

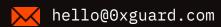
Smart contracts security assessment

Final report ariff: Standard

PulseAXE

July 2023





Contents

1.	Introduction	3
2.	Contracts checked	3
3.	Procedure	4
4.	Known vulnerabilities checked	4
5.	Classification of issue severity	5
6.	Issues	6
7.	Conclusion	8
8.	Disclaimer	9

Ox Guard

July 2023

2

Introduction

The report has been prepared for **PulseAXE**.

The PulseAXE project is a Tomb Finance fork, allowing users to acquire AXE and share CHOP tokens. Both AXE and CHOP tokens are ERC20 standard tokens with transfer tax up to 40%. AXE has privileged account allowed to mint.

RewardPool contract may charge a fee of up to 4% for each deposit.

The code is available at the @PulseAXEcom/contracts_v3 Github repo and was audited in the 26ebd8e commit.

The updated code was rechecked after the commit <u>fc6bfea</u>.

Name	PulseAXE	
Audit date	2023-07-19 - 2023-07-22	
Language	Solidity	
Platform	Pulse Chain	

Contracts checked

Name	Address
AXE.sol	

CHOP.sol

MAUL.sol

Masonry.sol

RewardPool.sol

Treasury.sol

Oracle.sol

Centralization risks

⊙x Guard July 2023 3

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

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

Ox Guard | July 2023 4

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 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.

Ox Guard | July 2023

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

High severity issues

1. Owner capabilities (Centralization risks)

Status: Partially fixed

The project is fully centralized.

AXE token is open for minting by operator account, which is assigned by the owner, other contracts are highly dependent on the owner's account.

Recommendation: Renounce ownership wherever possible and/or secure owner's account.

Team comment: Contracts will be renounced right after ensuring the smooth launch of the protocol.

Medium severity issues

1. Sell tax increase is avoidable (AXE.sol)

Status: Fixed

Sell tax percent is increased from 2.5% up to 40% based on AXE de-peg in Uniswap-like pair, see more in Oracle contract section. Since pair reserves can be manipulated, tax percent increase may be avoided.

```
function _transfer(
    address sender,
    address recipient,
    uint256 amount
) internal override {
    if (automatedMarketMakerPairs[recipient]) {
        uint256 _fee = basicSellFee;
}
```

Ox Guard | July 2023

```
uint256 _axeCurrentPrice = twap();
while (_axeCurrentPrice < axePriceOne) {
    __fee = _fee.mul(2);
    __axeCurrentPrice = _axeCurrentPrice.add(5 * 10 ** 16);
}
if (_fee > maxSellFee) _fee = maxSellFee;
uint256 _feeAmount = amount.mul(_fee).div(1000);
amount = amount.sub(_feeAmount);
super._transfer(sender, communityFund, _feeAmount);
}
super._transfer(sender, recipient, amount);
}
function twap() public view returns (uint256 _amountOut) {
    return IOracle(oracle).twap(address(this), 1e18);
}
```

Recommendation: Fix the Oracle.

2. Sell tax increase is avoidable (CHOP.sol)

Status: Fixed

Sell tax implementation is identical to the AXE contract. Tax percent increase may be avoided.

Recommendation: Fix the Oracle.

Low severity issues

No issues were found

○ Conclusion

PulseAXE AXE.sol, CHOP.sol, MAUL.sol, Masonry.sol, RewardPool.sol, Treasury.sol, Oracle.sol, Centralization risks contracts were audited. 1 high, 2 medium severity issues were found.

2 medium severity issues have been fixed in the update.

⊙x Guard | July 2023 8

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.

○x Guard | July 2023 9



