

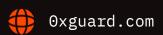
# Smart contracts security assessment

Final report

[ariff: Standard

# **PSYOPTRON**

September 2024





# Contents

1.	Introduction	3
2.	Contracts checked	3
3.	Procedure	3
4.	Known vulnerabilities checked	4
5.	Classification of issue severity	5
6.	Issues	5
7.	Conclusion	7
8.	Disclaimer	8

Ox Guard

## □ Introduction

In accordance with the Memtember initiative, the PSYOPTRON project was selected and subjected to an audit. The Memtember campaign, designed to foster innovation and community engagement within the blockchain ecosystem, sought to identify promising projects that align with the initiative's core values.

The PSYOPTRON is standard ERC20 token implemented with OpenZeppelin library which is considered as a best practice. After deployment transfers are blocked. The owner of the contract may allow transfers to and from owner account and open transfers for all token holders. Once transfers are open for all holders, transfer restrictions can't be set back.

Name	PSYOPTRON	
Audit date	2024-09-06 - 2024-09-06	
Language	Solidity	
Platform	TRON	

## Contracts checked

Name	Address
Token	TBFr8v7HkKGydiHAjDL8NzqYf7cJqNsTVY

## Procedure

We perform our audit according to the following procedure:

#### **Automated analysis**

- Scanning the project's smart contracts with several publicly available automated Solidity analysis tools
- Manual verification (reject or confirm) all the issues found by the tools

Ox Guard | September 2024

#### **Manual audit**

- Manually analyze smart contracts for security vulnerabilities
- Smart contracts' logic check

# ▼ Known vulnerabilities checked

Title	Check result
Unencrypted Private Data On-Chain	passed
Code With No Effects	passed
Message call with hardcoded gas amount	passed
Typographical Error	passed
DoS With Block Gas Limit	passed
Presence of unused variables	passed
Incorrect Inheritance Order	passed
Requirement Violation	passed
Weak Sources of Randomness from Chain  Attributes	passed
Shadowing State Variables	passed
Incorrect Constructor Name	passed
Block values as a proxy for time	passed
Authorization through tx.origin	passed
DoS with Failed Call	passed
Delegatecall to Untrusted Callee	passed
Use of Deprecated Solidity Functions	passed
Assert Violation	passed
State Variable Default Visibility	passed

Ox Guard

September 2024

Reentrancy passed Unprotected SELFDESTRUCT Instruction passed **Unprotected Ether Withdrawal** passed Unchecked Call Return Value passed Floating Pragma passed **Outdated Compiler Version** passed Integer Overflow and Underflow passed **Function Default Visibility** passed

# Classification of issue severity

**High severity** High severity issues can cause a significant or full loss of funds, change

of contract ownership, major interference with contract logic. Such issues

require immediate attention.

**Medium severity** Medium severity issues do not pose an immediate risk, but can be

detrimental to the client's reputation if exploited. Medium severity issues may lead to a contract failure and can be fixed by modifying the contract

state or redeployment. Such issues require attention.

**Low severity** Low severity issues do not cause significant destruction to the contract's

functionality. Such issues are recommended to be taken into

consideration.

## Issues



September 2024

### **High severity issues**

#### No issues were found

**Medium severity issues** 

#### No issues were found

Low severity issues

#### 1. Lack of events (Token)

Status: Open

The function setMode() changes token transfer restrictions but does not emit any events.

```
function setMode(uint v) public onlyOwner {
   if (_mode != MODE_NORMAL) {
      _mode = v;
   }
}
```

**Recommendation:** Create and emit event SetMode (uint mode) in the function.

# **○** Conclusion

PSYOPTRON Token contract was audited. 1 low severity issue was found.

○x Guard | September 2024 7

## 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 0xGuard 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 0xGuard 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.

OxGuard retains exclusive publishing rights for the results of this audit on its website and social networks.

○x Guard | September 2024 8



