expelee

Building the Futuristic Blockchain Ecosystem

Audit Report

FOR

Infinity Protocol

OVERVIEW

The Expelee team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analysed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks. According to the smart contract audit:

Audit Result	Passed with Low Risk
KYC Verification	Done
Audit Date	28 Oct 2022

-Team Expelee

PROJECT DESCRIPTION

Infinity Protocol

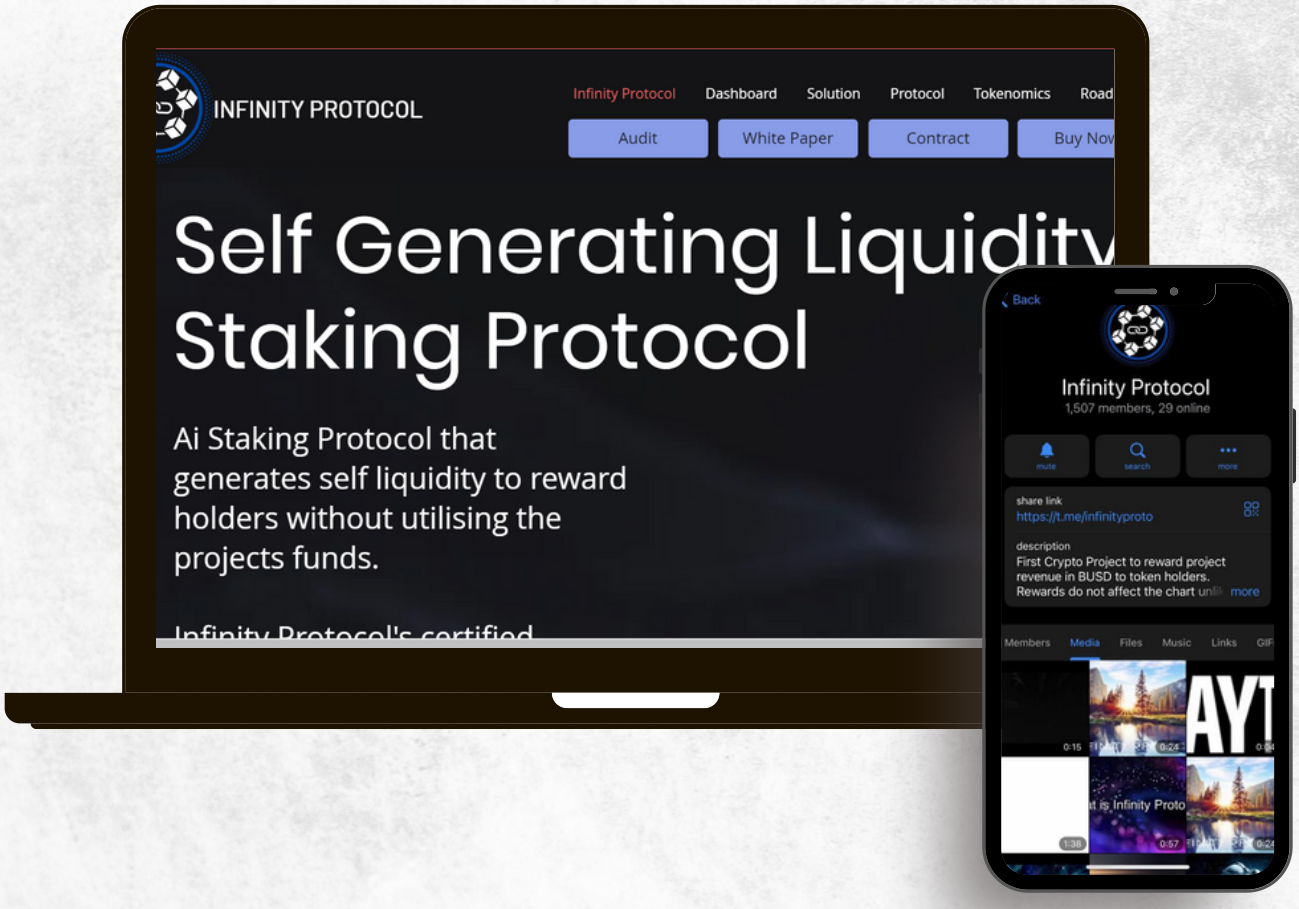
Infinity Protocol a new DeFi solution fully automatic and self sustained
The first rewards token that gives BUSD to holders without affecting the project's liquidity as Infinity Protocol generates its own revenue without risking the projects liquidity pool

expelee

expelee.com

Social Media Profiles

Infinity Protocol



https://infinityprotocol.app

https://t.me/infinityproto

https://twitter.com/Infinityprotocl

It's always good to check the social profiles of the project, before making your investment.

-Team Expelee

CONTRACT DETAILS

Token Name
Infinity Protocol

Symbol
Infinity

Network
BSC

Language
Solidity

Contract Address (Verified)
0x2ae6852A408E7A004830888ea79d4cD0BBF03CE0

Token Type
ERC 20

Decimals
18

Compiler
v0.8.15+commit.e14f2714

Total Supply
1,000,000,000

Contract SHA-256 Checksum:
09cc1b4293703d26a2038b18d13d44c809c6d85f9e9adfd884b68805e4b22e09

AUDIT METHODOLOGY

Audit Details

Our comprehensive audit report provides a full overview of the audited system's architecture, smart contract codebase, and details on any vulnerabilities found within the system.

Audit Goals

The audit goal is to ensure that the project is built to protect investors and users, preventing potentially catastrophic vulnerabilities after launch, that lead to scams and rugpulls.

Code Quality

Our analysis includes both automatic tests and manual code analysis for the following aspects:

- Exploits
- Back-doors
- Vulnerability
- Accuracy
- Readability

Tools

- DE
- Open Zeppelin
- Code Analyzer
- Solidity Code
- Complier
- Hardhat

VULNERABILITY CHECKLIST

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions & reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

RISK CLASSIFICATION

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

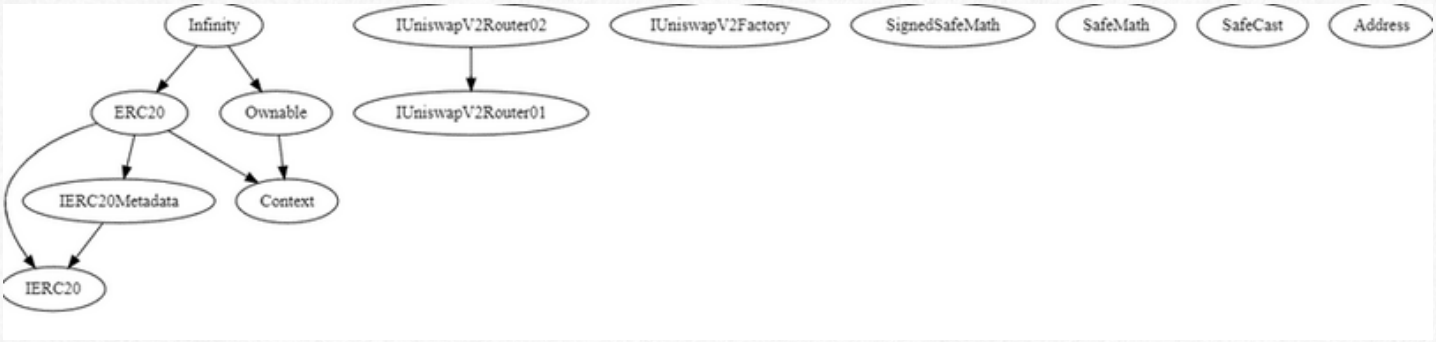
AUDIT SUMMARY

Ownership:

Deployer - 0xC03e47F61F5C8F143c870584D9A92cd170447558

Contracts & Inheritance Tree:

Infinity Protocol token is inheriting from this contracts



Summary

1- 10% buy tax and 20% sell tax currently
2- owner is not able to set taxes over 15%
3- owner is able to set a max amount for buying/selling/trasferring amount(minimum 1/300 of total supply)
4- owner is not able to disable trades
5- owner is not able to blacklist an arbitrary address
6- owner is not able to mint new tokens

MANUAL AUDIT

Severity Criteria

Expelee assesses the severity of disclosed vulnerabilities according to a methodology based on
OWASP standards.
Vulnerabilities are divided into three primary risk categories: high, medium, and low.

High-level considerations for vulnerabilities span the followingkey areas when conducting assessments:

- Malicious Input Handling
- Escalation of privileges
- Arithmetic
- Gas use

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Findings Summary

- High Risk Findings:0
- Medium Risk Findings:1
- Low Risk Findings:1
- Suggestions & discussion: 1
- Gas Optimizations : 1

Medium Risk Findings

Centralization – Owner is able to set a max amount for buying/selling/transferring amount, this amount can not be lower than 1/300 of total supply.

```
  function setMaxTxAmount(uint256 _maxTx) public onlyOwner {
maxTransactionAmount = _maxTx;
require(maxTransactionAmount >= totalSupply().div(300), "value is too low");
  }
```

Low Risk Findings

Centralization - Owner is able to set buy/sell taxes each one up to 15%, this means 30% if both of them are set to highest.

```
 function updateFee(uint256 _buyTax, uint256 _sellTax) public onlyOwner {
require(_buyTax <= 15, "buy tax too high");
      buyTax = _buyTax;
require(_sellTax <= 25, "sell tax too high");
      sellTax = _sellTax;
}
```

Gas Optimizations

- do not use SafeMath library to reduce gas usage

Suggestions

- for uniswap router/factory only import necessary functions to reduce contract size

ABOUT EXPELEE

Expelee is a product-based aspirational Web3 Start-up. Coping up with numerous solutions for blockchain Security and constructing a Web3 Ecosystem from Deal making platform to developer hosting open platform, while also developing our own commercial and sustainable blockchain.

www.expelee.com

expeleeofficial

expelee

Expelee

expelee

expelee_official

expelee-co

expelee

Building the Futuristic **Blockchain Ecosystem**

DISCLAIMER

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment. Team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document.

Always Do your own research and protect yourselves from being scammed. The Expelee team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools.

Under no circumstances did Expelee receive a payment to manipulate those results or change the awarding badge that we will be adding in our website. Always Do your own research and protect yourselves from scams.

This document should not be presented as a reason to buy or not buy any particular token. The Expelee team disclaims any liability for the resulting losses.