expelee

Building the Futuristic Blockchain Ecosystem

Audit Report
FOR

Twin 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**
🔍	**KYC Verification**	**Done**
📅	**Audit Date**	**12 Jan 2023**

Audit Passed With no Risk

-Team Expelee

PROJECT DESCRIPTION

Twin Protocol

Twin Protocol is PvP AMM Synthetic Assets Exchange, matching traders against each other in leverage trades with the option for liquidity providers to participate.

We take the best that DeFi has to offer and allow traders to open long or short positions at the current prices of synthetic assets.

Social Media Profiles

Twin Protocol

🌐 https://twinprotocol.xyz/

✈ https://t.me/Twinprotocolxyz

🐦 https://twitter.com/Twinprotocolxyz
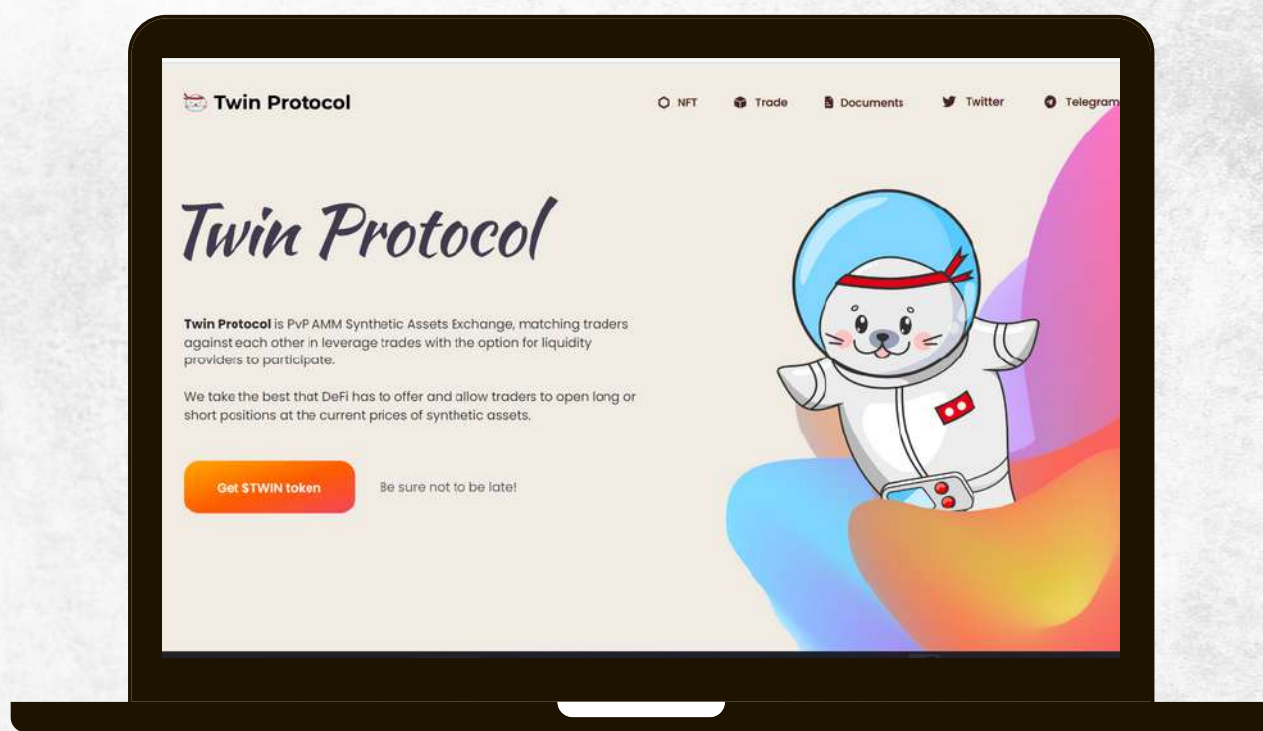
It's always good to check the social profiles of the project, before making your investment.

-Team Expelee

CONTRACT DETAILS

Token Name

Twin Protocol

Symbol

TWIN

Network

BSC

Language

Solidity

Contract Address (Verified)

0x4B1F493678e5DA4F19fEe5245430539e36Dccd19

Token Type

BEP20

Total Supply

10,000,000

Compiler

v0.8.4+commit.c7e474f2

License

MIT

Contract SHA-256 Checksum:

7b5ad604d7ba2ea760a86c234c1e90bc1d56a1c0c913da505197b49e87dcbc4d

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

FUNCTION OVERVIEW

Can Take Back Ownership	Not Detected
Owner Change Balance	Not Detected
Blacklist	Not Detected
Modify Fees	Not Detected
Proxy	Not Detected
Whitelisted	Not Detected
Anti Whale	Not Detected
Trading Cooldown	Not Detected
Transfer Pausable	Not Detected
Cannot Sell All	Not Detected
Hidden Owner	Not Detected
Mint	Not Detected

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.
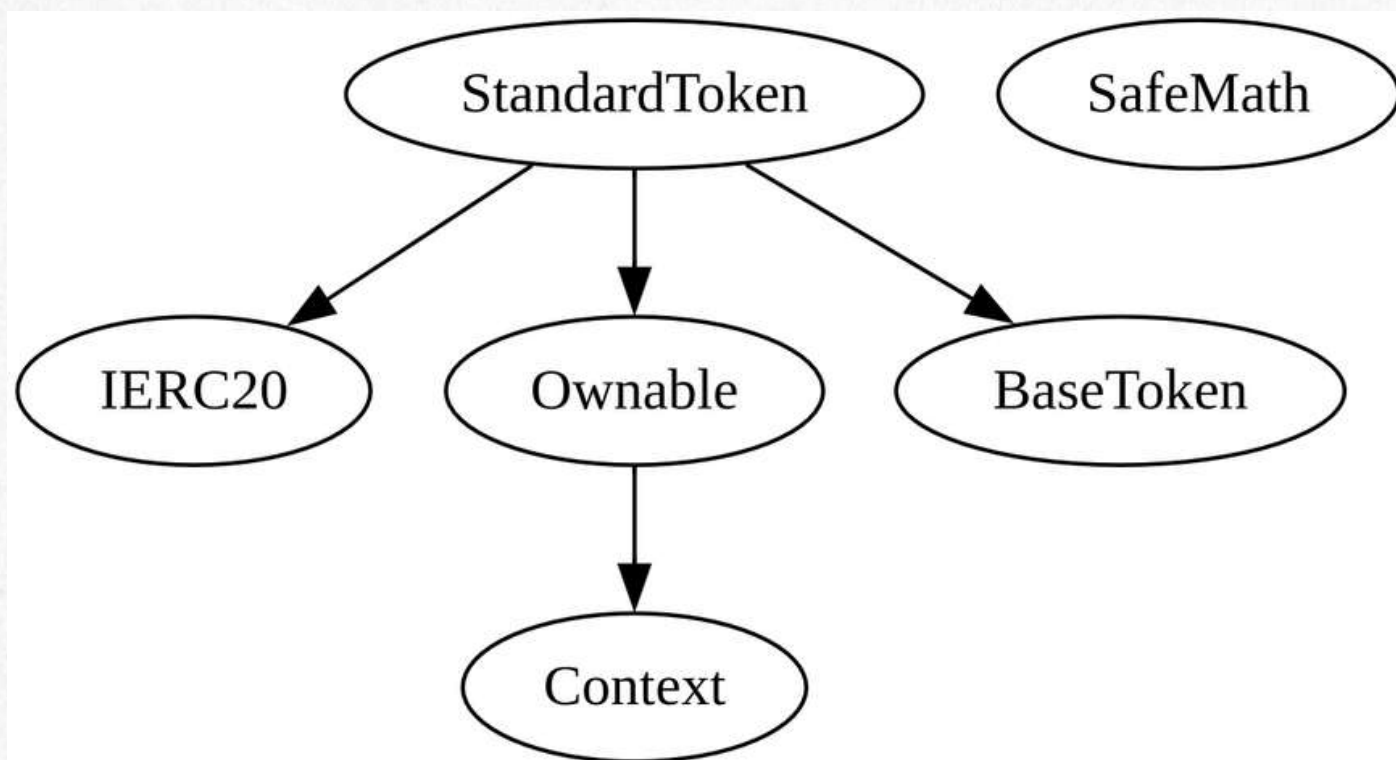
AUDIT SUMMARY

Ownership:

0xbfC141a02AE68124573Fe81765e5d7361A6206b2 is the owner of the contract

Contracts & Inheritance Tree:

All of below contracts are in this audit scope

Summary

- Owner is not able to change or set taxes (0% tax)
- Owner is not able to set a max amount for buys/sells/transfer
- Owner is not able to pause trades
- Owner is not able to mint new tokens
- Owner is not able to blacklist an arbitrary address

SWC:

floating pragma

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 following key areas when conducting assessments:

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

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

Findings Summary

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

No Risk Findings

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.