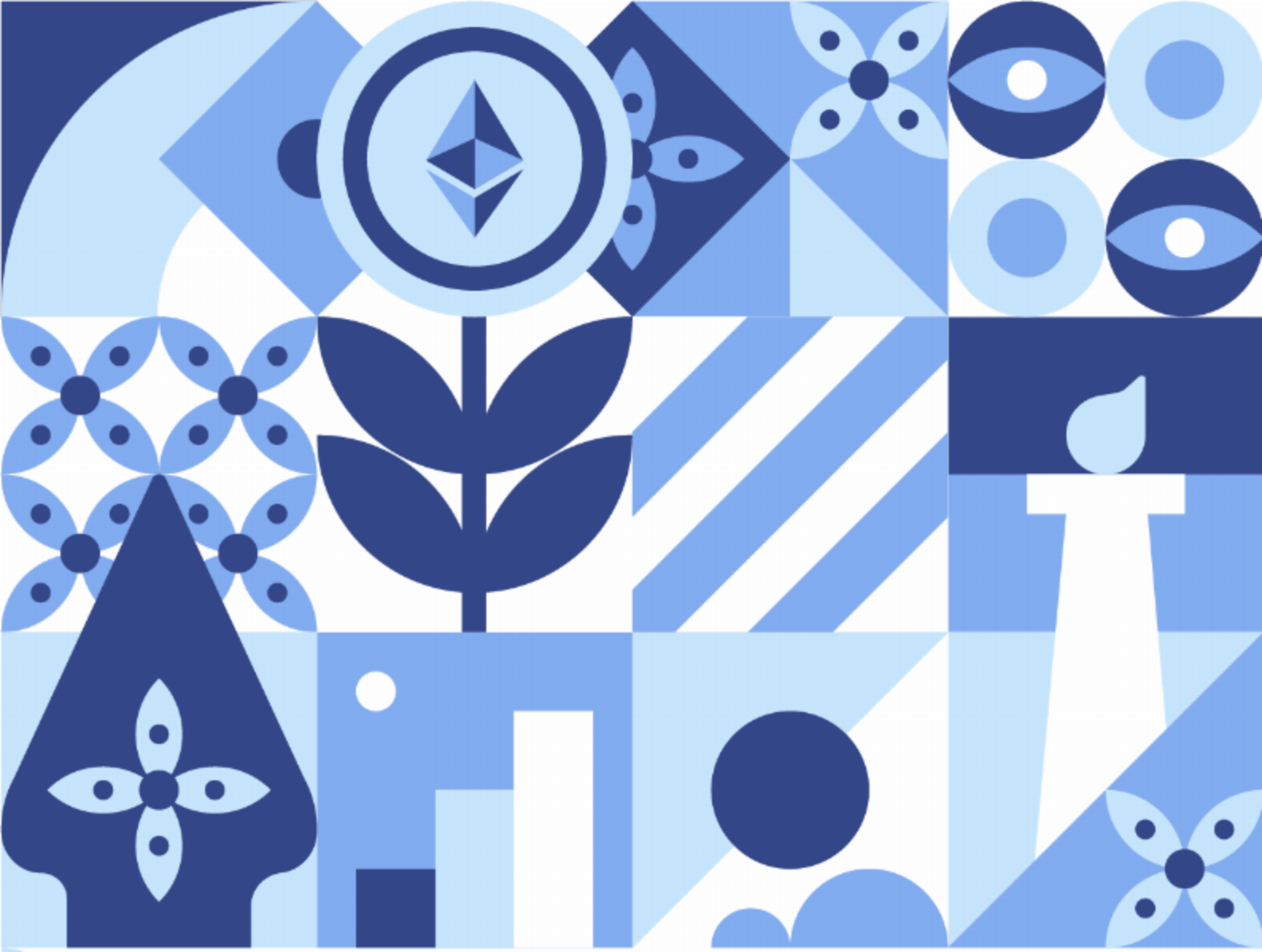

Momonosuke

Smart Contract Audit Report

SYSFIXED

22 Jan 2023

TABLE OF CONTENTS

Audited Details

- Audited Project
- Blockchain
- Addresses
- Project Website
- Codebase

Summary

- Contract Summary
- Audit Findings Summary
- Vulnerabilities Summary

Conclusion

Audit Results

Smart Contract Analysis

- Detected Vulnerabilities

Disclaimer

About Us

AUDITED DETAILS

Audited Project

Project name	Token ticker	Blockchain
Momonosuke	MOMO	Ethereum

Addresses

Contract address	0xa48f3422A740Db4135F83d7Bb186ccdAe22919C5
Contract deployer address	0x0567dd5F09a6F696d2BEC8E855901721435E5Dd4

Project Website

https://momothereum.com/

Codebase

https://etherscan.io/address/0xa48f3422A740Db4135F83d7Bb186ccdAe22919C5#code

SUMMARY

$MOMO is a token inspired by an anime character in the Onepiece series written by mangaka Eiichiro Oda, we plan to combine anime and current technologies for development such as multi-swap platforms, games, and nft

Contract Summary

Documentation Quality

Momonosuke provides a very good documentation with standard of solidity base code.

- The technical description is provided clearly and structured and also dont have any high risk issue.

Code Quality

The Overall quality of the basecode is standard.

- Standard solidity basecode and rules are already followed by Momonosuke with the discovery of several low issues.

Test Coverage

Test coverage of the project is 100% (Through Codebase)

Audit Findings Summary

- SWC-100 SWC-108 | Explicitly define visibility for all state variables on lines 132, 133, 139, 142, 143, 145, 146, 148, 149, 150, 151 and 160.
- SWC-101 | It is recommended to use vetted safe math libraries for arithmetic operations consistently on lines 20, 29, 36, 37, 45, 139, 139, 140, 140, 150, 159, 159, 214, 311, 311 and 317.
- SWC-103 | Pragma statements can be allowed to float when a contract is intended on lines 17.
- SWC-110 SWC-123 | It is recommended to use of revert(), assert(), and require() in Solidity, and the new REVERT opcode in the EVM on lines 259, 260, 295 and 296.

CONCLUSION

We have audited the Momonosuke project released on January 2023 to discover issues and identify potential security vulnerabilities in Momonosuke Project. This process is used to find technical issues and security loopholes which might be found in the smart contract.

The security audit report provides a satisfactory result with some low-risk issues.

The issues found in the Momonosuke smart contract code do not pose a considerable risk. The writing of the contract is close to the standard of writing contracts in general. The low-risk issues found are some arithmetic operation issues, a floating pragma is set, a state variable visibility is not set, and out of bounds array access which the index access expression can cause an exception in case of the use of an invalid array index value. We recommend specifying a fixed compiler version to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.

AUDIT RESULT

Article	Category	Description	Result
Default Visibility	SWC-100 SWC-108	Functions and state variables visibility should be set explicitly. Visibility levels should be specified consciously.	ISSUE FOUND
Integer Overflow and Underflow	SWC-101	If unchecked math is used, all math operations should be safe from overflows and underflows.	ISSUE FOUND
Outdated Compiler Version	SWC-102	It is recommended to use a recent version of the Solidity compiler.	PASS
Floating Pragma	SWC-103	Contracts should be deployed with the same compiler version and flags that they have been tested thoroughly.	ISSUE FOUND
Unchecked Call Return Value	SWC-104	The return value of a message call should be checked.	PASS
Unprotected Ether Withdrawal	SWC-105	Due to missing or insufficient access controls, malicious parties can withdraw from the contract.	PASS
SELFDESTRUCT Instruction	SWC-106	The contract should not be self-destructible while it has funds belonging to users.	PASS
Reentrancy	SWC-107	Check effect interaction pattern should be followed if the code performs recursive call.	PASS
Uninitialized Storage Pointer	SWC-109	Uninitialized local storage variables can point to unexpected storage locations in the contract.	PASS
Assert Violation	SWC-110 SWC-123	Properly functioning code should never reach a failing assert statement.	ISSUE FOUND
Deprecated Solidity Functions	SWC-111	Deprecated built-in functions should never be used.	PASS
Delegate call to Untrusted Callee	SWC-112	Delegatecalls should only be allowed to trusted addresses.	PASS

DoS (Denial of Service)	SWC-113 SWC-128	Execution of the code should never be blocked by a specific contract state unless required.	PASS
Race Conditions	SWC-114	Race Conditions and Transactions Order Dependency should not be possible.	PASS
Authorization through tx.origin	SWC-115	tx.origin should not be used for authorization.	PASS
Block values as a proxy for time	SWC-116	Block numbers should not be used for time calculations.	PASS
Signature Unique ID	SWC-117 SWC-121 SWC-122	Signed messages should always have a unique id. A transaction hash should not be used as a unique id.	PASS
Incorrect Constructor Name	SWC-118	Constructors are special functions that are called only once during the contract creation.	PASS
Shadowing State Variable	SWC-119	State variables should not be shadowed.	PASS
Weak Sources of Randomness	SWC-120	Random values should never be generated from Chain Attributes or be predictable.	PASS
Write to Arbitrary Storage Location	SWC-124	The contract is responsible for ensuring that only authorized user or contract accounts may write to sensitive storage locations.	PASS
Incorrect Inheritance Order	SWC-125	When inheriting multiple contracts, especially if they have identical functions, a developer should carefully specify inheritance in the correct order. The rule of thumb is to inherit contracts from more /general/ to more /specific/.	PASS
Insufficient Gas Griefing	SWC-126	Insufficient gas griefing attacks can be performed on contracts which accept data and use it in a sub-call on another contract.	PASS
Arbitrary Jump Function	SWC-127	As Solidity doesnt support pointer arithmetics, it is impossible to change such variable to an arbitrary value.	PASS

Typographical Error	SWC-129	A typographical error can occur for example when the intent of a defined operation is to sum a number to a variable.	PASS
Override control character	SWC-130	Malicious actors can use the Right-To-Left-Override unicode character to force RTL text rendering and confuse users as to the real intent of a contract.	PASS
Unused variables	SWC-131 SWC-135	Unused variables are allowed in Solidity and they do not pose a direct security issue.	PASS
Unexpected Ether balance	SWC-132	Contracts can behave erroneously when they strictly assume a specific Ether balance.	PASS
Hash Collisions Variable	SWC-133	Using abi.encodePacked() with multiple variable length arguments can, in certain situations, lead to a hash collision.	PASS
Hardcoded gas amount	SWC-134	The transfer() and send() functions forward a fixed amount of 2300 gas.	PASS
Unencrypted Private Data	SWC-136	It is a common misconception that private type variables cannot be read.	PASS

SMART CONTRACT ANALYSIS

Started	Saturday Jan 21 2023 00:35:13 GMT+0000 (Coordinated Universal Time)
Finished	Sunday Jan 22 2023 01:19:20 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Main Source File	Momothereum.sol

Detected Issues

ID	Title	Severity	Status
SWC-101	ARITHMETIC OPERATION "+" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "-" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "/" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "/" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "/" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "+" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "/" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "+" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "/" DISCOVERED	low	acknowledged

SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "+" DISCOVERED	low	acknowledged
SWC-103	A FLOATING PRAGMA IS SET.	low	acknowledged
SWC-108	STATE VARIABLE VISIBILITY IS NOT SET.	low	acknowledged
SWC-108	STATE VARIABLE VISIBILITY IS NOT SET.	low	acknowledged
SWC-108	STATE VARIABLE VISIBILITY IS NOT SET.	low	acknowledged
SWC-108	STATE VARIABLE VISIBILITY IS NOT SET.	low	acknowledged
SWC-108	STATE VARIABLE VISIBILITY IS NOT SET.	low	acknowledged
SWC-108	STATE VARIABLE VISIBILITY IS NOT SET.	low	acknowledged
SWC-108	STATE VARIABLE VISIBILITY IS NOT SET.	low	acknowledged
SWC-108	STATE VARIABLE VISIBILITY IS NOT SET.	low	acknowledged
SWC-108	STATE VARIABLE VISIBILITY IS NOT SET.	low	acknowledged
SWC-108	STATE VARIABLE VISIBILITY IS NOT SET.	low	acknowledged
SWC-108	STATE VARIABLE VISIBILITY IS NOT SET.	low	acknowledged
SWC-108	STATE VARIABLE VISIBILITY IS NOT SET.	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 20

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- Momothereum.sol

Locations

```
19   function add(uint256 a, uint256 b) internal pure returns (uint256) {
20   uint256 c = a + b;
21   require(c >= a, "SafeMath: addition overflow");
22   return c;
23   }
24
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 29

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- Momothereum.sol

Locations

```
28   require(b <= a, errorMessage);
29   uint256 c = a - b;
30   return c;
31   }
32   function mul(uint256 a, uint256 b) internal pure returns (uint256) {
33
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 36

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- Momothereum.sol

Locations

```
35   }
36   uint256 c = a * b;
37   require(c / a == b, "SafeMath: multiplication overflow");
38   return c;
39   }
40
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 37

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- Momothereum.sol

Locations

```
36   uint256 c = a * b;
37   require(c / a == b, "SafeMath: multiplication overflow");
38   return c;
39   }
40   function div(uint256 a, uint256 b) internal pure returns (uint256) {
41
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 45

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- Momothereum.sol

Locations

```
44   require(b > 0, errorMessage);
45   uint256 c = a / b;
46   return c;
47   }
48   }
49
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 139

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- Momothereum.sol

Locations

```
138
139   uint256 _totalSupply = 1_000_000 * (10 ** _decimals);
140   uint256 public _maxWalletAmount = (_totalSupply * 100) / 100;
141
142   mapping (address => uint256) _balances;
143
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 139

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- Momothereum.sol

Locations

```
138
139   uint256 _totalSupply = 1_000_000 * (10 ** _decimals);
140   uint256 public _maxWalletAmount = (_totalSupply * 100) / 100;
141
142   mapping (address => uint256) _balances;
143
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 140

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- Momothereum.sol

Locations

```
139   uint256 _totalSupply = 1_000_000 * (10 ** _decimals);
140   uint256 public _maxWalletAmount = (_totalSupply * 100) / 100;
141
142   mapping (address => uint256) _balances;
143   mapping (address => mapping (address => uint256)) _allowances;
144
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 140

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- Momothereum.sol

Locations

```
139   uint256 _totalSupply = 1_000_000 * (10 ** _decimals);
140   uint256 public _maxWalletAmount = (_totalSupply * 100) / 100;
141
142   mapping (address => uint256) _balances;
143   mapping (address => mapping (address => uint256)) _allowances;
144
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 150

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- Momothereum.sol

Locations

```
149   uint256 marketingFee = 3;
150   uint256 totalFee = liquidityFee + marketingFee;
151   uint256 feeDenominator = 100;
152
153   address private marketingFeeReceiver = 0xB5A9CED8d3A8B9364a25C579f99d22EC6cA62579;
154
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 159

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- Momothereum.sol

Locations

```
158   bool public swapEnabled = true;
159   uint256 public swapThreshold = _totalSupply / 1000 * 2; //
160   bool inSwap;
161   modifier swapping() { inSwap = true; _; inSwap = false; }
162
163
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 159

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- Momothereum.sol

Locations

```
158   bool public swapEnabled = true;
159   uint256 public swapThreshold = _totalSupply / 1000 * 2; //
160   bool inSwap;
161   modifier swapping() { inSwap = true; _; inSwap = false; }
162
163
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 214

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- Momothereum.sol

Locations

```
213   if (recipient != pair && recipient != DEAD) {
214   require(isTxLimitExempt[recipient] || _balances[recipient] + amount <=
_maxWalletAmount, "Transfer amount exceeds the bag size.");
215   }
216
217   if(shouldSwapBack()){ swapBack(); }
218
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 311

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- Momothereum.sol

Locations

```
310   function setWalletLimit(uint256 amountPercent) external onlyOwner {
311   _maxWalletAmount = (_totalSupply * amountPercent ) / 1000;
312   }
313
314   function setFee(uint256 _liquidityFee, uint256 _marketingFee) external onlyOwner {
315
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 311

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- Momothereum.sol

Locations

```
310   function setWalletLimit(uint256 amountPercent) external onlyOwner {
311   _maxWalletAmount = (_totalSupply * amountPercent ) / 1000;
312   }
313
314   function setFee(uint256 _liquidityFee, uint256 _marketingFee) external onlyOwner {
315
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 317

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- Momothereum.sol

Locations

```
316   marketingFee = _marketingFee;
317   totalFee = liquidityFee + marketingFee;
318   }
319
320   event AutoLiquify(uint256 amountETH, uint256 amountBOG);
321
```

SWC-103 | A FLOATING PRAGMA IS SET.

LINE 17

low SEVERITY

The current pragma Solidity directive is ""^0.8.5"". It is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.

Source File

- Momothereum.sol

Locations

```
16   // SPDX-License-Identifier: MIT
17   pragma solidity ^0.8.5;
18   library SafeMath {
19   function add(uint256 a, uint256 b) internal pure returns (uint256) {
20   uint256 c = a + b;
21
```

SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 132

low SEVERITY

It is best practice to set the visibility of state variables explicitly. The default visibility for "routerAdress" is internal. Other possible visibility settings are public and private.

Source File

- Momothereum.sol

Locations

```
131   using SafeMath for uint256;
132   address routerAdress = 0x7a250d5630B4cF539739dF2C5dAcb4c659F2488D;
133   address DEAD = 0x000000000000000000000000000000000000dEaD;
134
135   string constant _name = "Momonosuke";
136
```

SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 133

low SEVERITY

It is best practice to set the visibility of state variables explicitly. The default visibility for "DEAD" is internal. Other possible visibility settings are public and private.

Source File

- Momothereum.sol

Locations

```
132   address routerAdress = 0x7a250d5630B4cF539739dF2C5dAcb4c659F2488D;
133   address DEAD = 0x000000000000000000000000000000000000dEaD;
134
135   string constant _name = "Momonosuke";
136   string constant _symbol = "MOMO";
137
```

SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 139

low SEVERITY

It is best practice to set the visibility of state variables explicitly. The default visibility for "_totalSupply" is internal. Other possible visibility settings are public and private.

Source File

- Momothereum.sol

Locations

```
138
139   uint256 _totalSupply = 1_000_000 * (10 ** _decimals);
140   uint256 public _maxWalletAmount = (_totalSupply * 100) / 100;
141
142   mapping (address => uint256) _balances;
143
```

SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 142

low SEVERITY

It is best practice to set the visibility of state variables explicitly. The default visibility for "_balances" is internal. Other possible visibility settings are public and private.

Source File

- Momothereum.sol

Locations

```
141
142   mapping (address => uint256) _balances;
143   mapping (address => mapping (address => uint256)) _allowances;
144
145   mapping (address => bool) isFeeExempt;
146
```

SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 143

low SEVERITY

It is best practice to set the visibility of state variables explicitly. The default visibility for "_allowances" is internal. Other possible visibility settings are public and private.

Source File

- Momothereum.sol

Locations

```
142   mapping (address => uint256) _balances;
143   mapping (address => mapping (address => uint256)) _allowances;
144
145   mapping (address => bool) isFeeExempt;
146   mapping (address => bool) isTxLimitExempt;
147
```

SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 145

low SEVERITY

It is best practice to set the visibility of state variables explicitly. The default visibility for "isFeeExempt" is internal. Other possible visibility settings are public and private.

Source File

- Momothereum.sol

Locations

```
144
145   mapping (address => bool) isFeeExempt;
146   mapping (address => bool) isTxLimitExempt;
147
148   uint256 liquidityFee = 0;
149
```

SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 146

low SEVERITY

It is best practice to set the visibility of state variables explicitly. The default visibility for "isTxLimitExempt" is internal. Other possible visibility settings are public and private.

Source File

- Momothereum.sol

Locations

```
145   mapping (address => bool) isFeeExempt;
146   mapping (address => bool) isTxLimitExempt;
147
148   uint256 liquidityFee = 0;
149   uint256 marketingFee = 3;
150
```

SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 148

low SEVERITY

It is best practice to set the visibility of state variables explicitly. The default visibility for "liquidityFee" is internal. Other possible visibility settings are public and private.

Source File

- Momothereum.sol

Locations

```
147
148   uint256 liquidityFee = 0;
149   uint256 marketingFee = 3;
150   uint256 totalFee = liquidityFee + marketingFee;
151   uint256 feeDenominator = 100;
152
```

SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 149

low SEVERITY

It is best practice to set the visibility of state variables explicitly. The default visibility for "marketingFee" is internal. Other possible visibility settings are public and private.

Source File

- Momothereum.sol

Locations

```
148   uint256 liquidityFee = 0;
149   uint256 marketingFee = 3;
150   uint256 totalFee = liquidityFee + marketingFee;
151   uint256 feeDenominator = 100;
152
153
```

SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 150

low SEVERITY

It is best practice to set the visibility of state variables explicitly. The default visibility for "totalFee" is internal. Other possible visibility settings are public and private.

Source File

- Momothereum.sol

Locations

```
149   uint256 marketingFee = 3;
150   uint256 totalFee = liquidityFee + marketingFee;
151   uint256 feeDenominator = 100;
152
153   address private marketingFeeReceiver = 0xB5A9CED8d3A8B9364a25C579f99d22EC6cA62579;
154
```

SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 151

low SEVERITY

It is best practice to set the visibility of state variables explicitly. The default visibility for "feeDenominator" is internal. Other possible visibility settings are public and private.

Source File

- Momothereum.sol

Locations

```
150   uint256 totalFee = liquidityFee + marketingFee;
151   uint256 feeDenominator = 100;
152
153   address private marketingFeeReceiver = 0xB5A9CED8d3A8B9364a25C579f99d22EC6cA62579;
154
155
```

SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 160

low SEVERITY

It is best practice to set the visibility of state variables explicitly. The default visibility for "inSwap" is internal. Other possible visibility settings are public and private.

Source File

- Momothereum.sol

Locations

```
159   uint256 public swapThreshold = _totalSupply / 1000 * 2; //
160   bool inSwap;
161   modifier swapping() { inSwap = true; _; inSwap = false; }
162
163   constructor () Ownable(msg.sender) {
164
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 259

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- Momothereum.sol

Locations

```
258   address[] memory path = new address[](2);
259   path[0] = address(this);
260   path[1] = router.WETH();
261
262   uint256 balanceBefore = address(this).balance;
263
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 260

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- Momothereum.sol

Locations

```
259   path[0] = address(this);
260   path[1] = router.WETH();
261
262   uint256 balanceBefore = address(this).balance;
263
264
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 295

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- Momothereum.sol

Locations

```
294   address[] memory path = new address[](2);
295   path[0] = router.WETH();
296   path[1] = address(this);
297
298   router.swapExactETHForTokensSupportingFeeOnTransferTokens{value: amount}(
299
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 296

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- Momothereum.sol

Locations

```
295   path[0] = router.WETH();
296   path[1] = address(this);
297
298   router.swapExactETHForTokensSupportingFeeOnTransferTokens{value: amount}(
299   0,
300
```

DISCLAIMER

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you ("Customer" or the "Company") in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. 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 Sysfixed's prior written consent in each instance.

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 considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Sysfixed to perform a security assessment. This report 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 is a limited report on our findings based on our analysis, in accordance with good industry practice as of the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing 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.

This report is provided for information purposes only and on a non-reliance basis and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and Sysfixed and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers, and other representatives) (Sysfixed) owe no duty of care.

ABOUT US

Sysfixed is a blockchain security certification organization established in 2021 with the objective to provide smart contract security services and verify their correctness in blockchain-based protocols. Sysfixed automatically scans for security vulnerabilities in Ethereum and other EVM-based blockchain smart contracts. Sysfixed a comprehensive range of analysis techniques—including static analysis, dynamic analysis, and symbolic execution—can accurately detect security vulnerabilities to provide an in-depth analysis report. With a vibrant ecosystem of world-class integration partners that amplify developer productivity, Sysfixed can be utilized in all phases of your project's lifecycle. Our team of security experts is dedicated to the research and improvement of our tools and techniques used to fortify your code.