NUMEN

Smart Contract Audit Report

fomocup Smart Contract

9 Dec 2022

Numen Cyber Labs - Security Services

Table of Content

1 Executive Summary

Numen Cyber Technology was engaged by fomocup to review smart contract implementation. The assessment was conducted in accordance with our systematic approach to evaluate potential security issues based upon customer requirement. The report provides detailed recommendations to resolve the issue and provide additional suggestions or recommendations for improvement.

Two Medium severities findings are related to owner authority, centralized risk.

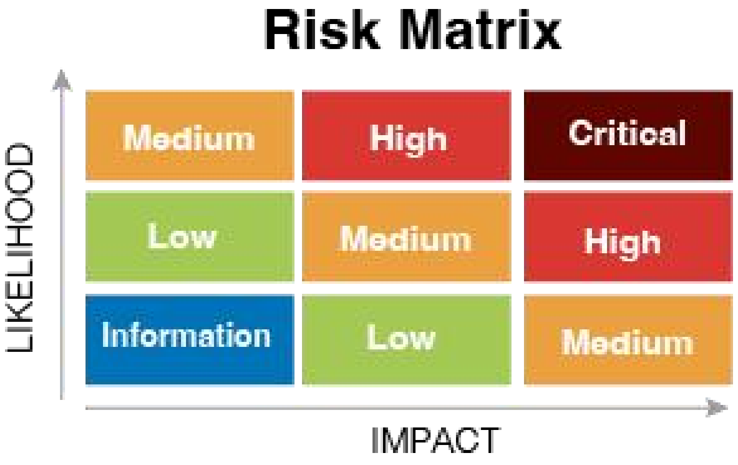
The outcome of the assessment outlined in chapter 3 provides the system's owners a full description of the vulnerabilities identified, the associated risk rating for each vulnerability, and detailed recommendations that will resolve the underlying technical issue.

Methodology

To standardize the evaluation, we define the following terminology based on OWASP Risk Rating Methodology [10] which is the gold standard in risk assessment using the following risk models:

- Likelihood: represents how likely a particular vulnerability is to be uncovered and exploited in the wild.
- Impact: measures the technical loss and business damage of a successful attack.
- Severity: determine the overall criticality of the risk.

Likelihood and impact are categorized into three ratings: High, Medium and Low. Severity is determined by likelihood and impact and can be classified into four categories accordingly, Critical, High, Medium, Low shown in table 1.1.



Medium	High	Critical
Low	Medium	High
Information	Low	Medium

Table 1.1: Overall Risk Severity

To evaluate the risk, we will be going through a list of items, and each would be labelled with a severity category. The audit was performed with a systematic approach guided by a comprehensive assessment list carefully designed to identify known and impactful security issues. If our tool or analysis does not identify any issue, the contract can be considered safe regarding the assessed item. For any discovered issue, we might further deploy contracts on our private test environment and run tests to confirm the findings. If necessary, we would additionally build a PoC to demonstrate the possibility of exploitation. The concrete list of check items is shown in Table 1.2.

- Basic Coding Bugs: We first statically analyze given smart contracts with our proprietary static code analyzer for known coding bugs, and then manually verify (reject or confirm) all the issues found by our tool.

- Code and business security testing: We further review business logics, examine system operations, and place DeFi-related aspects under scrutiny to uncover possible pitfalls and/or bugs.

- Additional Recommendations: We also provide additional suggestions regarding the coding and development of smart contracts from the perspective of proven programming practices.

Category	Assessment Item
Basic Coding Assessment	Apply Verification Control
	Authorization Access Control
	Forged Transfer Vulnerability
	Forged Transfer Notification
	Numeric Overflow
	Transaction Rollback Attack
	Transaction Block Stuffing Attack
	Soft fail Attack
	Hard fail Attack
	Abnormal Memo
	Abnormal Resource Consumption
	Secure Random Number
Advanced Source Code Scrutiny	Asset Security
	Cryptography Security
	Business Logic Review
	Source Code Functional Verification
	Account Authorization Control
	Sensitive Information Disclosure

	Circuit Breaker
	Blacklist Control
	System API Call Analysis
	Contract Deployment Consistency Check
Additional Recommendations	Semantic Consistency Checks
	Following Other Best Practices

Table 1.2: The Full List of Assessment Items

To better describe each issue we identified, we categorize the findings with Common Weakness Enumeration (CWE-699) [14], which is a community-developed list of software weakness types to better delineate and organize weaknesses around concepts frequently encountered in software development.

2 Findings Overview

2.1 Project info and Contract address

Project Name: fomocup

Project URL: http://www.fomocup.top/

Audit Time: 2022/12.6 - 2022/12.9

Language: solidity

Contract Name	Smart Contract Address
Fomocup.sol	https://bscscan.com/address/0x1F6D7cAfC46B172A82bdbe0Bbe5150ce2d72f676
GuessChampion.sol	https://bscscan.com/address/0x2A43A1e160c978b29412a0aC1374Aa97231514c5

Token Info:

Token Name	Tickets
Token Symbol	TK
Decimals	18
TotalSupply	The current circulation is 4701(the total supply no upper limit, it will be generated with the number of buy keys)
Token Type	BEP20

2.2 Summary

Severity	Found	
Critical	0	

High	0	
Medium	2	🟧 🟧
Low	0	
Informational	0	

2.3 Key Findings

Two Medium severities findings are related to owner authority, centralized risk.

ID	Severity	Findings Title	Status	Confirm
NVE-001	Medium	Owner has higher authority	Ignore	Confirmed
NVE-002	Medium	Centralized risk	Ignore	Confirmed

Table 2.1: Key Audit Findings

3 Detailed Description of Findings

3.1 Owner has higher authority

ID: NVE-001

Location: Fomocup.sol

Severity: Medium

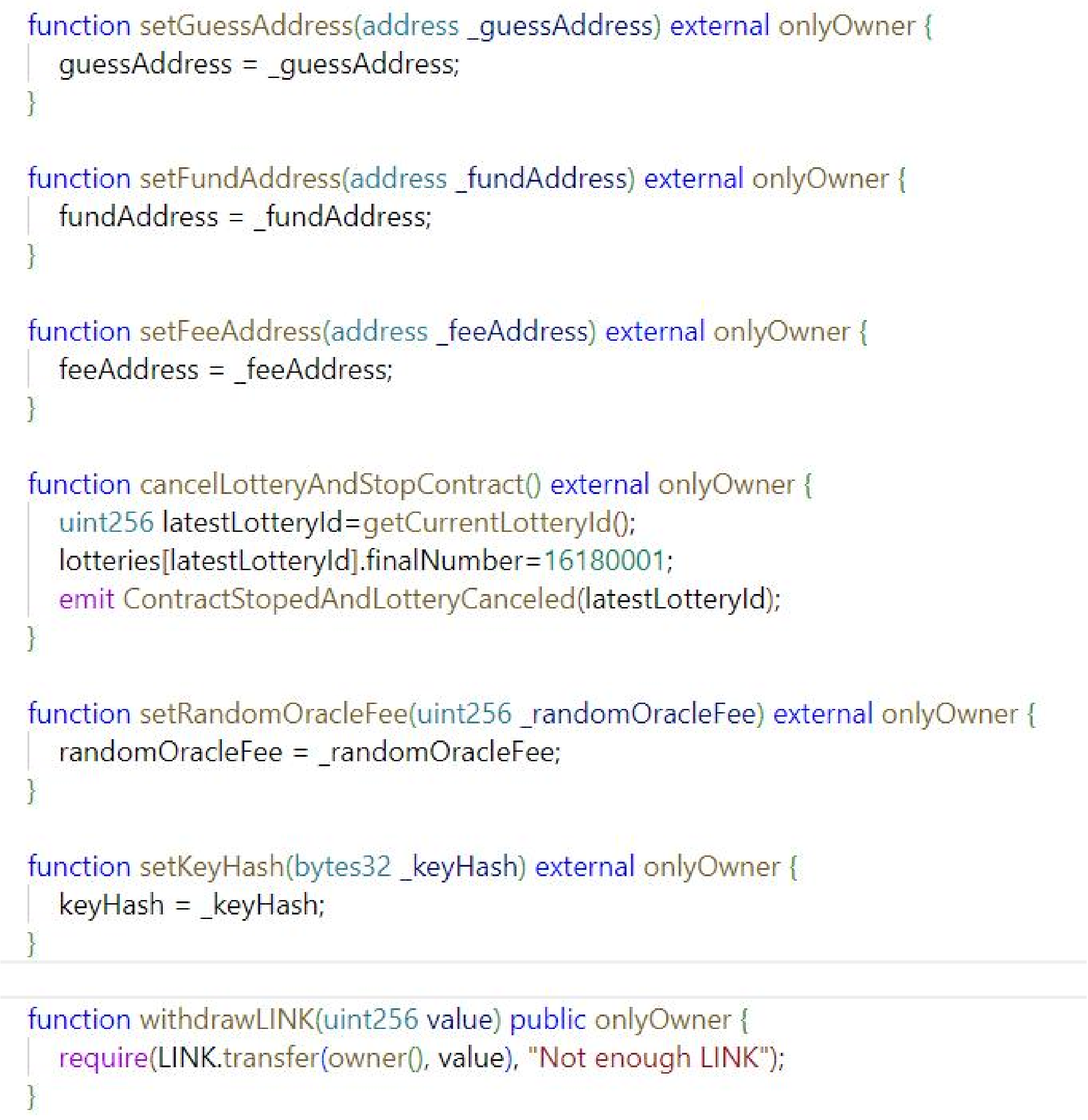
Category: Authority Issues

Likelihood: Medium

Impact: Medium

Description:

As shown in figure 1 below, the contract owner can modify the buy amounts parameters of keys and the payment receiving address. Under certain circumstances, the contract owner can call cancelLotteryAndStopContract() function to pause the buy function through modify the finalNumber of the specified id in "lotteries".



```
function setGuessAddress(address _guessAddress) external onlyOwner {
    guessAddress = _guessAddress;
}

function setFundAddress(address _fundAddress) external onlyOwner {
    fundAddress = _fundAddress;
}

function setFeeAddress(address _feeAddress) external onlyOwner {
    feeAddress = _feeAddress;
}

function cancelLotteryAndStopContract() external onlyOwner {
    uint256 latestLotteryId=getCurrentLotteryId();
    lotteries[latestLotteryId].finalNumber=16180001;
    emit ContractStopedAndLotteryCanceled(latestLotteryId);
}

function setRandomOracleFee(uint256 _randomOracleFee) external onlyOwner {
    randomOracleFee = _randomOracleFee;
}

function setKeyHash(bytes32 _keyHash) external onlyOwner {
    keyHash = _keyHash;
}
```

```
function withdrawLINK(uint256 value) public onlyOwner {
    require(LINK.transfer(owner(), value), "Not enough LINK");
}
```

Figure 1 part of the code

Recommendations:

Numen Cyber Lab recommends to reasonable use of owner permissions.

Result: Pass

Fix Result:

Ignore (After communicating with the project party, this permission is required for the project design and is only used in special circumstances.)

3.2 Centralized risk

ID: NVE-002 Location:GuessChampion.sol

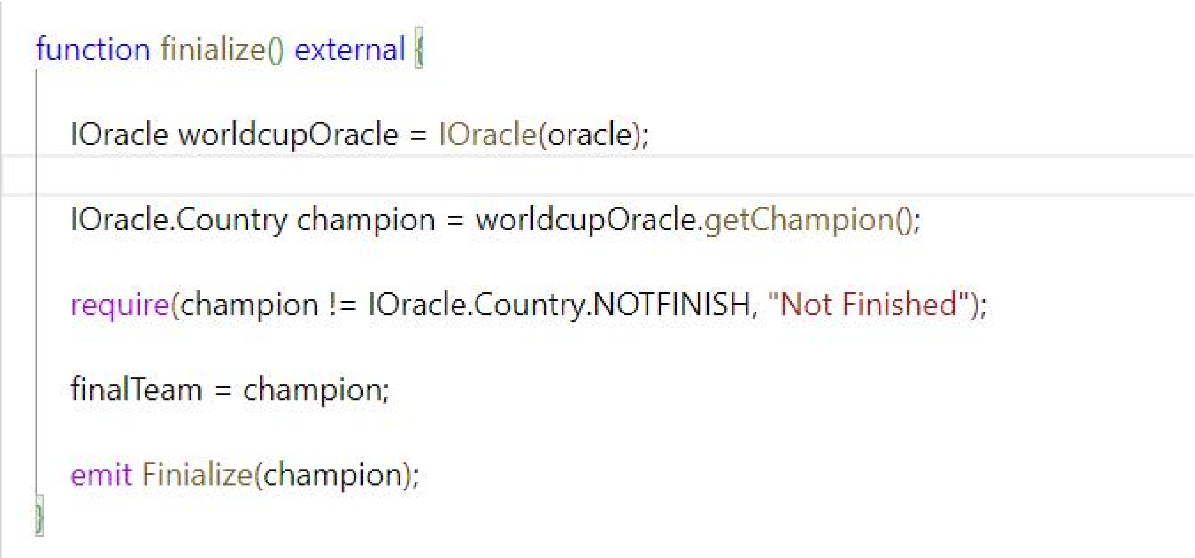
Severity: Medium Category: Oracle Issues

Likelihood: Medium

Impact: Medium

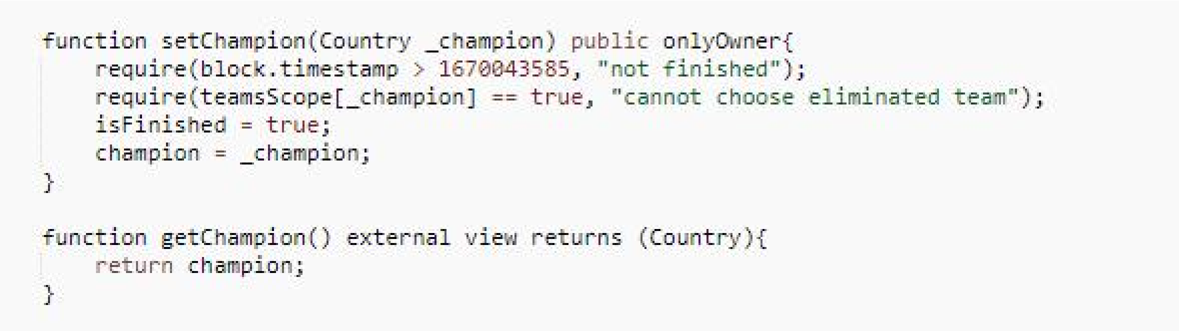
Description:

As shown in Figure 2,3 below, the data of the champion team is obtained from the "getChampion" function in the external "oracle" address. Current "oracle" address is 0xf279963393d7bafb3a67d05b2e129d062a590051. There is a centralization risk that the champion team data is entered by the contract owner after the specified time.



```
function finialize() external {
    IOracle worldcupOracle = IOracle(oracle);
    IOracle.Country champion = worldcupOracle.getChampion();
    require(champion != IOracle.Country.NOTFINISH, "Not Finished");
    finalTeam = champion;
    emit Finialize(champion);
}
```

Figure 2 finialize function



```
function setChampion(Country _champion) public onlyOwner{
    require(block.timestamp > 1670043585, "not finished");
    require(teamsScope[_champion] == true, "cannot choose eliminated team");
    isFinished = true;
    champion = _champion;
}

function getChampion() external view returns (Country){
    return champion;
}
```

Figure 3 getChampion function

Recommendations:

Numen Cyber Lab recommends to the oracle uses a third-party data source or sets the championship team to adopt a multi-signature method.

Result: Pass

Fix Result:

Ignore(After communicating with the oracle party, they will strictly control the use of the contract owner).

4 Conclusion

In this audit, we thoroughly analyzed fomocup smart contract implementation. The problems found are described and explained in detail in Section 3. The problems found in the audit have been brought up to the project party, ignored issues are in line with the project design, and permissions are only used for the project to properly function. We therefore deem the audit result to be a **PASS.** To improve this report, we greatly appreciate any constructive feedbacks or suggestions, on our methodology, audit findings, or potential gaps in scope/coverage.

5 Appendix

5.1 Basic Coding Assessment

5.1.1 Apply Verification Control

- Description: The security of apply verification
- Result: Not found
- Severity: Critical

5.1.2 Authorization Access Control

- Description: Permission checks for external integral functions
- Result: Not found
- Severity: Critical

5.1.3 Forged Transfer Vulnerability

- Description: Assess whether there is a forged transfer notification vulnerability in the contract
- Result: Not found
- Severity: Critical

5.1.4 Transaction Rollback Attack

- Description: Assess whether there is transaction rollback attack vulnerability in the contract.
- Result: Not found
- Severity: Critical

5.1.5 Transaction Block Stuffing Attack

- Description: Assess whether there is transaction blocking attack vulnerability.
- Result: Not found
- Severity: Critical

5.1.6 soft fail Attack Assessment

- Description: Assess whether there is soft fail attack vulnerability.
- Result: Not found
- Severity: Critical

5.1.7 hard fail Attack Assessment

- Description: Examine for hard fail attack vulnerability
- Result: Not found
- Severity: Critical

5.1.8 Abnormal Memo Assessment

- Description: Assess whether there is abnormal memo vulnerability in the contract.
- Result: Not found
- Severity: Critical

5.1.9 Abnormal Resource Consumption

- Description: Examine whether abnormal resource consumption in contract processing.
- Result: Not found
- Severity: Critical

5.1.10 Random Number Security

- Description: Examine whether the code uses insecure random number.
- Result: Not found
- Severity: Critical

5.2 Advanced Code Scrutiny

5.2.1 Cryptography Security

- Description: Examine for weakness in cryptograph implementation.
- Results: Not Found
- Severity: High

5.2.2 Account Permission Control

- Description: Examine permission control issue in the contract
- Results: Not Found
- Severity: Medium

5.2.3 Malicious Code Behaviour

- Description: Examine whether sensitive behaviour present in the code
- Results: Not found
- Severity: Medium

5.2.4 Sensitive Information Disclosure

- Description: Examine whether sensitive information disclosure issue present in the code.
- Result: Not found
- Severity: Medium

5.2.5 System API

- Description: Examine whether system API application issue present in the code
- Results: Not found
- Severity: Low

6 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 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 without Numen'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 considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Numen 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 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.

Blockchain technology and cryptographic assets present a high level of ongoing risk. Numen's position is that each company and individual are responsible for their own due diligence and continuous security. Numen'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.

REFERENCES

[1] MITRE. CWE- 191: Integer Underflow (Wrap or Wraparound). https://cwe.mitre.org/data/ definitions/191.html.

[2] MITRE. CWE- 197: Numeric Truncation Error. https://cwe.mitre.org/data/definitions/197. html.

[3] MITRE. CWE-400: Uncontrolled Resource Consumption. https://cwe.mitre.org/data/ definitions/400.html.

[4] MITRE. CWE-440: Expected Behavior Violation. https://cwe.mitre.org/data/definitions/440. html.

[5] MITRE. CWE-684: Protection Mechanism Failure. https://cwe.mitre.org/data/definitions/ 693.html.

[6] MITRE. CWE CATEGORY: 7PK - Security Features. https://cwe.mitre.org/data/definitions/ 254.html.

[7] MITRE. CWE CATEGORY: Behavioral Problems. https://cwe.mitre.org/data/definitions/438. html.

[8] MITRE. CWE CATEGORY: Numeric Errors. https://cwe.mitre.org/data/definitions/189.html.

[9] MITRE. CWE CATEGORY: Resource Management Errors. https://cwe.mitre.org/data/ definitions/399.html.

[10] OWASP. Risk Rating Methodology. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Numen Cyber Technology Pte. Ltd.

11 North Buona Vista Drive, #04-09,

The Metropolis, Singapore 138589

Tel: 65-63555555

Fax: 65-63666666

Email: sales@numencyber.com

Web: https://numencyber.com