IMOV

# Smart Contract Audit Report

SYSFIXED

22 Jul 2022

# TABLE OF CONTENTS

# AUDITED DETAILS

## Audited Project

| Project name | Token ticker | Blockchain |
|---|---|---|
| IMOV | IMOV | Binance Smart Chain |

## Addresses

| | |
|---|---|
| **Contract address** | 0x7b8779e01d117ec7e220f8299a6f93672e8eae23 |
| **Contract deployer address** | 0xfC724429159A416332e7746AA8aC40a8491c0194 |

## Project Website

**https://imov.app/**

## Codebase

**https://bscscan.com/address/0x7b8779e01d117ec7e220f8299a6f93672e8eae23#code**

# SUMMARY

IMOV is a Web3 lifestyle app with inbuilt Game-Fi and Social-Fi elements, and the first inclusive fitness app for people of all abilities. Users equip themselves with NFTs in the form of Sneakers. By walking, jogging, or running outdoors, users will earn game currency, which can either be used in-game, or cashed out for profit.

## Contract Summary

**Documentation Quality**

IMOV 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 IMOV with the discovery of several low issues.

**Test Coverage**

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

## Audit Findings Summary

- SWC-101 | It is recommended to use vetted safe math libraries for arithmetic operations consistently on lines 134, 144, 152, 171, 173, 185, 186, 200, 202, 462, 462, 462, 464, 464, 617, 617, 618, 641 and 649.
- 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 631 and 632.

# CONCLUSION

We have audited the IMOV project released on July 2021 to discover issues and identify potential security vulnerabilities in IMOV 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. This smart contract doesn't have any issues.

We didn't find any issues in our audit results for IMOV smart contracts. This result is very satisfying.

Judging from the code base of this smart contract, this smart contract follows the official Solidity style guide.

# AUDIT RESULT

| Article | Category | Description | Result |
|---|---|---|---|
| Default Visibility | SWC-100<br>SWC-108 | Functions and state variables visibility should be set explicitly. Visibility levels should be specified consciously. | PASS |
| 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. | PASS |
| 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<br>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<br>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<br>SWC-121<br>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<br>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** | Thursday Jul 21 2022 14:10:40 GMT+0000 (Coordinated Universal Time) |
| **Finished** | Friday Jul 22 2022 07:46:03 GMT+0000 (Coordinated Universal Time) |
| **Mode** | Standard |
| **Main Source File** | IMOV.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-101 | ARITHMETIC OPERATION "-" DISCOVERED | low | acknowledged |
| SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED | low | acknowledged |
| SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED | 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 134

## low SEVERITY

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

## Source File

- IMOV.sol

## Locations

```
133   unchecked {
134   _approve(sender, _msgSender(), currentAllowance - amount);
135   }
136   }
137
138
```

# SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 144

## low SEVERITY

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

## Source File

- IMOV.sol

## Locations

```
143   function increaseAllowance(address spender, uint256 addedValue) public virtual
returns (bool) {
144   _approve(_msgSender(), spender, _allowances[_msgSender()][spender] + addedValue);
145   return true;
146   }
147
148
```

# SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 152

## low SEVERITY

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

## Source File

- IMOV.sol

## Locations

```
151   unchecked {
152   _approve(_msgSender(), spender, currentAllowance - subtractedValue);
153   }
154
155   return true;
156
```

# SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 171

## low SEVERITY

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

## Source File

- IMOV.sol

## Locations

```
170   unchecked {
171   _balances[sender] = senderBalance - amount;
172   }
173   _balances[recipient] += amount;
174
175
```

# SWC-101 | ARITHMETIC OPERATION "+=" DISCOVERED

LINE 173

## low SEVERITY

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

## Source File

- IMOV.sol

## Locations

```
172   }
173   _balances[recipient] += amount;
174
175   emit Transfer(sender, recipient, amount);
176
177
```

# SWC-101 | ARITHMETIC OPERATION "+=" DISCOVERED

LINE 185

## low SEVERITY

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

## Source File

- IMOV.sol

## Locations

```
184
185   _totalSupply += amount;
186   _balances[account] += amount;
187   emit Transfer(address(0), account, amount);
188
189
```

# SWC-101 | ARITHMETIC OPERATION "+=" DISCOVERED

LINE 186

## low SEVERITY

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

## Source File

- IMOV.sol

## Locations

```
185   _totalSupply += amount;
186   _balances[account] += amount;
187   emit Transfer(address(0), account, amount);
188
189   _afterTokenTransfer(address(0), account, amount);
190
```

# SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 200

## low SEVERITY

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

## Source File

- IMOV.sol

## Locations

```
199   unchecked {
200   _balances[account] = accountBalance - amount;
201   }
202   _totalSupply -= amount;
203
204
```

# SWC-101 | ARITHMETIC OPERATION "-=" DISCOVERED

LINE 202

## low SEVERITY

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

## Source File

- IMOV.sol

## Locations

```
201   }
202   _totalSupply -= amount;
203
204   emit Transfer(account, address(0), amount);
205
206
```

# SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 462

## low SEVERITY

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

## Source File

- IMOV.sol

## Locations

```
461   operator = msg.sender;
462   swapTokensAtAmount = 100_000_000 * (10 ** 18) / 5000;
463   marketingWallet = newOwner;
464   _mint(owner(), 100_000_000 * (10 ** 18));
465   sellFee = 20;
466
```

# SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 462

## low SEVERITY

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

## Source File

- IMOV.sol

## Locations

```
461   operator = msg.sender;
462   swapTokensAtAmount = 100_000_000 * (10 ** 18) / 5000;
463   marketingWallet = newOwner;
464   _mint(owner(), 100_000_000 * (10 ** 18));
465   sellFee = 20;
466
```

# SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 462

## low SEVERITY

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

## Source File

- IMOV.sol

## Locations

```
461   operator = msg.sender;
462   swapTokensAtAmount = 100_000_000 * (10 ** 18) / 5000;
463   marketingWallet = newOwner;
464   _mint(owner(), 100_000_000 * (10 ** 18));
465   sellFee = 20;
466
```

# SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 464

## low SEVERITY

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

## Source File

- IMOV.sol

## Locations

```
463   marketingWallet = newOwner;
464   _mint(owner(), 100_000_000 * (10 ** 18));
465   sellFee = 20;
466
467   IUniswapV2Router02 _uniswapV2Router =
IUniswapV2Router02(0x10ED43C718714eb63d5aA57B78B54704E256024E);
468
```

# SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 464

## low SEVERITY

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

## Source File

- IMOV.sol

## Locations

```
463   marketingWallet = newOwner;
464   _mint(owner(), 100_000_000 * (10 ** 18));
465   sellFee = 20;
466
467   IUniswapV2Router02 _uniswapV2Router =
IUniswapV2Router02(0x10ED43C718714eb63d5aA57B78B54704E256024E);
468
```

# SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 617

## low SEVERITY

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

## Source File

- IMOV.sol

## Locations

```
616   if(takeFee && to == uniswapV2Pair && sellFee > 0) {
617   uint256 fees = (amount * sellFee) / 100;
618   amount = amount - fees;
619   super._transfer(from, address(this), fees);
620   }
621
```

# SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 617

## low SEVERITY

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

## Source File

- IMOV.sol

## Locations

```
616   if(takeFee && to == uniswapV2Pair && sellFee > 0) {
617   uint256 fees = (amount * sellFee) / 100;
618   amount = amount - fees;
619   super._transfer(from, address(this), fees);
620   }
621
```

# SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 618

## low SEVERITY

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

## Source File

- IMOV.sol

## Locations

```
617   uint256 fees = (amount * sellFee) / 100;
618   amount = amount - fees;
619   super._transfer(from, address(this), fees);
620   }
621
622
```

# SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 641

## low SEVERITY

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

## Source File

- IMOV.sol

## Locations

```
640
641   uint256 newBalance = address(this).balance - initialBalance;
642
643   sendBNB(payable(marketingWallet), newBalance);
644
645
```

# SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 649

## low SEVERITY

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

## Source File

- IMOV.sol

## Locations

```
648   function setSwapTokensAtAmount(uint256 newAmount) external onlyOwner{
649   require(newAmount > totalSupply() / 100000, "SwapTokensAtAmount must be greater
than 0.001% of total supply");
650   swapTokensAtAmount = newAmount;
651   }
652   }
653
```

# SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 631

## low SEVERITY

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

## Source File

- IMOV.sol

## Locations

```
630   address[] memory path = new address[](2);
631   path[0] = address(this);
632   path[1] = uniswapV2Router.WETH();
633
634   uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(
635
```

# SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 632

## low SEVERITY

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

## Source File

- IMOV.sol

## Locations

```
631   path[0] = address(this);
632   path[1] = uniswapV2Router.WETH();
633
634   uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(
635   tokenAmount,
636
```

# 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.