



SMART CONTRACT SECURITY AUDIT

WATCHTOWER

DISCLAIMER

Watchtower has completed this report to provide a summary of the Smart Contract functions, and any security, dependency or cybersecurity vulnerabilities. This is often a constrained report on our discoveries based on our investigation and understanding of the current programming versions as at the date of this report. In order to understand the full scope of our analysis, it is vital for you to review the complete report. Although we have done our best in conducting our investigation and creating this report, it is vital to note that you should not depend on this report and cannot make any claim against Watchtower or its Subsidiaries and Team members on the premise of what has or has not been included in the report. Please remember to conduct your own independent examinations before making any investment choices. We do not provide investment advice or in any way claim to determine if the project will be successful or not.

DISCLAIMER: By perusing this report or any portion of it, you concur to the terms of this disclaimer. In the unlikely situation where you do not concur to the terms, you should immediately terminate reading this report, and erase and discard any and all duplicates of this report downloaded and/or printed by you. This report is given for data purposes as it were and on a non-reliance premise, and does not constitute speculation counsel. No one should have any right to depend on the report or its substance, and Watchtower and its members (including holding companies, shareholders, backups, representatives, chiefs, officers and other agents) Watchtower and its subsidiaries owe no obligation of care towards you or any other person, nor does Watchtower make any guarantee or representation to any individual on the precision or completeness of the report.

ABOUT THE AUDITOR:

Watchtower is an Anti-Scam Token Utility which reviews Smart Contracts and Token information to Identify Rug Pull and Honey Pot scamming activity.

Watchtowers Development Team consists of a number of Smart Contract creators, Auditors Developers and Blockchain experts.

Watchtowers Website Scanner reviews a number of Risk factors to provide an adequate Risk summary of token projects.

In Addition to this the team also helps with Creation of Smart Contracts for legitimate projects, Audits and Promotion.





OVERVIEW

Watchtower was commissioned by Pecunia to complete a Smart Contract audit.

The objective of the Audit is to achieve the following:

- Review the Project and experience and Development team
- Ensure that the Smart Contract functions are necessary and operate as intended.
- Identify any vulnerabilities in the Smart Contract code.

DISCLAIMER: This Audit is intended to inform about token Contract Risks, the result does not imply an endorsement or provide financial advice in any way, All investments are made at your own risk.

(<https://www.cryptowatchtower.io/>)



SMART CONTRACT REVIEW



Contract Created on the 09th September 2021

Contract name	Pecunia
Contract address	0x33837Ad88d3488020F140996dcBD44E7eebe8fD4
Total supply	1,000,000,000,000
Token ticker	PEC
Decimals	9
Token holders	826
Transactions count	5089
Top 5 holders dominance	19.93% / 28.48% Burn Adjusted
Tax fee	10%
Total fees	10% ~ BUY / SELL
Contract deployer address	0xede0399a15320ce5bb7c2d90ba30a6a6f03e8251
Contract's current owner address	0xede0399a15320ce5bb7c2d90ba30a6a6f03e8251



Project Overview

Project Details: (From Project Website)

Our goal is above all to represent an environment within the crypto space which serves as a connection between blockchain technology and real-time investments. We want to make it possible for everyone who is interested to invest in funding pools for bigger deals and be able to share a part of the profits.

Tokenomics:

Starting Supply: 1,000,000,000,000 (1 Trillion)

10% Tax for Buys and Sells comprising of:

1% Charity Fee

4% Liquidity Fee

3% Marketing Fee

2% Reflections/Rewards of Native token to holders

Team Doxxed:

The Pecunia team has been doxxed and their profiles are available on their website:

<https://pecuniacrypto.com/>



CONTRACT FUNCTIONS DETAILS

Functions (Public)

This contract has 20 available public functions which the owner can call.

These functions were reviewed and can be viewed on BSC Scan or through a DAPP.

LINK

<https://www.bscscan.com/address/0x33837Ad88d3488020F140996dcBD44E7eebe8fD4#writeContract>

Function risks: No Scam Functions Identified!

- Tax fees can be increased to high levels making it harder to sell, which is quite normal with Rewards contracts.
- Watchtower believes the Pecunia owners are operating with honesty as there are no alternate methods of scamming such as a mint function.



Contract Stress Test

Imported Libraries / Interfaces

- IERC20
- SafeMath
- Context
- Address
- Ownable
- IUniswapV2Factory
- IUniswapV2Pair
- IUniswapV2Router01
- IUniswapV2Router02

Overview

1. ADDITION OF COMMENTS:	8
2. CALL STACK DEPTH ATTACK:	10
3. TIME STAMP DEPENDENCY:	10
4. PARTY MULTISIG BUG:	10
5. USE OF LIBRARIES/DEPENDENCIES (FROM TRUSTED SOURCES):	8
a. TRANSACTION-ORDERING DEPENDENCY:	10
6. ACCESS CONTROL AND AUTHORIZATION:	10
7. REENTRANCY ATTACKS:	10
8. ERC/BEP STANDARD VIOLATIONS:	10
9. USAGE OF VISIBILITY LEVELS:	10



ISSUES CHECKING STATUS



Issue description	Checking status
1. Compiler errors.	Passed
2. Race conditions and Reentrancy. Cross-function race conditions.	Passed
3. Possible delays in data delivery.	Passed
4. Oracle calls.	Passed
5. Front running.	Passed
6. Timestamp dependence.	Passed
7. Integer Overflow and Underflow.	Passed
8. DoS with Revert.	Passed
9. DoS with block gas limit.	Passed
10. Methods execution permissions.	Passed



Issue description	Checking status
11. Economy model of the contract.	Passed
12. The impact of the exchange rate on the logic.	Passed
13. Private user data leaks.	Passed
14. Malicious Event log.	Passed
15. Scoping and Declarations.	Passed
16. Uninitialized storage pointers.	Passed
17. Arithmetic accuracy.	Passed
18. Design Logic.	Passed
19. Cross-function race conditions.	Passed
20. Safe Open Zeppelin contracts implementation and usage.	Passed
21. Fallback function security.	Passed



SECURITY ISSUES



High Severity Issues

- `_getTValues()` has an error in `tTransferAmount` calculation:

```
function _getTValues(uint256 tAmount) private view returns (uint256, uint256, uint256) {  
    uint256 tFee = calcTaxFee(tAmount);  
    uint256 tLiquidity = calculateLiquidityFee(tAmount);  
    uint256 tTransferAmount = tAmount.sub(tFee);  
    return (tTransferAmount, tFee, tLiquidity);
```

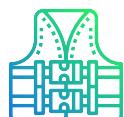


Medium Severity Issues

- **numTokensSellToAddToLiquidity** is set to **500,000,000,000** and it could cause a dump.
- **Immutable router address:** Router address can't be changed. If pancakeswap will release V3, the contracts main features will be useless.
- **Gas Efficiency:** `removeAllFees()` doesn't check if `_charityFee` and `_marketingFee` are 0. This could cause a waste of gas to set all the fees to 0.



SECURITY ISSUES (CONT)



Low Severity Issues

- **Gas Efficiency:**

When the contract enters the branch else if (!_isExcluded[sender] && !_isExcluded[recipient]), the contract will execute the same piece of code _transferStandard(sender, recipient, amount) We recommend removing the following code:

- else if (!_isExcluded[sender] && !_isExcluded[recipient]) {
 _transferStandard(sender, recipient, amount);
- **Line 917: Typo Error** —> tokensIntoLiquidity (instead of tokensIntoLiquidity)
- **Line 1020-1022: Wrong usage of if-else statements.** The else include the situation represented in the first else if
- **Unused function:** There are two _transferTokens(). One is never used.



CONCLUSION

Watchtower reviewed Pecunias' deployed and verified contract to conduct this audit. Watchtower is satisfied that the team is operating with integrity however as noted above there are a number of gas efficiency errors and if pancake swap changes routers some of the functions of the contract will fail.

Watchtower Disclaimer:

Please check the disclaimer page and note, this Audit is intended to inform about token Contract Risks, the result does not imply an endorsement or in any way provide financial advice, please do your own research. By reading this report you accept and agree to the disclaimer and understand investments are made at your own risk.
(<https://www.cryptowatchtower.io/>)

Contact Us

-  @Watchtower_WTW
-  Watchtower-WTW
-  Watchtowercrypto

