



Smart Contract Security Audit

Project: UltramanBSC

Aug 17, 2022



Contract Address

0x72933BC0Fd746E262Fc4d8967536502B029ed013

Table of Contents

- 1 Disclaimer**
- 2 Audit Review**
- 3 Project Review**
- 4 Smart Contract Vulnerability Checks**
- 5 Manual Code Review**
- 6 Owner Privileges**
 - 6.1 Contract Ownership
 - 6.2 Liquidity Overview
- 7 Tokenomics**
- 8 Social Media Check**
- 9 Website Review**
- 10 Audit Conclusion**

Disclaimer

The contents of this report reflect only the CRACKEN TECH audit team's understanding of the current progress and status of the security of the code audited, to verify the integrity of the code provided for the scope of this audit. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. Given the size of the project, the findings detailed here are not to be considered exhaustive, and further testing and audit are recommended after the issues covered are fixed. We do not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report.

The review does not address the compiler layer, any other areas beyond the programming language, or other programming aspects that could present security risks. If the audited source files are smart contract files, risks or issues introduced by using data feeds from off-chain sources are not extended by this review either.

Audit Review

The source code of the UltramanBSC was audited in order to acquire a clear impression of how the project was implemented. The Cracken Tech audit team conducted in-depth research, analysis, and scrutiny, resulting in a series of observations. A detailed list of each issue found, and vulnerabilities in the source code will be included in the audit report. The problems and potential solutions are given in this report, we will identify common sources for such problems and comments for improvement.

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

- Review of the specifications, sources, and instructions provided to Cracken 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 Cracken describe.
- Test coverage analysis determines whether the test cases are covering the code and how much code is exercised when we run the test cases.
- Symbolic execution is analyzing 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.

Project Review

Token Summary

| Parameter | Result |
|------------------------|--|
| Token Name | UltramanBSC |
| Token Symbol | UTM |
| Token Decimal | 9 |
| Total Supply | 100,000,000 |
| Platform | BSC |
| Buy Tax Fee | 3% |
| Sell Tax Fee | 3% |
| Contract Creation Date | Aug 16, 2022 |
| Liquidity Status | Not Available |
| Liquidity Lockup Time | Not Available |
| Compiler Version | v0.8.15+commit.e14f2714 |
| Optimization | Yes with 200 runs |
| Contract Address | 0x72933BC0Fd746E262Fc4d8967536502B029ed013 |
| Deployer Address | 0x0aa4c3DE9E4e249E207fDef957eD208312230920 |
| Owner Address | 0x0aa4c3DE9E4e249E207fDef957eD208312230920 |

Source Code

CRACKEN was commissioned by UltramanBSC to perform an audit based on the following smart contract:

<https://bscscan.com/address/0x72933BC0Fd746E262Fc4d8967536502B029ed013>

Smart Contract Vulnerability Checks





| Vulnerability | Auto-Scan | Manual-Scan | Result |
|---|-----------|-------------|---------------|
| Unencrypted Private Data On-Chain | Complete | Complete | Low / No Risk |
| Code With No Effects | Complete | Complete | Low / No Risk |
| Message call with hardcoded gas amount | Complete | Complete | Low / No Risk |
| Hash Collisions with Multiple Variable Length Arguments | Complete | Complete | Low / No Risk |
| Unexpected Ether balance | Complete | Complete | Low / No Risk |
| Presence of unused variables | Complete | Complete | Low / No Risk |
| Right-To-Left-Override control character (U+202E) | Complete | Complete | Low / No Risk |
| Typographical Error | Complete | Complete | Low / No Risk |
| DoS With Block Gas Limit | Complete | Complete | Low / No Risk |
| Arbitrary Jump with Function Type Variable | Complete | Complete | Low / No Risk |
| Insufficient Gas Grieving | Complete | Complete | Low / No Risk |
| Incorrect Inheritance Order | Complete | Complete | Low / No Risk |
| Write to Arbitrary Storage Location | Complete | Complete | Low / No Risk |
| Requirement Violation | Complete | Complete | Low / No Risk |
| Missing Protection against Signature Replay Attacks | Complete | Complete | Low / No Risk |
| Weak Sources of Randomness from Chain Attributes | Complete | Complete | Low / No Risk |
| Authorization through tx. origin | Complete | Complete | Low / No Risk |
| Delegate call to Untrusted Callee | Complete | Complete | Low / No Risk |







| Vulnerability | Auto-Scan | Manual-Scan | Result |
|---------------------------------------|-----------|-------------|---------------|
| Use of Deprecated Solidity Functions | Complete | Complete | Low / No Risk |
| Assert Violation | Complete | Complete | Low / No Risk |
| Reentrancy | Complete | Complete | Low / No Risk |
| Unprotected SELF-DESTRUCT Instruction | Complete | Complete | Low / No Risk |
| Unprotected Ether Withdrawal | Complete | Complete | Low / No Risk |
| Outdated Compiler Version | Complete | Complete | Low / No Risk |
| Integer Overflow and Underflow | Complete | Complete | Low / No Risk |
| Function Default Visibility | Complete | Complete | Low / No Risk |

Manual Code Review

Classification of Issues

| Severity | Description |
|---|---|
|  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. |
|  Informational | A vulnerability that has an informational character but is not affecting any of the code. |

Findings

| Severity | Found |
|---|-------|
|  High-Risk | 0 |
|  Medium-Risk | 0 |
|  Low-Risk | 0 |
|  Informational | 1 |
| Total | 1 |

- **Informational:** Implementation of certain corrective actions or accepting the risk.

Set AntiBot

Description:

The owner can set anti bot function.

```
// anti bot
```

```
address public _PresaleAddress =
```

```
0x00000000000000000000000000000000dEaD;
```

```
bool public liquidityLaunched = false; // to track if launchLiquidity function has been
called
```

```
bool public isFirstLaunch = true; // to track if launchLiquidity function has been called
```

```
uint256 public lastSnipeTaxBlock; // set to blocks after liq added
```

```
uint8 public snipeBlocks = 0;
```

Privileged Functions

onlyOwner

| Function Name | Parameters | Visibility |
|---------------------------|---|------------|
| decreaseAllowance | address spender, uint256 subtractedValue | Public |
| IncreaseAllowance | address spender, uint256 addedValue | Public |
| setIsExcludedFromFee | address account, bool newValue | Public |
| setMarketPairStatus | address account, bool newValue | Public |
| setMarketingWalletAddress | address newAddress | External |
| setNumTokensBeforeSwap | uint256 newLimit | External |
| transfer | address recipient, uint256 amount | Public |
| transferFrom | address sender, address recipient, uint256 amount | Public |
| transferOwnership | address newOwner | Public |
| | | |
| | | |

Contract Ownership

The contract ownership of UltramanBSC is not currently renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible ownable functions that may alter the state of the protocol.

The current owner is the address 0x0aa4c3DE9E4e249E207fDef957eD208312230920 which can be viewed: [HERE](#)

The owner wallet has the power to call the functions displayed on the privileged functions list above, if the owner wallet is compromised these privileges could be exploited.

We recommend the team renounce ownership at the right timing if possible, or gradually migrate to a time lock with governing functionalities in respect of transparency and safety considerations.

Liquidity Overview

Liquidity Information

| Parameter | Result |
|---------------------|--|
| Pair Address | 0xc50e4a420ae3314c12d469c42e3ecdf6292c28e8 |
| UTM Reserves | 0.00 UTM |
| BNB Reserves | 0.00 BNB |
| Liquidity Value | \$0 USD |
| Liquidity Ownership | The token does not have liquidity at the moment of the audit |

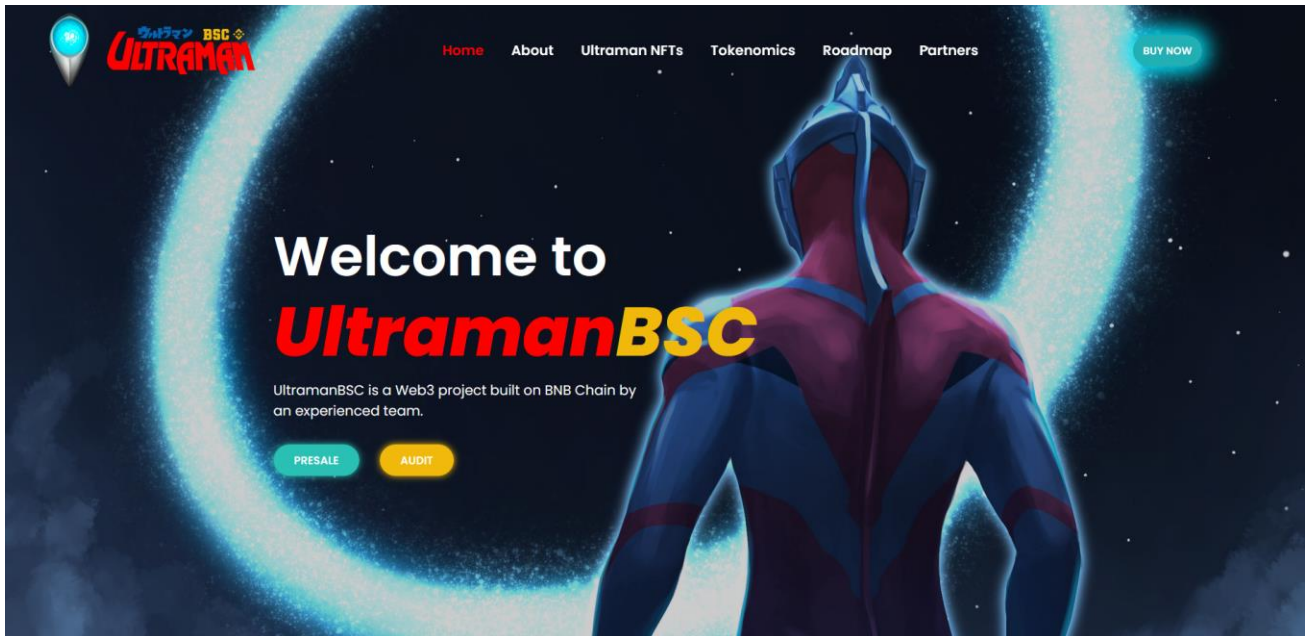
Tokenomics

| Rank | Address | Quantity (Token) | Percentage |
|------|--|------------------|------------|
| 1 | 0x0aa4c3DE9E4e249E207fDef957eD208312230920 | 100,000,000,000 | 100.0000% |

Social Media Check

| Social Media Type | Link | Result |
|-------------------|---|---------|
| Website | http://www.ultramanbsc.com | Checked |
| Twitter | https://twitter.com/UltramanBSC/ | Checked |
| Telegram | https://t.me/UltramanBSC_Global/ | Checked |
| Reddit | https://www.reddit.com/r/UltramanBSC/ | Checked |

Website Review



- Mobile Friendly
- Contains no code errors
- SSL is not secured
- No spelling errors

Audit Conclusion

- The owner cannot pause trading
- The owner cannot mint new tokens
- The owner cannot blacklist users
- The owner cannot set the max transaction amount.
- The owner cannot change the buy/sell fee
- The contract has an antibot function

AUDIT IS PASSED