGOOD.sol#L56,65,66,67,68,175,188,197,202,209
Status	Unresolved

Description

The Solidity style guide is a set of guidelines for writing clean and consistent Solidity code. Adhering to a style guide can help improve the readability and maintainability of the Solidity code, making it easier for others to understand and work with.

The followings are a few key points from the Solidity style guide:

1. Use camelCase for function and variable names, with the first letter in lowercase (e.g., myVariable, updateCounter).
2. Use PascalCase for contract, struct, and enum names, with the first letter in uppercase (e.g., MyContract, UserStruct, ErrorEnum).
3. Use uppercase for constant variables and enums (e.g., MAX_VALUE, ERROR_CODE).
4. Use indentation to improve readability and structure.
5. Use spaces between operators and after commas.
6. Use comments to explain the purpose and behavior of the code.
7. Keep lines short (around 120 characters) to improve readability.

```
function WETH() external pure returns (address);
uint8 private constant _decimals = 9
uint256 private constant _totalSupply = 100_000_000 * (10 ** _decimals)
string private constant _name = "DoGood Giveaways"
string private constant _symbol = "DOGOOD"
address _lp
bool _enabled
address _wallet
uint256 _thresholdPercent
uint256 _thresholdDivisor
```

Recommendation

By following the Solidity naming convention guidelines, the codebase increased the readability, maintainability, and makes it easier to work with.
Find more information on the Solidity documentation
https://docs.soliditylang.org/en/stable/style-guide.html#naming-conventions.

L17 - Usage of Solidity Assembly

Criticality	Minor / Informative
Location	DOGOOD.sol#L182
Status	Unresolved

Description

Using assembly can be useful for optimizing code, but it can also be error-prone. It's important to carefully test and debug assembly code to ensure that it is correct and does not contain any errors.

Some common types of errors that can occur when using assembly in Solidity include Syntax, Type, Out-of-bounds, Stack, and Revert.

```
assembly {
            size := extcodesize(_addr)
        }
```

Recommendation

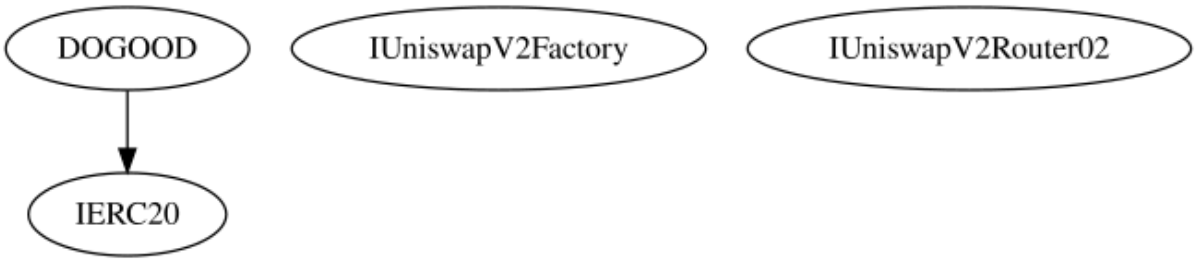
It is recommended to use assembly sparingly and only when necessary, as it can be difficult to read and understand compared to Solidity code.

Functions Analysis

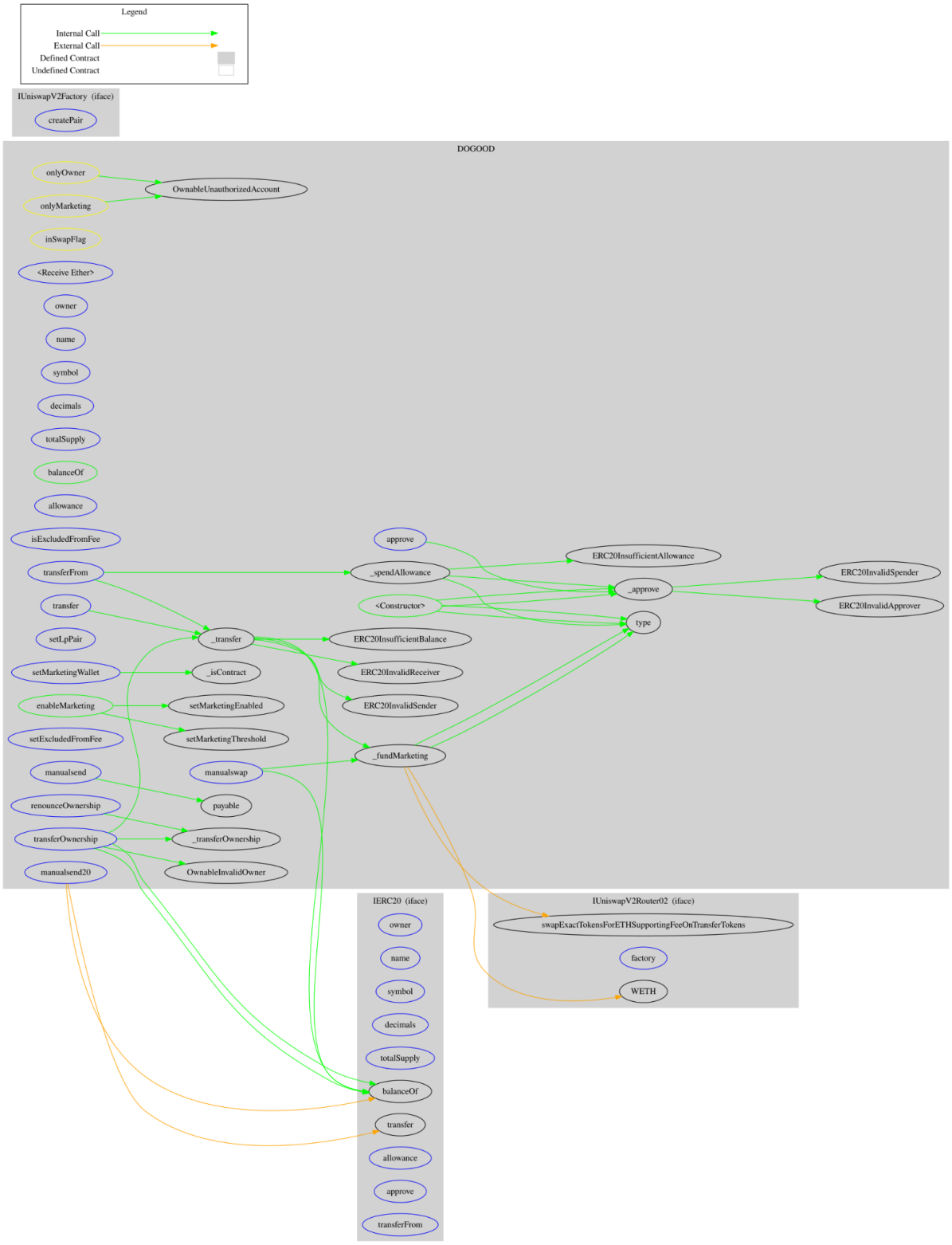
Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
DOGOOD	Implementation	IERC20		
		Public	Payable	-
		External	Payable	-
	owner	External		-
	name	External		-
	symbol	External		-
	decimals	External		-
	totalSupply	External		-
	balanceOf	Public		-
	allowance	External		-
	isExcludedFromFee	External		-
	approve	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	setLpPair	External	✓	onlyOwner
	_isContract	Internal		
	setMarketingWallet	External	✓	onlyOwner
	setMarketingEnabled	Public	✓	onlyOwner
	setMarketingThreshold	Public	✓	onlyOwner

	enableMarketing	Public	✓	onlyOwner
	setExcludedFromFee	External	✓	onlyOwner
	manualsend	External	✓	onlyMarketing
	manualsend20	External	✓	onlyMarketing
	manualswap	External	✓	onlyMarketing
	renounceOwnership	External	✓	onlyOwner
	transferOwnership	External	✓	onlyOwner
	_transferOwnership	Internal	✓	
	_fundMarketing	Internal	✓	inSwapFlag
	_transfer	Internal	✓	
	_approve	Internal	✓	
	_spendAllowance	Internal	✓	

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
IUniswapV2Factory (iface)
createPair
DOGOOD
onlyOwner
onlyMarketing
OwnableUnauthorizedAccount
inSwapFlag
<Receive Ether>
owner
name
symbol
decimals
totalSupply
balanceOf
allowance
isExcludedFromFee
transferFrom
transfer
setLpPair
setMarketingWallet
enableMarketing
setExcludedFromFee
manualsend
renounceOwnership
transferOwnership
manualsend20
_transfer
_isContract
setMarketingEnabled
setMarketingThreshold
manualswap
payable
_transferOwnership
OwnableInvalidOwner
approve
_spendAllowance
<Constructor>
_approve
type
ERC20InsufficientAllowance
ERC20InvalidSpender
ERC20InvalidApprover
ERC20InsufficientBalance
ERC20InvalidReceiver
ERC20InvalidSender
_fundMarketing
IERC20 (iface)
owner
name
symbol
decimals
totalSupply
balanceOf
transfer
allowance
approve
transferFrom
IUniswapV2Router02 (iface)
swapExactTokensForETHSupportingFeeOnTransferTokens
factory
WETH

Summary

DoGood Giveaways contract implements a token mechanism. This audit investigates security issues, business logic concerns and potential improvements. DoGood Giveaways 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 access some admin functions that can not be used in a malicious way to disturb the users' transactions. There is also a limit of max 5% 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