CRACKEN

Smart Contract Security Audit

Project: StepHunt

May 19, 2022

Contract Address

0x24B80b49574cb6Ca103d1e27c7be6752C8b48759

Table of Contents

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 Step Hunt 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.
- Comparison to specification, which is the process of checking whether the code does what the specifications, sources, and instructions provided to Cracken describe.
- Test coverage analysis is the process of determining whether the test cases are actually 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	Step Hunt
Token Symbol	HUNT
Token Decimal	18
Total Supply	1,000,000,000
Platform	BSC
Buy Tax Fee	5%
Sell Tax Fee	5%
Contract Creation Date	May 16, 2022
Liquidity Status	Locked
Liquidity Lockup Time	365 Days after listing
Compiler Version	v0.8.9+commit.e5eed63a
Optimization	Yes with 300 runs
Contract Address	0x24B80b49574cb6Ca103d1e27c7be6752C8b48759
Deployer Address	0x0ab478ccB5effCc2510326257Ce0525cD91FcfB1
Owner Address	0x3Bb4253f3188E7440eB7e5f6b9e3577201aD19D6

Source Code

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

https://bscscan.com/address/0x24B80b49574cb6Ca103d1e27c7be6752C8b48759

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	Exploits, vulnerabilities, or errors that will certainly or probabilistically lead to loss of funds, control, or impairment of the contract and its functions. Issues under this classification are recommended to be fixed with utmost urgency.
Medium	Bugs or issues with that may be subject to exploitation, though their impact is somewhat limited. Issues under this classification are recommended to be fixed as soon as possible.
Low	Effects are minimal in isolation and do not pose a significant danger to the project or its users. Issues under this classification are recommended to be fixed nonetheless.
Info	Consistency, syntax, or style best practices. Generally, pose a negligible level of risk, if any.

Findings

Severity	Found
High	0
Medium	0
Low	0
Info	0
Total	0

Privileged Functions

onlyOwner

Function Name	Parameters	Visibility
setPercentTaxBuy	Uint256_percentTax	External
setPercentTaxSell	Uint256_percentTax	External

- The owner cannot set buy and sell fees over 50%.

Contract Ownership

The contract ownership of Step Hunt 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 0x3Bb4253f3188E7440eB7e5f6b9e3577201aD19D6 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	Not available
Step Hunt Reserves	0.00 HUNT
BNB Reserves	0.00 BNB
Liquidity Value	$0 USD
Liquidity Ownership	The token does not have liquidity at the moment of the audit

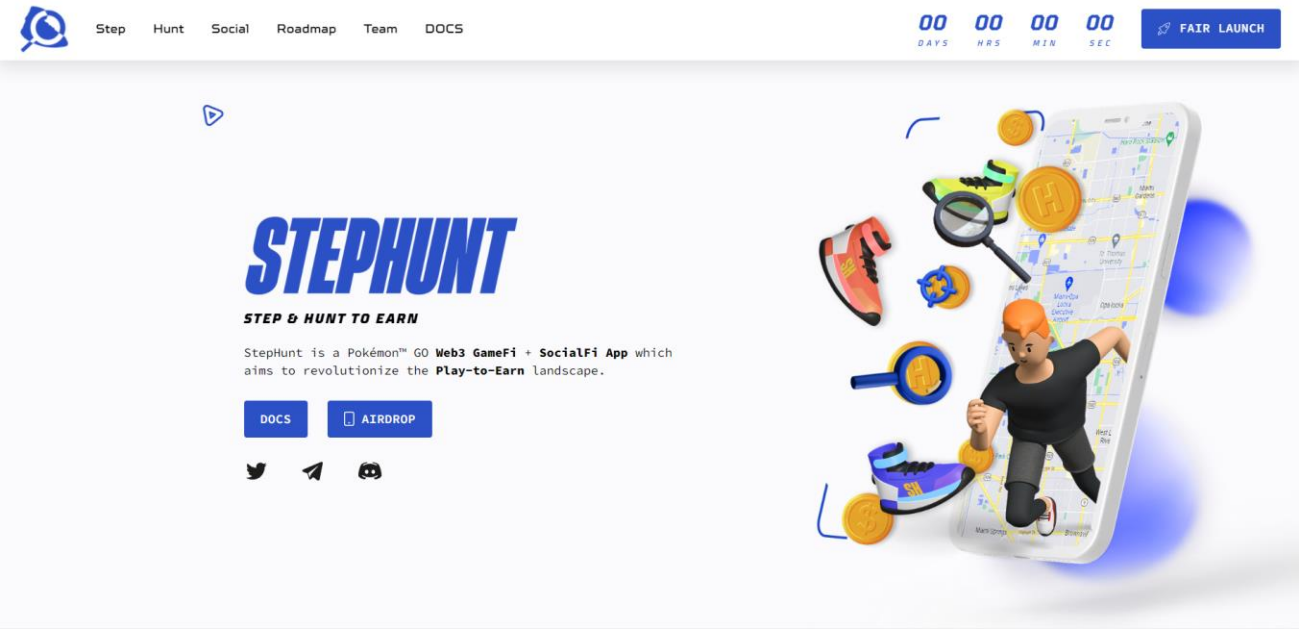
Tokenomics

Rank	Address	Quantity (Token)	Percentage
1	0x1fb89a4d14a9d066863ef6af096e33d50ea490da	921,500,000	92.1500%
2	0x3bb4253f3188e7440eb7e5f6b9e3577201ad19d6	78,500,000	7.8500%

Social Media Check

Social Media Type	Link	Result
Website	https://stephunt.com/	No problems
Twitter	https://twitter.com/stephuntapp	No problems
Telegram	https://t.me/stephuntapp	No problems
Facebook	https://twitter.com/stephuntapp	Not match
GitHub	https://whitepaper.stephunt.com/	Not match

Website Review



- Mobile Friendly
- Contains no code errors
- SSL Secured
- No spelling errors