



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 Obsidium 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 22nd October 2021

Solidity compiler v0.8.4

Contract name	Obsidium
Contract address	0xc6f509274fcc1f485644167cb911fd0c61545e6c
Total supply	14,500,000
Token ticker	OBS
Decimals	18
Token holders	2
Transactions count	4
Top 5 holders dominance	NOT LAUNCHED
Tax fee	6%
Total fees	0% ~ BUY / 6% ~ SELL (For the first 6 months Only)
Contract deployer address	0x436b5742d34d76a501cc4d2ea71a78f37bc9171b
Contract's current owner address	0x436b5742d34d76a501cc4d2ea71a78f37bc9171b



Project Overview



Project Details: (Website: <https://obsidium.info/>)

Obsidium is an ecosystem serverless, cross-chain, layer-2 solution that fuel the crypto space with DeFi, AAM & NFTs. Its benefits include infinite scalability, high throughput sub-second confirmation time, and fees at a tenth of a cent. Obsidium (\$OBS) was created to develop the concept of “Zero Initial Supply”.

Tokenomics:

Starting Supply: 14,500,000 (14.5 Million)

0% Tax for Buys and 6% for Sells comprising of:

4.5% Liquidity

1% Marketing

0.5% Buyback

Team Review:

Watchtower reviewed a number of factors including the teams background and Cryptocurrency experience, social media interaction and availability, project momentum, token risks and community trust score.

The Obsidium clearly have some expert devs behind their project.

Their platform is proposing a number of large scale utilities.

Obsidium is proposing to build an 4D scanning app to empower anyone to register real assets into the blockchain technology which can then be virtually registered or tokenised. We have not seen any proof of the platform but if it is true then it could be a large scale project.

TEAM DOXXED:

The website shows a leadership section which has not been updated yet and the team have advised they are looking to dox themselves in the future but are not doxxed yet.



CONTRACT FUNCTIONS DETAILS

Functions (Public)

This contract has 19 available public functions which the owner can call. These functions were identified to be safe and can be viewed on BSC Scan or through a DAPP.

LINK:

<https://bscscan.com/token/0xc6f509274fcc1f485644167cb911fd0c61545e6c#writeContract>

Function risks:

-No Scam Functions Identified!



Contract Stress Test

Imported Libraries / Interfaces

- Context
- IBEP20
- IUniswapV2Factory
- IUniswapV2Router02
- Ownable
- SafeMath

Overview

1. ADDITION OF COMMENTS:	10
2. CALL STACK DEPTH ATTACK:	10
3. TIME STAMP DEPENDENCY:	10
4. PARTY MULTISIG BUG:	10
5. USE OF LIBRARIES/DEPENDENCIES (FROM TRUSTED SOURCES):	10
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

Coding Error:

`_tokenSold[from]` is updated before the `require` statement. It should be updated only after the `require` check! Also, in the `else` section, the `_tokenSold[from]` should be equal to the amount that is being sold, not 0.

This means that the Max sell function may fail.



Medium Severity Issues

Internal Swap tokenomics of Marketing and Buy back have slight math deficiencies but this will not affect holders.

Contract has been deployed and tested through simulations and the tax fees (6%) was accurate for holders.

BNB Stuck in Contract:

`contractBalanceSend()` allows the owner to withdraw all except 0.1 BNB from the contract balance. (Not Liquidity) This means that 0.01 BNB will remain stuck in the contract forever.

Centralisation Risk:

Owner can set `_maxSoldAmount` to 0 and block all sell transactions.



CONCLUSION

Watchtower reviewed Obsidiums' deployed and verified contract to conduct this audit.

Watchtower is satisfied that the contract has no malicious coding.

The owner does have privileges and caution is still required.

The team is using Pinksale Finance to launch their token and pre-sale. Pinksale have been verified to focus on Safe launches with Anti-sniper functions and token distribution criteria.

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

