Byte Detective

Smart Contract Audit & Blockchain Development

https://bytedetective.tech

Types of Severities

High

A high severity issue or vulnerability means that your smart contract can be exploited. Issueson this level are critical to the smart contract’s performance or functionality, and we recommend these issues be fixed before moving to a live environment.

Medium

The issues marked as medium severity usually arise because of errors and deficiencies in thesmart contract code. Issues on this level could potentially bring problems, and they should still be fixed.

Low

Low-level severity issues can cause minor impact and or are just warnings that can remainunfixed for now. It would be better to fix these issues at some point in the future.

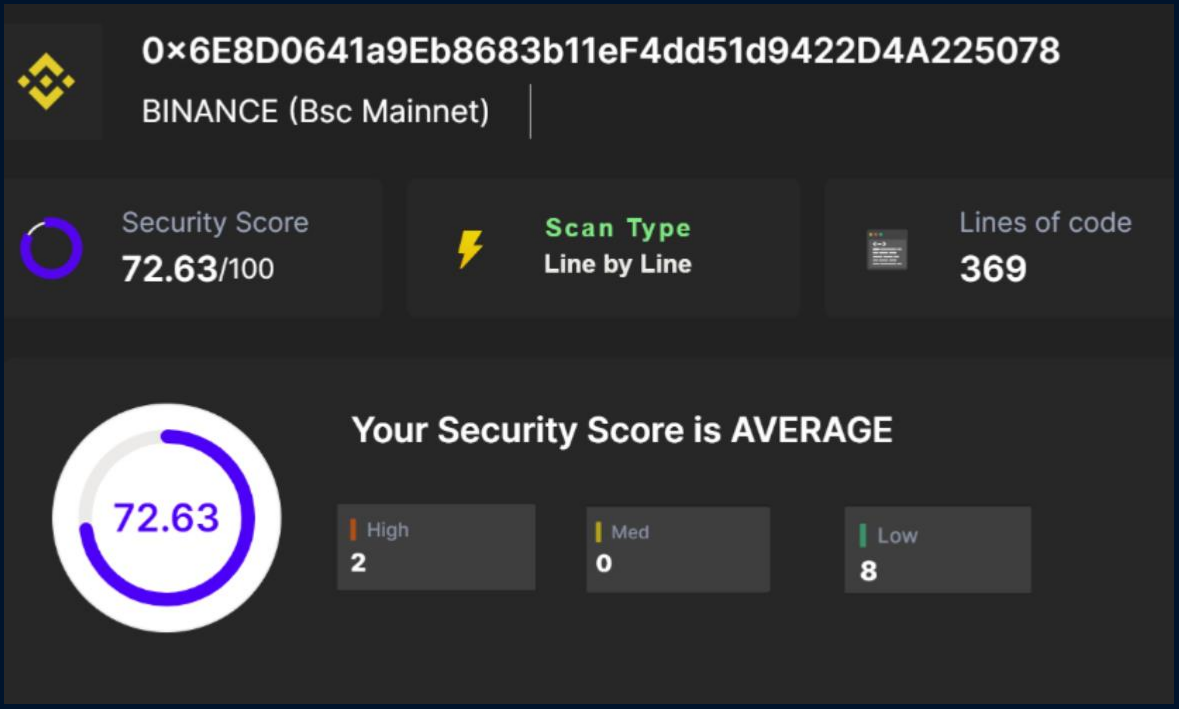
PROJECT NAME: **Flork Metaverse**

OFFICIAL LOGO:

Team Doxed: **No**

WEBSITE: **https://www.florkmetaverse.net/**

Checked Vulnerabilities



0×6E8D0641a9Eb8683b11eF4dd51d9422D4A225078

BINANCE (Bsc Mainnet)

Security Score
72.63/100

Scan Type
Line by Line

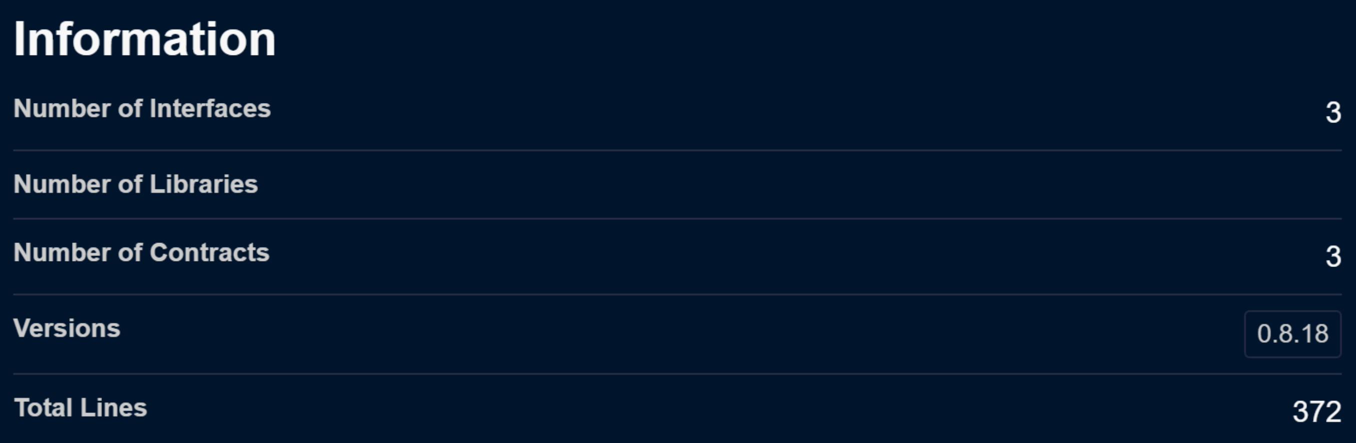
Lines of code
369

72.63

Your Security Score is AVERAGE

High	Med	Low
2	0	8

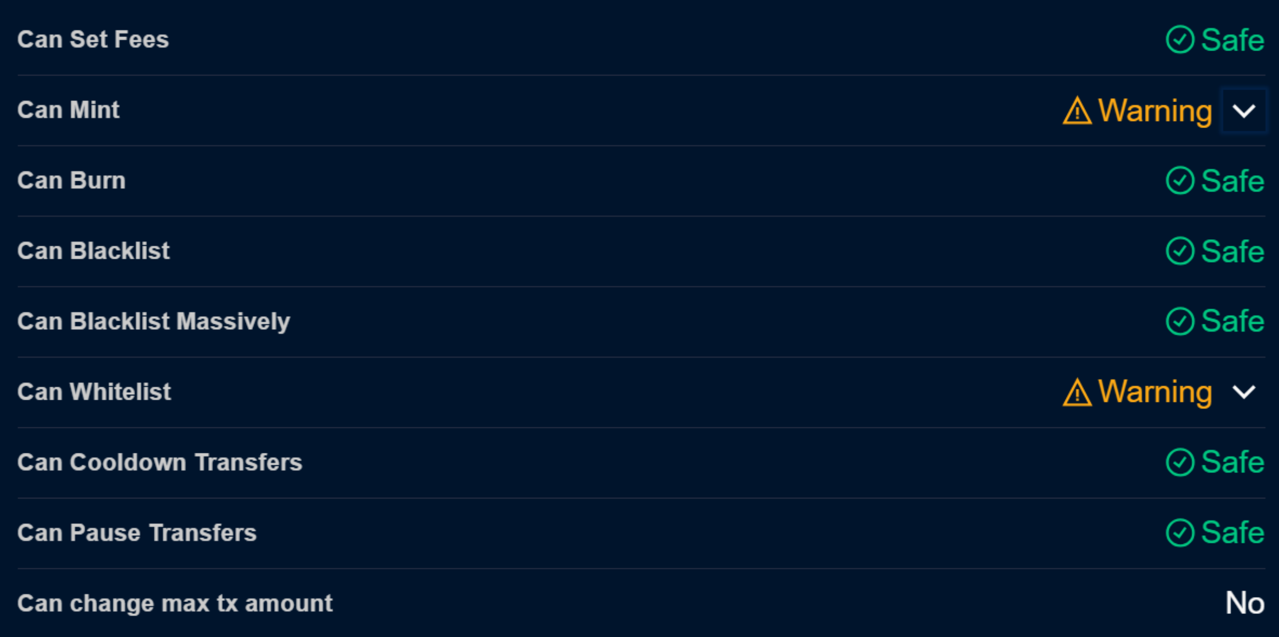
FlorkMetaverseToken.sol



Information

Number of Interfaces	3
Number of Libraries	
Number of Contracts	3
Versions	0.8.18
Total Lines	372

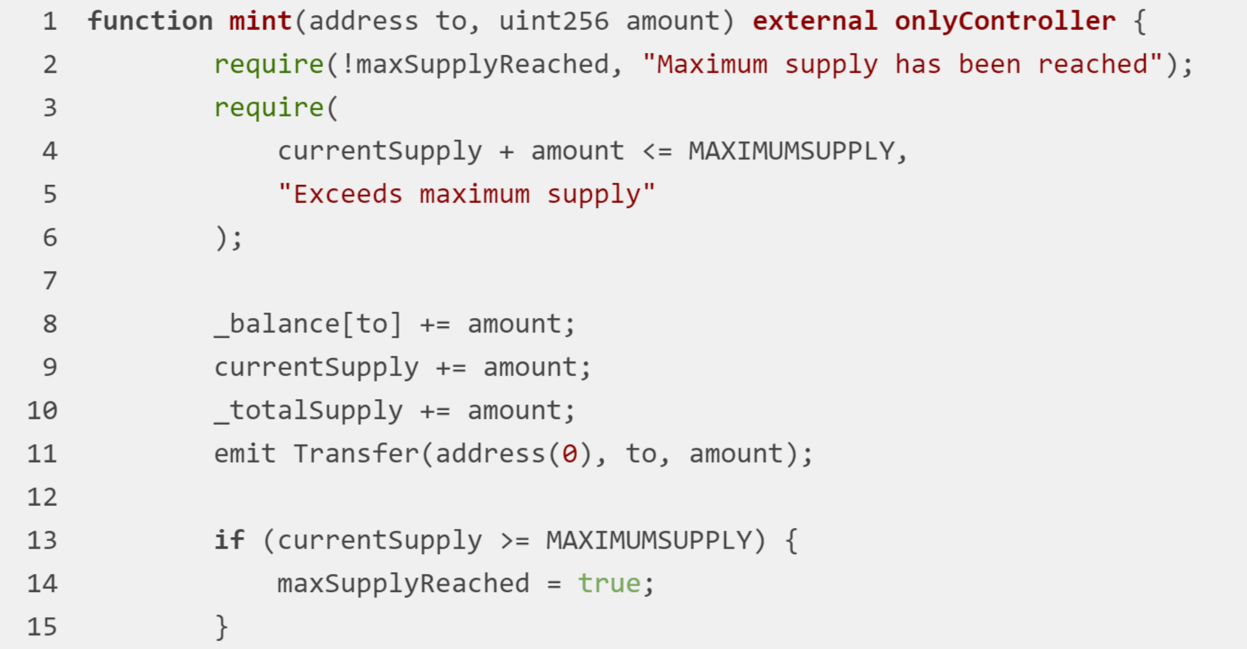
FlorkMetaverseToken.sol



Can Set Fees	✓ Safe
Can Mint	⚠ Warning
Can Burn	✓ Safe
Can Blacklist	✓ Safe
Can Blacklist Massively	✓ Safe
Can Whitelist	⚠ Warning
Can Cooldown Transfers	✓ Safe
Can Pause Transfers	✓ Safe
Can change max tx amount	No

Mint Warning: **The following warning corresponds to the fact that only a portion of the tokens from the total supply is being utilized; this method cannot issue more than 77,777,777,777,777 tokens.**

Circulating tokens: 6,222,222,222,222 FLORK

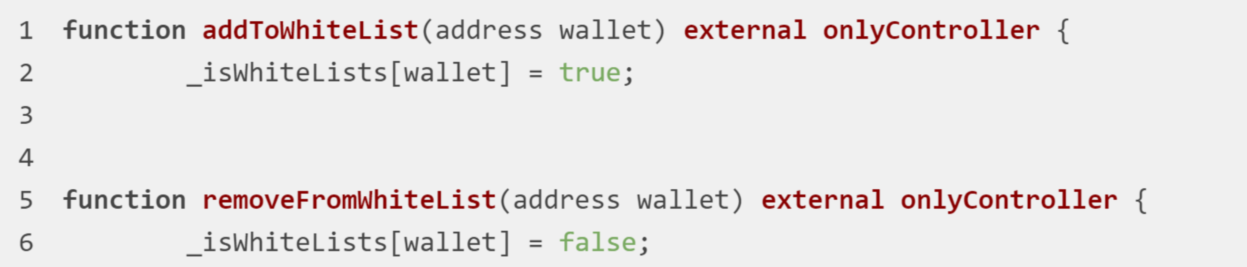


```
function mint(address to, uint256 amount) external onlyController {
        require(!maxSupplyReached, "Maximum supply has been reached");
        require(
            currentSupply + amount <= MAXIMUMSUPPLY,
            "Exceeds maximum supply"
        );

        _balance[to] += amount;
        currentSupply += amount;
        _totalSupply += amount;
        emit Transfer(address(0), to, amount);

        if (currentSupply >= MAXIMUMSUPPLY) {
            maxSupplyReached = true;
        }
```

Whitelist Warning: Option for FLORK Tokens



```
function addToWhiteList(address wallet) external onlyController {
        _isWhiteLists[wallet] = true;


function removeFromWhiteList(address wallet) external onlyController {
        _isWhiteLists[wallet] = false;
```

Please note that the whitelist option for FLORK tokens is currently active. Access to specific functionalities or transactions may be restricted or granted based on whitelist inclusion. Ensure you are on the whitelist to access the full range of features. Contact support for whitelist inquiries or assistance.

SOURCE CODE VERIFIED

The contract’s source code is verified.
Source code verification provides transparency for users interacting with smart contracts. Block explorers validate the compiled code with the one on the blockchain. This also gives users a chance to audit the contracts.

PRESENCE OF MINTING FUNCTION

The contract cannot mint new tokens. The `_mint` functions was not detected in the contracts.
Mint functions are used to create new tokens and transfer them to the user’s/owner’s wallet to whom the tokens are minted. This increases the overall circulation of the tokens.

PRESENCE OF BURN FUNCTION

The tokens can not be burned in this contract.
Burn functions are used to increase the total value of the tokens by decreasing the total supply.

SOLIDITY PRAGMA VERSION

The contract can not be compiled with an older Solidity version.
Pragma versions decide the compiler version with which the contract can be compiled. Having older pragma versions means that the code may be compiled with outdated and vulnerable compiler versions, potentially introducing vulnerabilities and CVEs.

PROXY-BASED UPGRADABLE CONTRACT

This is not an upgradable contract.
Having upgradeable contracts or proxy patterns allows owners to make changes to the contract’s functions, token circulation, and distribution.

OWNERS CANNOT BLACKLIST TOKENS OR USERS

Owners cannot blacklist tokens or users.
If the owner of a contract has permission to blacklist users or tokens, all the transactions related to those entities will be halted immediately.

IS ERC-20 TOKEN

The contract was found to be using ERC-20 token standard.
ERC-20 is the technical standard for fungible tokens that defines a set of properties that makes all the tokens similar in type and value.

PAUSABLE CONTRACTS

This is not a Pausable contract.
If a contract is pausable, it allows privileged users or owners to halt the execution of certain critical functions of the contract in case malicious transactions are found.

CRITICAL ADMINISTRATIVE FUNCTIONS

Critical functions that add, update, or delete owner/admin addresses are not detected
These functions control the ownership of the contract and allow privileged users to add, update, or delete owner or administrative addresses. Owners are usually allowed to control all the critical aspects of the contract.

CONTRACT/TOKEN SELF DESTRUCT

The contract cannot be self-destructed by owners.
`selfdestruct()` is a special function in Solidity that destroys the contract and transfers all the remaining funds to the address specified during the call. This is usually access-control protected.

HARDCODED ADDRESSES

The contract was hardcoding addresses in the code. This may represent that those parameters can never be changed or updated unless it’s a proxy contract. It is recommended to go through the code to know more about these hardcoded values and its use.

OWNERS UPDATING TOKEN BALANCE

The contract does not have any owner-controlled functions modifying token balances for users or the contract

OWNER WALLET TOKEN SUPPLY

The Owner’s wallet contains 6222222222222.0 tokens which is more than 5% of the circulating token supply

FUNCTION RETRIEVING OWNERSHIP

No such functions were found
If this function exists, it is possible for the project owner to regain ownership even after relinquishing it.

ERC20 RACE CONDITION

The contract is vulnerable to ERC-20 approve Race condition vulnerability.
ERC-20 approve function is vulnerable to a frontrunning attack which can be exploited by the token receiver to withdraw more tokens than the allowance. Proper mitigation steps should be implemented to prevent such vulnerabilities.

RENOUNCED OWNERSHIP

The contract's owner was not found.
Renounced ownership shows that the contract is truly decentralized and once deployed, it can’t be manipulated by administrators.

Project Website Analysis Data

History

Final URL

https://www.florkmetaverse.net/

Serving IP Address

67.223.118.29

Status Code

200

Body Length

37.03 KB

Body SHA-256

a2798c082ea89e290ce8330773fa53a46708af164aadb62df4ec97b596bd6267

last-modified

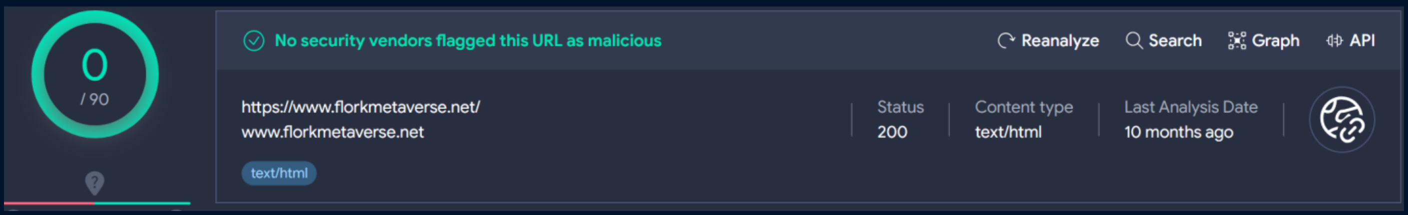
Tue, 16 Aug 2022 18:28:20 GMT

x-turbo-charged-by

Official Page of the Flork metaverse, Flork Coin Mining, NTFs and multiple ways to multiply your investment.

Outgoing links

- https://t.me/FlorkMetaverseChannel
- https://t.me/FlorkMetaverseGroup
- https://www.facebook.com/FlorkCoin-104985765642184/
- https://twitter.com/CoinFlork



No security vendors flagged this URL as malicious

https://www.florkmetaverse.net/
www.florkmetaverse.net

Status 200

Content type text/html

Last Analysis Date 10 months ago

text/html

VERIFIED BY BYTE DETECTIVE

★ ENTEGRITY ★ TRUST ★

THANK YOU!

11/23/2023