auditace.tech

AuditAce
FROM INCEPTION TO SUCCESS

Smart Contract Audit

FOR

Xmar Token

DATED : 20 November 23'

MANUAL TESTING

Centralization – Owner can blacklist wallets.

Severity: High

function: blacklist

Status: Open

Overview:

The owner can blacklist wallets from transferring tokens for an indefinite period of time
which is not recommended. Which can lock the user's token.

```
function addToBlacklist(address _address) external
onlyOwner {
    _isBlacklisted[_address] = true;
  }
```

Suggestion:

There should be a locking period so that the wallet cannot be locked for an indefinite
Period of time.

MANUAL TESTING

Centralization – Owner can pause the token.

Severity: High

function: _pause

Status: Open

Overview:

The owner can pause the functionality of the contract.

.

```
function _pause() internal virtual whenNotPaused {
    _paused = true;
    emit Paused(_msgSender());
}
```

Suggestion:

There must be a locking period as if the contract is locked in an unlimited period of time, Then no transfer of the token will be possible so it is recommended to add a locking period or just remove the functionality.

AUDIT SUMMARY

Project name – Xmar Token

Date: 20 November 2023

Scope of Audit- Audit Ace was consulted to conduct the smart contract audit of the solidity source codes.

Audit Status: FAILED

Issues Found

Status	Critical	High	Medium	Low	Suggestion
Open	0	2	0	2	0
Acknowledged	0	0	0	0	0
Resolved	0	0	0	0	0

USED TOOLS

Tools:

1- Manual Review:
A line by line code review has been performed by audit ace team.

2- BSC Test Network: All tests were conducted on the BSC Test network, and each test has a corresponding transaction attached to it. These tests can be found in the "Functional Tests" section of the report.

3- Slither :
The code has undergone static analysis using Slither.

Testnet version:
The tests were performed using the contract deployed on the BSC Testnet, which can be found at the following address:
https://testnet.bscscan.com/address/0xa4c3d43ac02df4f24a537637468869b5f88591fd#code

Token Information

Token Address: -
0x85126a231dEe1519E49cE82898eEf09bFdF45Fd5

Name: Xmar Token

Symbol: XT

Decimals: 18

Network: Binance smart chain

Token Type: ERC20

Owner: - 0x97bd0d90a07ab3d169471aaab5e0574c391cdea2

Deployer: -
0x97bd0d90a07ab3d169471aaab5e0574c391cdea2

Token Supply: 10000000000

Checksum: f06ccd36e9e3b2fd838a21fa78925cae

Testnet version:
The tests were performed using the contract deployed on the Binance smart chain Testnet, which can be found at the following address:
https://testnet.bscscan.com/address/0xa4c3d43ac02df4f24a537637468869b5f88591fd#code

TOKEN OVERVIEW

Max tax

Buy : 6%

Sell : 10%

Transfer : 0%

AUDIT METHODOLOGY

The auditing process will follow a routine as special considerations by Auditace:

- Review of the specifications, sources, and instructions provided to Auditace to make sure the contract logic meets the intentions of the client without exposing the user's funds to risk.
- Manual review of the entire codebase by our experts, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
- Specification comparison is the process of checking whether the code does what the specifications, sources, and instructions provided to Auditace describe.
- Test coverage analysis determines whether the test cases are covering the code and how much code isexercised when we run the test cases.
- Symbolic execution is analysing a program to determine what inputs cause each part of a program to execute.
- Reviewing the codebase to improve maintainability, security, and control based on the established industry and academic practices.

VULNERABILITY CHECKLIST

- [x] Return values of low-level calls
- [x] Private modifier
- [x] Multiple Sends
- [x] Using Suicide
- [x] Gas Limitand Loops
- [x] Address hardcoded
- [x] Exception Disorder
- [x] Using inline assembly
- [x] Divide before multiply
- [x] Missing Zero Address Validation
- [x] Compiler version not fixed
- [x] **Gasless Send**
- [x] Using block.timestamp
- [x] Re-entrancy
- [x] Tautology or contradiction
- [x] Timestamp Dependence
- [x] Revert/require functions
- [x] Use of tx.origin
- [x] Integer overflow/underflow
- [x] Dangerous strict equalities
- [x] Using SHA3
- [x] Using throw

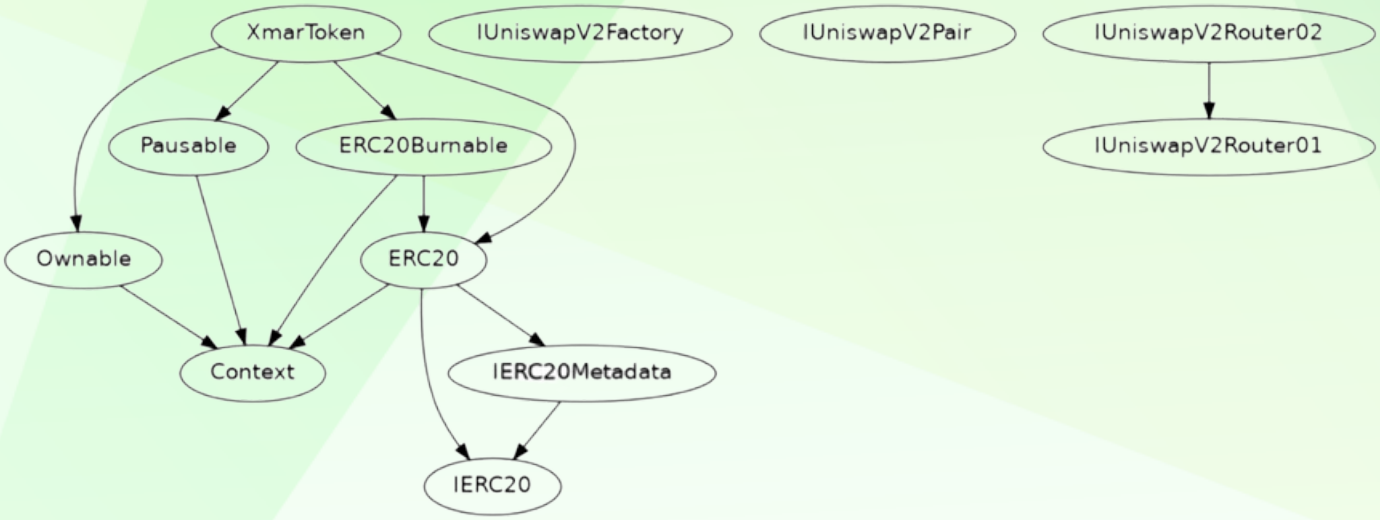
CLASSIFICATION OF RISK

Severity	Description
Critical	These vulnerabilities could be exploited easily and can lead to asset loss, data loss, asset, or data manipulation. They should be fixed right away.
High-Risk	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.
Medium-Risk	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.
Low-Risk	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.
Gas Optimization /Suggestion	A vulnerability that has an informational character but is not affecting any of the code.

Findings

Severity	Found
Critical	0
High-Risk	2
Medium-Risk	0
Low-Risk	2
Gas Optimization / Suggestions	0

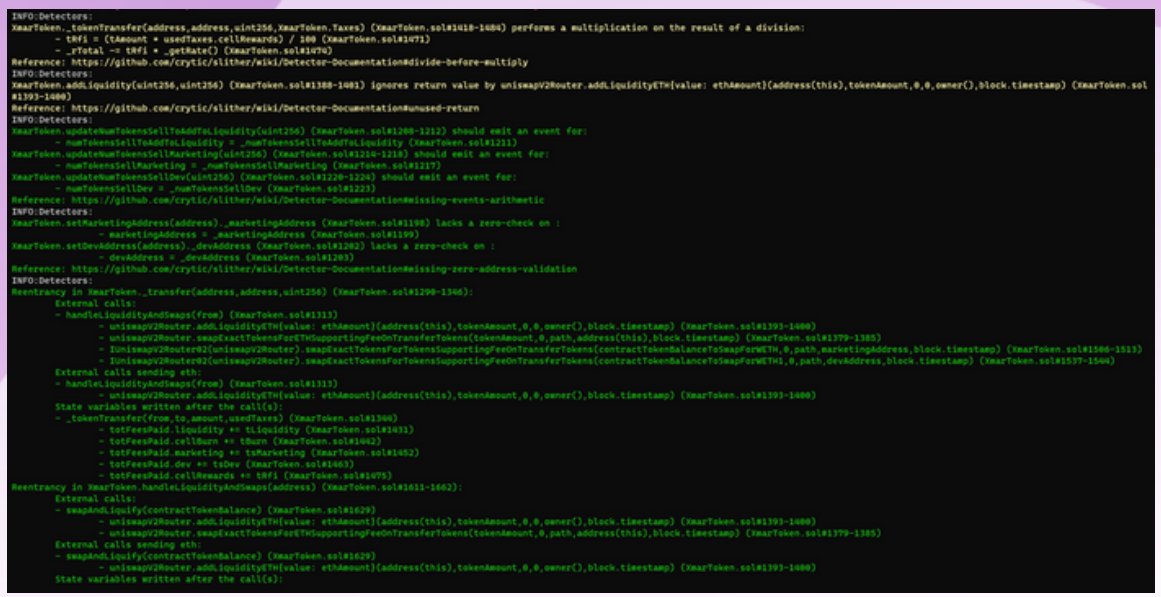
INHERITANCE TREE

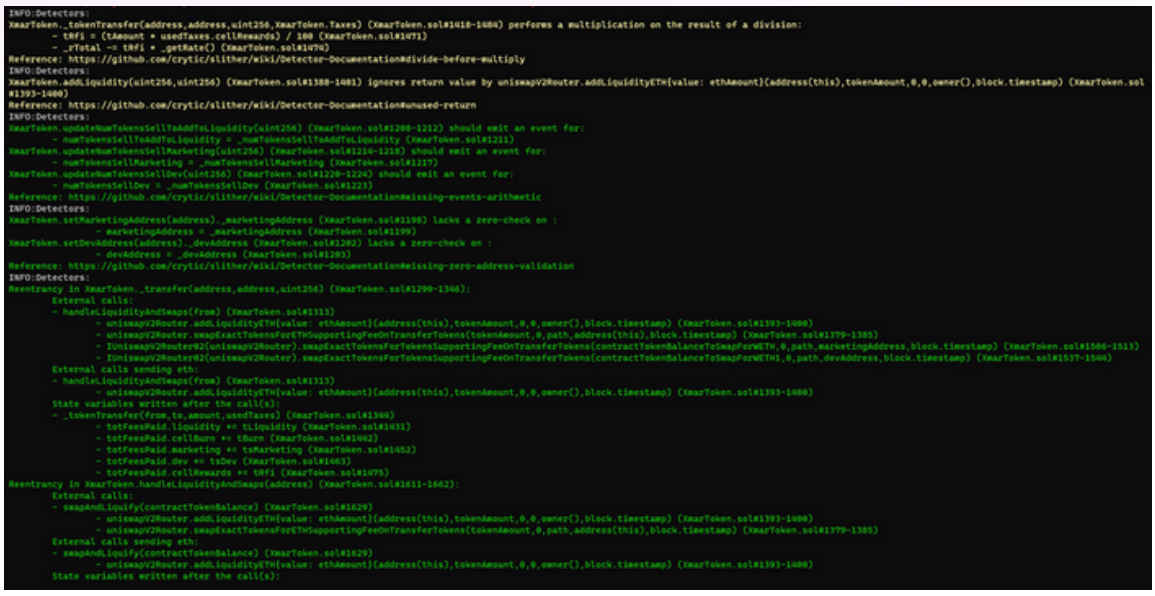


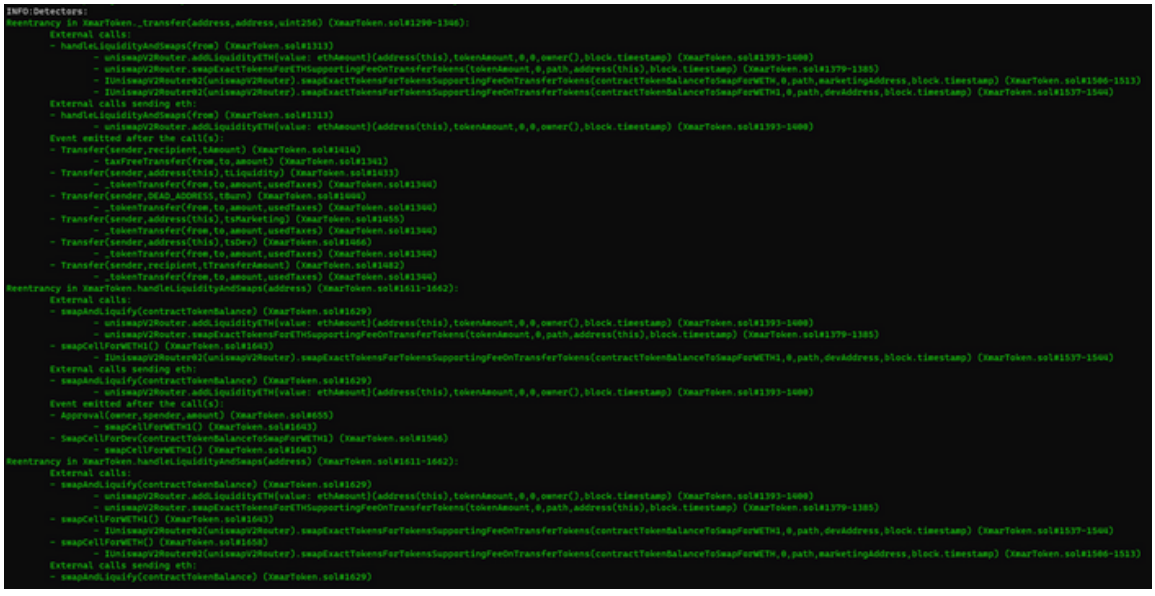
POINTS TO NOTE

- Owner can blacklist wallets
- Owner can enable/disable trade status
- Owner can set marketing wallet address,
- Dev wallet address

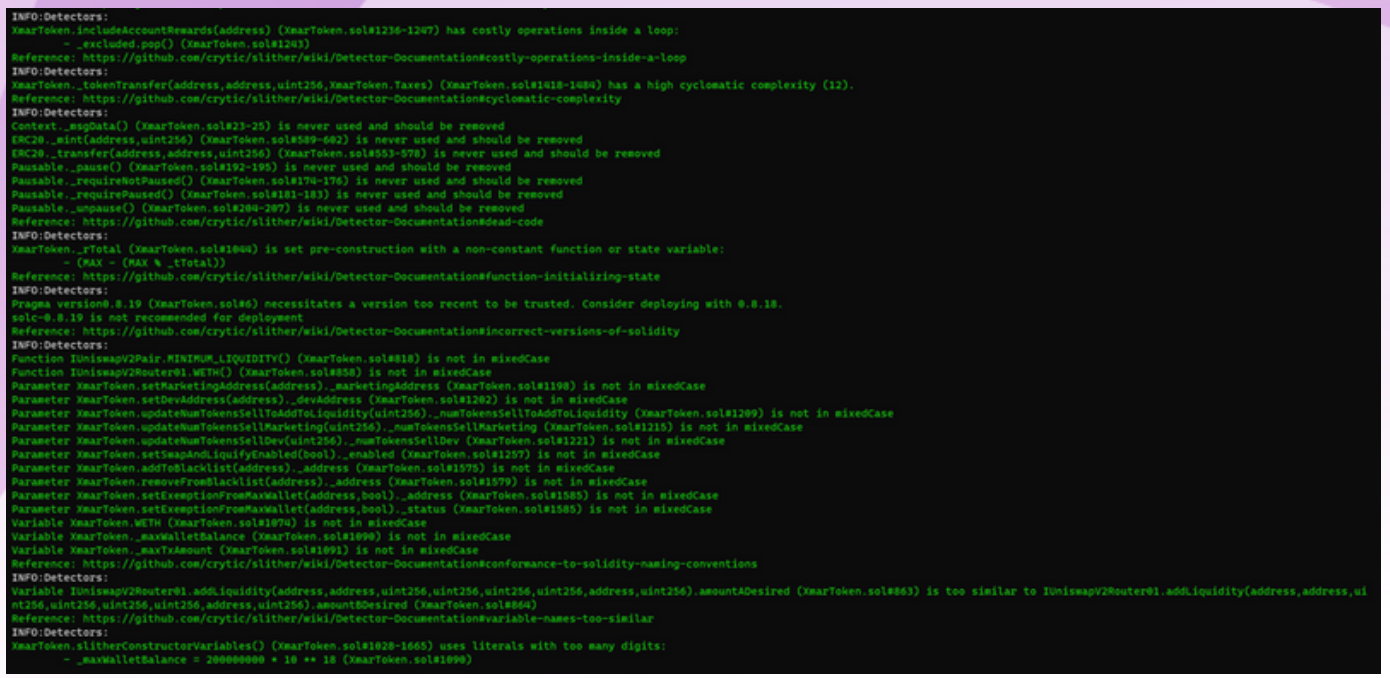
STATIC ANALYSIS

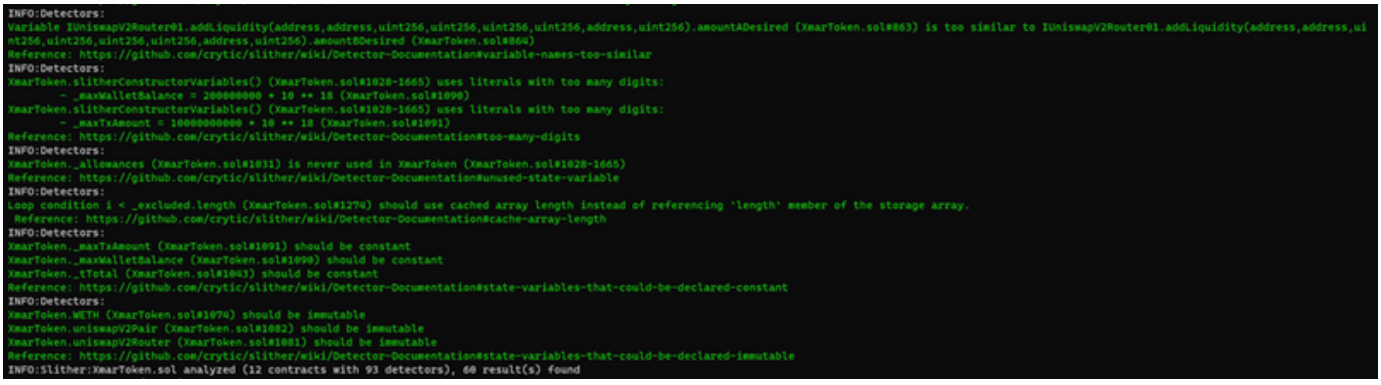






STATIC ANALYSIS





Result => A static analysis of contract's source code has been performed using slither,

No major issues were found in the output

FUNCTIONAL TESTING

1- Add To Blacklist (passed):

https://testnet.bscscan.com/tx/0x7cb8aef4e1765b007f78daaf5bb5b573f675aa102dd88c375d0007667bf13dec

2- Approve (passed):

https://testnet.bscscan.com/tx/0xde41a456adf0ae616d1e82588106bc2099cfd5cb2bedd5dc6375be2e31a8ceba

3- Increase Allowance (passed):

https://testnet.bscscan.com/tx/0x00e972acd01a32391d7ee1c8627c627b0c4755a46558a598ce321d810f55a8ee

4- Decrease Allowance (passed):

https://testnet.bscscan.com/tx/0x4c694efec1d0cd4785d8c2582e3689ca653a51dda45f3589612988eb84450062

5- Set Dev Address (passed):

https://testnet.bscscan.com/tx/0x86634a816a67d6c96cf0c61589cf229c1071417d3eaf566901ed8802df79f6fe

6- Set Marketing Address (passed):

https://testnet.bscscan.com/tx/0x321891d9fc44fe55277a33dbd53cf0dafe81f32d956660b738af8944f23a03b2

7- Remove From Blacklist (passed):

https://testnet.bscscan.com/tx/0xc0ac8d8284069306b33993248da5cba677e81dd20ff9da6317d9c52b6516383c

8- Renounce Ownership(passed):

https://testnet.bscscan.com/tx/0x7ce7cac2abae74c41bf6797728d4e25bfe6f05db63e3906c46892cec7d84de87

MANUAL TESTING

Centralization – Owner can blacklist wallets.

Severity: High

function: blacklist

Status: Open

Overview:

The owner can blacklist wallets from transferring tokens for an indefinite period of time
which is not recommended. Which can lock the user's token.

```
function addToBlacklist(address _address) external
onlyOwner {
    _isBlacklisted[_address] = true;
  }
```

Suggestion:

There should be a locking period so that the wallet cannot be locked for an indefinite
Period of time.

MANUAL TESTING

Centralization – Owner can pause the token.

Severity: High

function: _pause

Status: Open

Overview:

The owner can pause the functionality of the contract.

.

```
function _pause() internal virtual whenNotPaused {
    _paused = true;
    emit Paused(_msgSender());
}
```

Suggestion:

There must be a locking period as if the contract is locked in an unlimited period of time, Then no transfer of the token will be possible so it is recommended to add a locking period or just remove the functionality.

MANUAL TESTING

Centralization – Missing Zero Address

Severity: Low

function: setMarketingAddress/setDevAddress

Status: Open

Overview:

functions can take a zero address as a parameter (0x00000...). If a function parameter of address type is not properly validated by checking for zero addresses, there could be serious consequences for the contract's functionality.

```
function setMarketingAddress(address _marketingAddress) external onlyOwner {
    marketingAddress = _marketingAddress;
  }
function setDevAddress(address _devAddress) external onlyOwner {
    devAddress = _devAddress;
  }
```

Suggestion:

It is suggested that the address should not be zero or dead.

MANUAL TESTING

Optimization

Severity: Low

subject: Missing Events

Status: Open

Overview:

They serve as a mechanism for emitting and recording data onto the blockchain, making it
transparent and easily accessible.

```
function setMarketingAddress(address _marketingAddress)
external onlyOwner {
    marketingAddress = _marketingAddress;
  }
function setDevAddress(address _devAddress) external
onlyOwner {
    devAddress = _devAddress;
  }
```

Suggestion:

Add an event to these important functions where address updation is happening. This can also be marked as an indexed event for better off-chain tracking.

DISCLAIMER

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment. Team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Always Do your own research and protect yourselves from being scammed. The Auditace team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools. Under no circumstances did Auditace receive a payment to manipulate those results or change the awarding badge that we will be adding in our website. Always Do your own research and protect yourselves from scams. This document should not be presented as a reason to buy or not buy any particular token. The Auditace team disclaims any liability for the resulting losses.

ABOUT AUDITACE

We specializes in providing thorough and reliable audits for Web3 projects. With a team of experienced professionals, we use cutting-edge technology and rigorous methodologies to evaluate the security and integrity of blockchain systems. We are committed to helping our clients ensure the safety and transparency of their digital assets and transactions.

https://auditace.tech/

https://t.me/Audit_Ace

https://twitter.com/auditace_

https://github.com/Audit-Ace