CYSRO

Cyber Security

SMART CONTRACT SECURITY AUDIT

MEMELOTTERY

Table of Contents

Project Summary

Project name	MEMELOTTERY
Platform	Ethereum
Language	Solidity
Contract address	https://bscscan.com/address/0x94Ad2D084f9e77DD394815cC32aA7D7C09420aF1#readContract
Repository	NA
Contract owner address	0x2DCBD1742BDE8815c211Ea82FB0d642D5eEA0D5A
Deployers contract address	0x2DCBD1742BDE8815c211Ea82FB0d642D5eEA0D5A
Decimal	9
Total supply	1000000000000000000000
Website	NA
Social media	NA
Audit methodology	Whitebox Testing
Delivery Date	July 10, 2021

Introduction

Given the opportunity to review MEMELOTTERY Project’s smart contract source code, we in the report outline our systematic approach to evaluate potential security issues in the smart contract implementation, expose possible semantic inconsistencies between smart contract code and design document, and provide additional suggestions or recommendations for improvement. Our results show that the given version of smart contracts is ready to launch after resolving the mentioned issues, there are no critical or high issues found related to business logic, security or performance.

Scope of work

The files that needed to be evaluated for the security assessment were given to us by the Team. The files listed below were used for this audit. Other files and contracts that are not listed here are not audited by us hence we will not be responsible for any security issues caused by those contracts.

	File	Checksum
1	0x94Ad2D084f9e77DD394815cC32aA7D7C09420aF1	NA

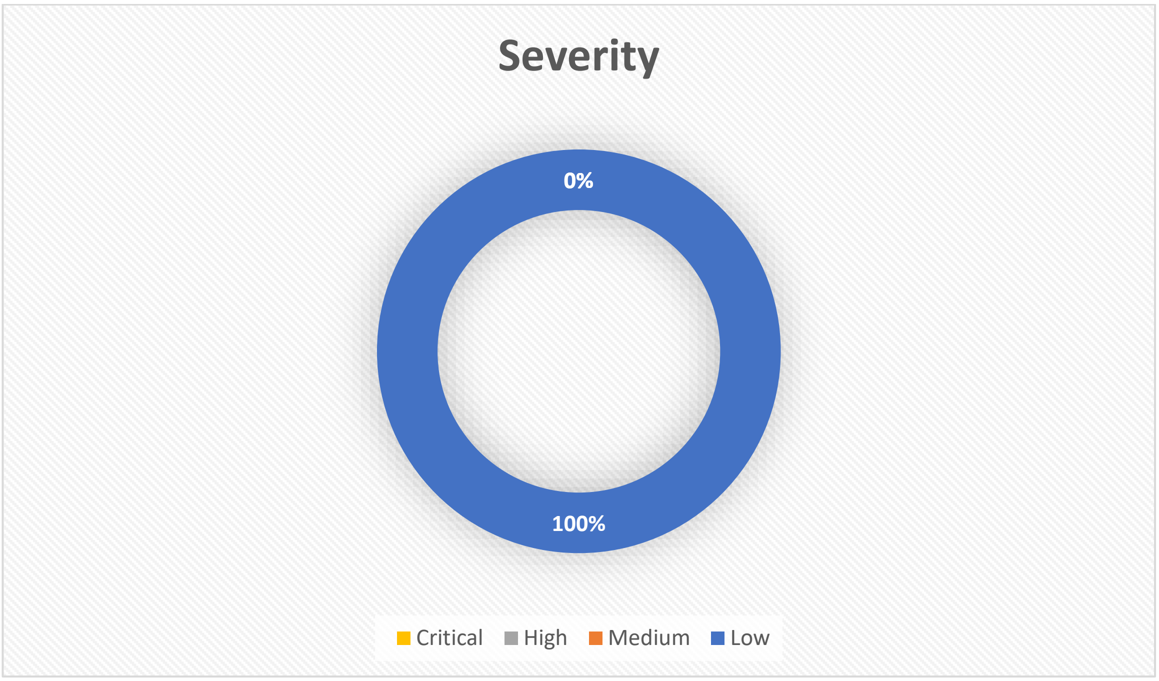
Vulnerability severity information

- ● Critical
- ● High
- ● Medium
- ● Low
- ● Informational

Level	**Description**
Critical	Critical severity vulnerabilities will have a significant effect on the security of the DeFi project, and it is strongly recommended to fix the critical vulnerabilities.
High	High severity vulnerabilities will affect the normal operation of the DeFi project. It is strongly recommended to fix high-risk vulnerabilities.
Medium	Medium severity vulnerability will affect the operation of the DeFi project. It is recommended to fix medium-risk vulnerabilities.
Low	Low severity vulnerabilities may affect the operation of the DeFi project in certain scenarios. It is suggested that the project party should evaluate and consider whether these vulnerabilities need to be fixed.
Informational	There are safety risks theoretically, but it is extremely difficult to reproduce in engineering.

Findings

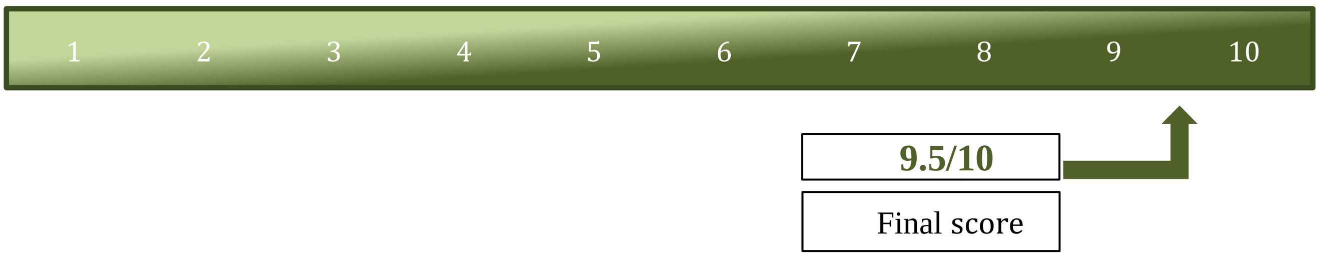
Total issues: 1



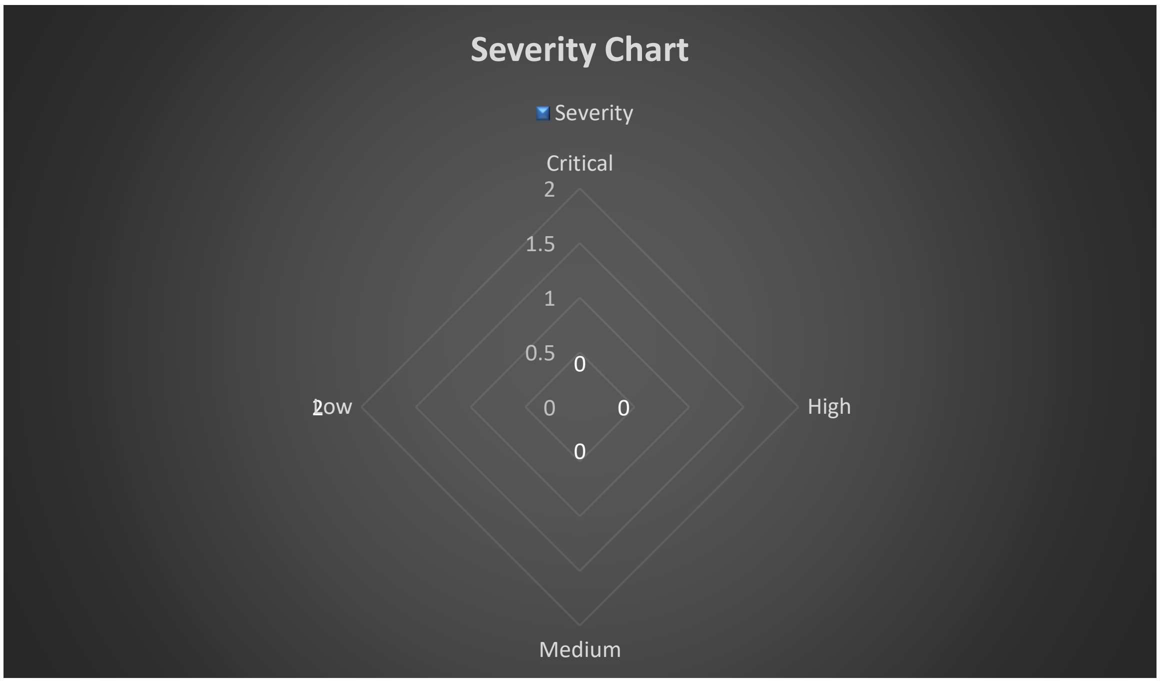
Critical	High	Medium	Low	Informational
0	0	0	1	0

Security Score

As a result of the audit, the code contains no issues. Therefore, the security score is 9.5/10.



Severity chart



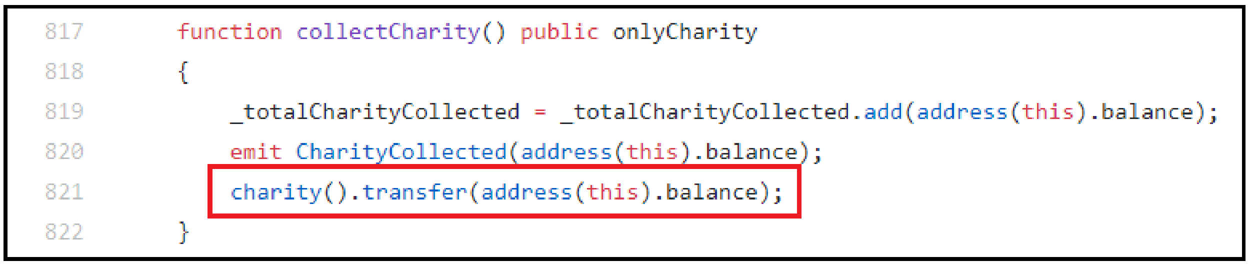
We have so far identified that there are potential issues with severity of 0 Critical, 1 High, 0 Medium, and 1 Low. Overall, these smart contracts are well-designed and engineered.

1. Message call with hardcoded gas amount

Severity	Location	Classification	Status
Low	https://bscscan.com/address/0x94Ad2D084f9e77DD394815cC32aA7D7C09420aF1#code		Open

Description

Call with hardcoded gas amount. The highlighted function call forwards a fixed amount of gas. This is discouraged as the gas cost of EVM instructions may change in the future, which could break this contract's assumptions. If this was done to prevent reentrancy attacks, consider alternative methods such as the checks-effects-interactions pattern or reentrancy locks instead.



```
    function collectCharity() public onlyCharity
    {
        _totalCharityCollected = _totalCharityCollected.add(address(this).balance);
        emit CharityCollected(address(this).balance);
        charity().transfer(address(this).balance);
    }
```

Relationships

CWE-655: Improper Initialization

Remediations

Avoid the use of transfer() and send() and do not otherwise specify a fixed amount of gas when performing calls. Use .call.value(...)("") instead. Use the checks-effects-interactions pattern and/or reentrancy locks to prevent reentrancy attacks.

Function overview

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
IERC20	Interface			
	totalSupply	External		NO
	balanceOf	External		NO
	transfer	External	●	NO
	allowance	External		NO
	approve	External	●	NO
	transferFrom	External	●	NO
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Address	Library			
	isContract	Internal		
	sendValue	Internal	●	
	functionCall	Internal	●	
	functionCall	Internal	●	
	functionCallWithValue	Internal	●	
	functionCallWithValue	Internal	●	
	_functionCallWithValue	Private	●	
Ownable	Implementation	Context		
	<Constructor>	Internal	●	
	owner	Public		NO
	lockedLiquidity	Public		NO
	charity	Public		NO
	burn	Public		NO
	renounceOwnership	Public	●	onlyOwner
	setCharityAddress	Public	●	onlyOwner
	setLockedLiquidityAddress	Public	●	onlyOwner
IUniswapV2Factory	Interface			
	feeTo	External		NO
	feeToSetter	External		NO

	getPair	External		NO
	allPairs	External		NO
	allPairsLength	External		NO
	createPair	External	●	NO
	setFeeTo	External	●	NO
	setFeeToSetter	External	●	NO
IUniswapV2Pair	Interface			
	name	External		NO
	symbol	External		NO
	decimals	External		NO
	totalSupply	External		NO
	balanceOf	External		NO
	allowance	External		NO
	approve	External	●	NO
	transfer	External	●	NO
	transferFrom	External	●	NO
	DOMAIN_SEPARATOR	External		NO
	PERMIT_TYPEHASH	External		NO
	nonces	External		NO
	permit	External	●	NO
	MINIMUM_LIQUIDITY	External		NO
	factory	External		NO
	token0	External		NO
	token1	External		NO
	getReserves	External		NO
	price0CumulativeLast	External		NO
	price1CumulativeLast	External		NO
	kLast	External		NO
	mint	External	●	NO
	burn	External	●	NO
	swap	External	●	NO
	skim	External	●	NO
	sync	External	●	NO
	initialize	External	●	NO
IUniswapV2Router01	Interface			
	factory	External		NO
	WETH	External		NO
	addLiquidity	External	●	NO
	addLiquidityETH	External	■	NO
	removeLiquidity	External	●	NO
	removeLiquidityETH	External	●	NO
	removeLiquidityWithPermit	External	●	NO
	removeLiquidityETHWithPermit	External	●	NO
	swapExactTokensForTokens	External	●	NO
	swapTokensForExactTokens	External	●	NO
	swapExactETHForTokens	External	■	NO
	swapTokensForExactETH	External	●	NO

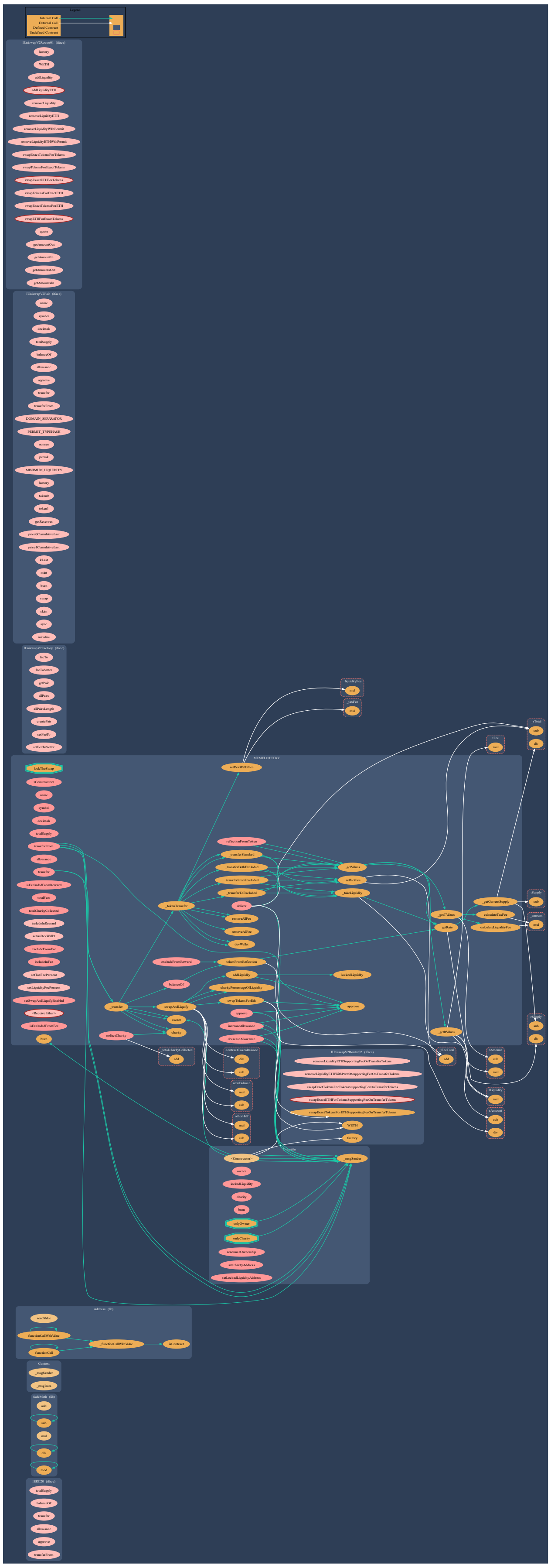
	swapExactTokensForETH	External	🛑	NO
	swapETHForExactTokens	External	■	NO
	quote	External		NO
	getAmountOut	External		NO
	getAmountIn	External		NO
	getAmountsOut	External		NO
	getAmountsIn	External		NO
IUniswapV2Router02	Interface	IUniswapV2Router01		
	removeLiquidityETHSupportingFeeOnTransferTokens	External	🛑	NO
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	🛑	NO
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	🛑	NO
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	■	NO
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	🛑	NO
MEMELOTTERY	Implementation	Context, IERC20, Ownable		
	<Constructor>	Public	🛑	NO
	name	Public		NO
	symbol	Public		NO
	decimals	Public		NO
	totalSupply	Public		NO
	balanceOf	Public		NO
	transfer	Public	🛑	NO
	allowance	Public		NO
	approve	Public	🛑	NO
	transferFrom	Public	🛑	NO
	increaseAllowance	Public	🛑	NO
	decreaseAllowance	Public	🛑	NO
	isExcludedFromReward	Public		NO
	totalFees	Public		NO
	charityPercentageOfLiquidity	Public		NO
	totalCharityCollected	Public		NO
	deliver	Public	🛑	NO
	reflectionFromToken	Public		NO
	tokenFromReflection	Public		NO
	excludeFromReward	Public	🛑	onlyOwner
	includeInReward	External	🛑	onlyOwner
	devWallet	Public		NO
	setAsDevWallet	External	🛑	onlyOwner
	_transferBothExcluded	Private	🛑	
	excludeFromFee	Public	🛑	onlyOwner

includeInFee	Public	●	onlyOwner
setTaxFeePercent	External	●	onlyOwner
setLiquidityFeePercent	External	●	onlyOwner
setSwapAndLiquifyEnabled	Public	●	onlyOwner
<Receive Ether>	External	■	NO
_reflectFee	Private	●	
_getValues	Private		
_getTValues	Private		
_getRValues	Private		
_getRate	Private		
_getCurrentSupply	Private		
_takeLiquidity	Private	●	
calculateTaxFee	Private		
calculateLiquidityFee	Private		
removeAllFee	Private	●	
restoreAllFee	Private	●	
setDevWalletFee	Private	●	
isExcludedFromFee	Public		NO
_approve	Private	●	
_transfer	Private	●	
collectCharity	Public	●	onlyCharity
swapAndLiquify	Private	●	lockTheSwap
swapTokensForEth	Private	●	
addLiquidity	Private	●	
_tokenTransfer	Private	●	
_transferStandard	Private	●	
_transferToExcluded	Private	●	
_transferFromExcluded	Private	●	

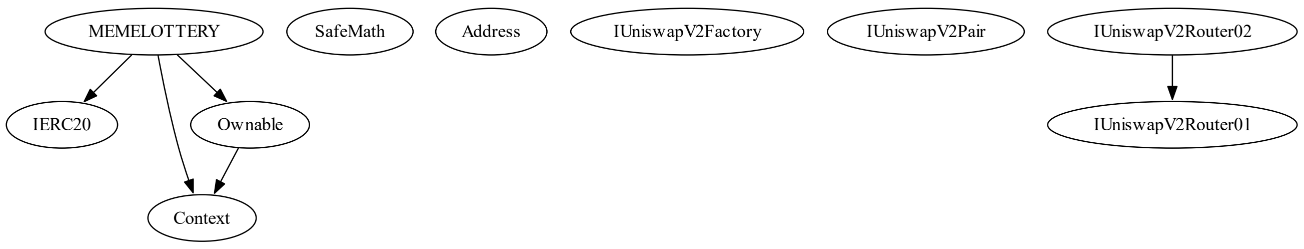
Where Symbol Meaning

- **Function can modify state** ■ **Function is payable**

Functional Flow diagram



Inheritance graph



Liquidity lock

Liquidity locked period	Status
Yes	NA

Token Ownership renounced

Token ownership Renounced	Status
NA	NA

Deployers actions

Can the deployer/owner mint a new token?	Status
NO	NA

Can the deployer/owner blacklist any wallet from selling?	Status
NA	NA

Can deployer/owner lock or burn user funds?	Status
No	NA

Can the deployer/owner pause the contract?	Status
NO	NA

Can the deployer/owner increase the fees?	Status
Yes	NA

SWC Attacks

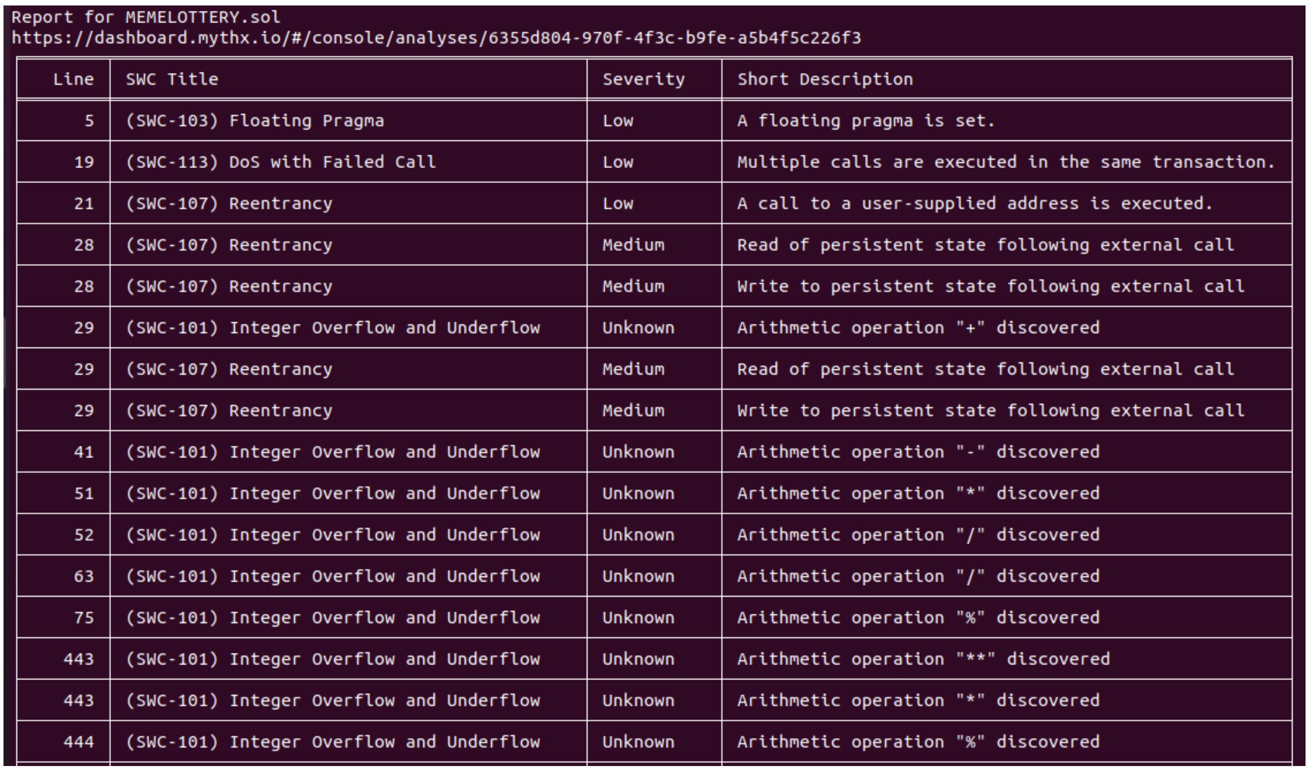
Line	SWC	Severity	Description	Status
https://bscscan.com/address/0x94Ad2D084f9e77DD394815cC32aA7D7C09420aF1#code	134	Low	Call with hardcoded gas amount. The highlighted function call forwards a fixed amount of gas. This is discouraged as the gas cost of EVM instructions may change in the future, which could break this contract's assumptions. If this was done to prevent reentrancy attacks, consider alternative methods such as the checks-effects-interactions pattern or reentrancy locks instead.	Open

Test Results

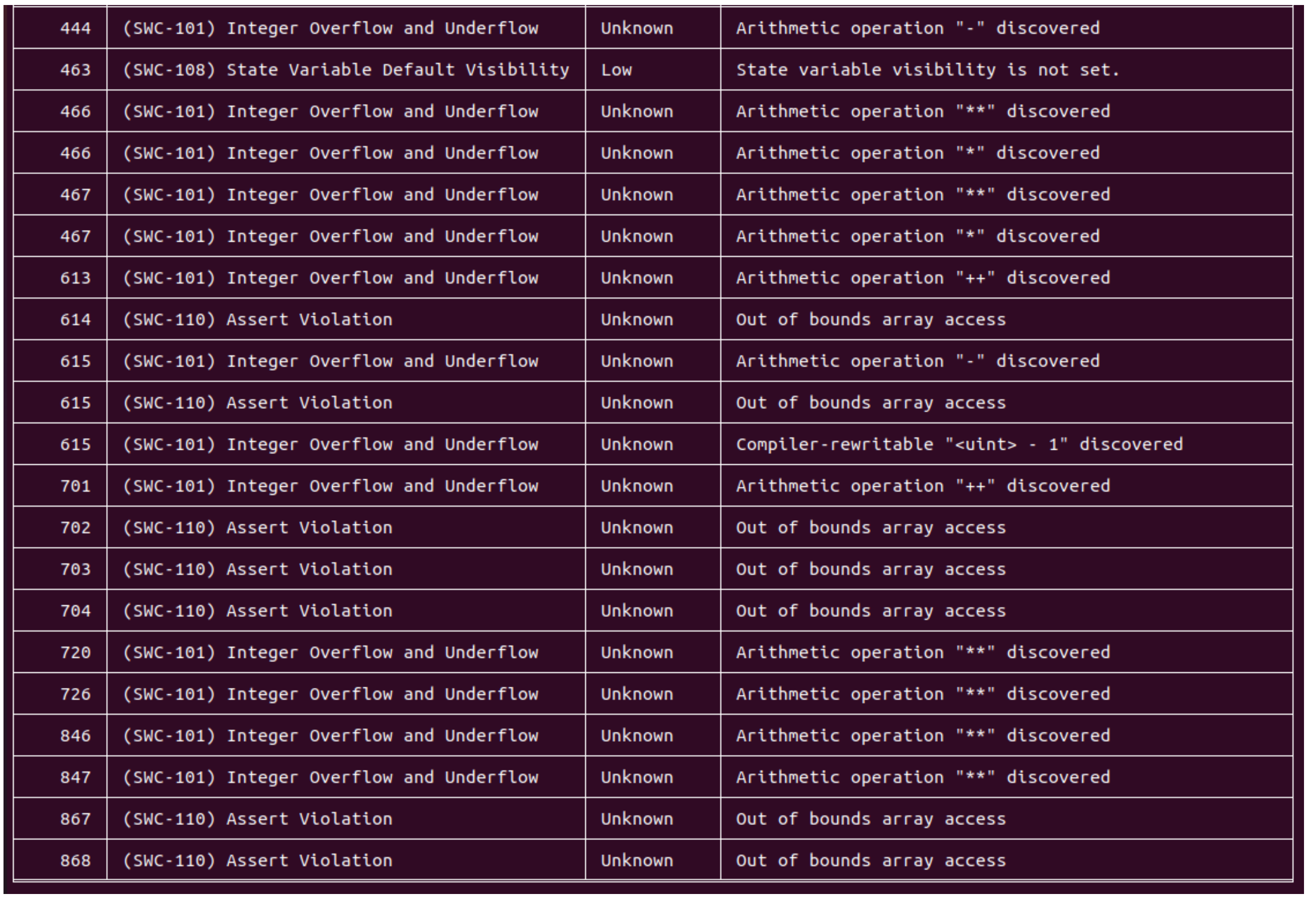
Slither results

NA

Mythx results



```
Report for MEMELOTTERY.sol
https://dashboard.mythx.io/#/console/analyses/6355d804-970f-4f3c-b9fe-a5b4f5c226f3
╒════════╤════════════════════════════════════════╤════════════╤═══════════════════════════════════════════════════╕
│   Line │ SWC Title                              │ Severity   │ Short Description                                 │
╞════════╪════════════════════════════════════════╪════════════╪═══════════════════════════════════════════════════╡
│      5 │ (SWC-103) Floating Pragma              │ Low        │ A floating pragma is set.                         │
├────────┼────────────────────────────────────────┼────────────┼───────────────────────────────────────────────────┤
│     19 │ (SWC-113) DoS with Failed Call         │ Low        │ Multiple calls are executed in the same transaction. │
├────────┼────────────────────────────────────────┼────────────┼───────────────────────────────────────────────────┤
│     21 │ (SWC-107) Reentrancy                   │ Low        │ A call to a user-supplied address is executed.    │
├────────┼────────────────────────────────────────┼────────────┼───────────────────────────────────────────────────┤
│     28 │ (SWC-107) Reentrancy                   │ Medium     │ Read of persistent state following external call  │
├────────┼────────────────────────────────────────┼────────────┼───────────────────────────────────────────────────┤
│     28 │ (SWC-107) Reentrancy                   │ Medium     │ Write to persistent state following external call │
├────────┼────────────────────────────────────────┼────────────┼───────────────────────────────────────────────────┤
│     29 │ (SWC-101) Integer Overflow and Underflow │ Unknown  │ Arithmetic operation "+" discovered               │
├────────┼────────────────────────────────────────┼────────────┼───────────────────────────────────────────────────┤
│     29 │ (SWC-107) Reentrancy                   │ Medium     │ Read of persistent state following external call  │
├────────┼────────────────────────────────────────┼────────────┼───────────────────────────────────────────────────┤
│     29 │ (SWC-107) Reentrancy                   │ Medium     │ Write to persistent state following external call │
├────────┼────────────────────────────────────────┼────────────┼───────────────────────────────────────────────────┤
│     41 │ (SWC-101) Integer Overflow and Underflow │ Unknown  │ Arithmetic operation "-" discovered               │
├────────┼────────────────────────────────────────┼────────────┼───────────────────────────────────────────────────┤
│     51 │ (SWC-101) Integer Overflow and Underflow │ Unknown  │ Arithmetic operation "*" discovered               │
├────────┼────────────────────────────────────────┼────────────┼───────────────────────────────────────────────────┤
│     52 │ (SWC-101) Integer Overflow and Underflow │ Unknown  │ Arithmetic operation "/" discovered               │
├────────┼────────────────────────────────────────┼────────────┼───────────────────────────────────────────────────┤
│     63 │ (SWC-101) Integer Overflow and Underflow │ Unknown  │ Arithmetic operation "/" discovered               │
├────────┼────────────────────────────────────────┼────────────┼───────────────────────────────────────────────────┤
│     75 │ (SWC-101) Integer Overflow and Underflow │ Unknown  │ Arithmetic operation "%" discovered               │
├────────┼────────────────────────────────────────┼────────────┼───────────────────────────────────────────────────┤
│    443 │ (SWC-101) Integer Overflow and Underflow │ Unknown  │ Arithmetic operation "**" discovered              │
├────────┼────────────────────────────────────────┼────────────┼───────────────────────────────────────────────────┤
│    443 │ (SWC-101) Integer Overflow and Underflow │ Unknown  │ Arithmetic operation "*" discovered               │
├────────┼────────────────────────────────────────┼────────────┼───────────────────────────────────────────────────┤
│    444 │ (SWC-101) Integer Overflow and Underflow │ Unknown  │ Arithmetic operation "%" discovered               │
├────────┼────────────────────────────────────────┼────────────┼───────────────────────────────────────────────────┤
```



```
 444 | (SWC-101) Integer Overflow and Underflow   | Unknown | Arithmetic operation "-" discovered
 463 | (SWC-108) State Variable Default Visibility | Low     | State variable visibility is not set.
 466 | (SWC-101) Integer Overflow and Underflow   | Unknown | Arithmetic operation "**" discovered
 466 | (SWC-101) Integer Overflow and Underflow   | Unknown | Arithmetic operation "*" discovered
 467 | (SWC-101) Integer Overflow and Underflow   | Unknown | Arithmetic operation "**" discovered
 467 | (SWC-101) Integer Overflow and Underflow   | Unknown | Arithmetic operation "*" discovered
 613 | (SWC-101) Integer Overflow and Underflow   | Unknown | Arithmetic operation "++" discovered
 614 | (SWC-110) Assert Violation                 | Unknown | Out of bounds array access
 615 | (SWC-101) Integer Overflow and Underflow   | Unknown | Arithmetic operation "-" discovered
 615 | (SWC-110) Assert Violation                 | Unknown | Out of bounds array access
 615 | (SWC-101) Integer Overflow and Underflow   | Unknown | Compiler-rewritable "<uint> - 1" discovered
 701 | (SWC-101) Integer Overflow and Underflow   | Unknown | Arithmetic operation "++" discovered
 702 | (SWC-110) Assert Violation                 | Unknown | Out of bounds array access
 703 | (SWC-110) Assert Violation                 | Unknown | Out of bounds array access
 704 | (SWC-110) Assert Violation                 | Unknown | Out of bounds array access
 720 | (SWC-101) Integer Overflow and Underflow   | Unknown | Arithmetic operation "**" discovered
 726 | (SWC-101) Integer Overflow and Underflow   | Unknown | Arithmetic operation "**" discovered
 846 | (SWC-101) Integer Overflow and Underflow   | Unknown | Arithmetic operation "**" discovered
 847 | (SWC-101) Integer Overflow and Underflow   | Unknown | Arithmetic operation "**" discovered
 867 | (SWC-110) Assert Violation                 | Unknown | Out of bounds array access
 868 | (SWC-110) Assert Violation                 | Unknown | Out of bounds array access
```

Linter results

NA

Conclusion

In this audit, we thoroughly analysed MEMELOTTERY's Smart Contract. The current code base is well organized but there is promptly some Low type of issues found in the first phase of Smart Contract Audit.

Meanwhile, we need to emphasize that smart contracts as a whole are still in an early, but exciting stage of development. To improve this report, we greatly appreciate any constructive feedback or suggestions, on our methodology, audit findings, or potential gaps in scope/coverage.

Disclaimer

Cysro has analysed this smart contract in accordance with the best practices at the date of this report. This report is based on extensive methodological examination and analysis of code, in relation to the cyber security vulnerabilities, blockchain security, and cryptocurrency. The report only represents advice and remediations for clients to improve the quality of code while intending to diminish the inherent risks of blockchains. Cysro recommends conducting a bug bounty program to confirm a high level of security of this smart contract. Cysro does not provide any assurance of a complete bug-free contract.

While Cysro has given its best in conducting the analysis and producing this report, it is important to note that you should not rely on this report to make any decision for investment or involvement in any particular project. This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. Please conduct your own due diligence before investing in any asset. Cysro shall not be liable for any losses incurred in these cases.

The analysis of the security by Cysro is solely based on the smart contract. No other applications or functionalities were reviewed.

About

Cysro is a privately held London and India based cyber security and blockchain technology company. It is built by a team of ethical hackers to aid businesses in battling off cyberattacks.

We specialize in providing services of penetration testing, smart contract auditing, and know your customer. Our mission is to offer the best services possible with the right people, right methodology, right scope, and right report.

Our detailed audit reports shall assist you in comprehending your risk exposure, addressing security issues, and improving data security for your business.

CYSRO

Cyber Security

SMART CONTRACT SECURITY AUDIT