expelee

Building the Futuristic Blockchain Ecosystem

Audit Report

FOR

BlockXpress

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	30 Oct 2022

-Team Expelee

PROJECT DESCRIPTION

BlockXpress

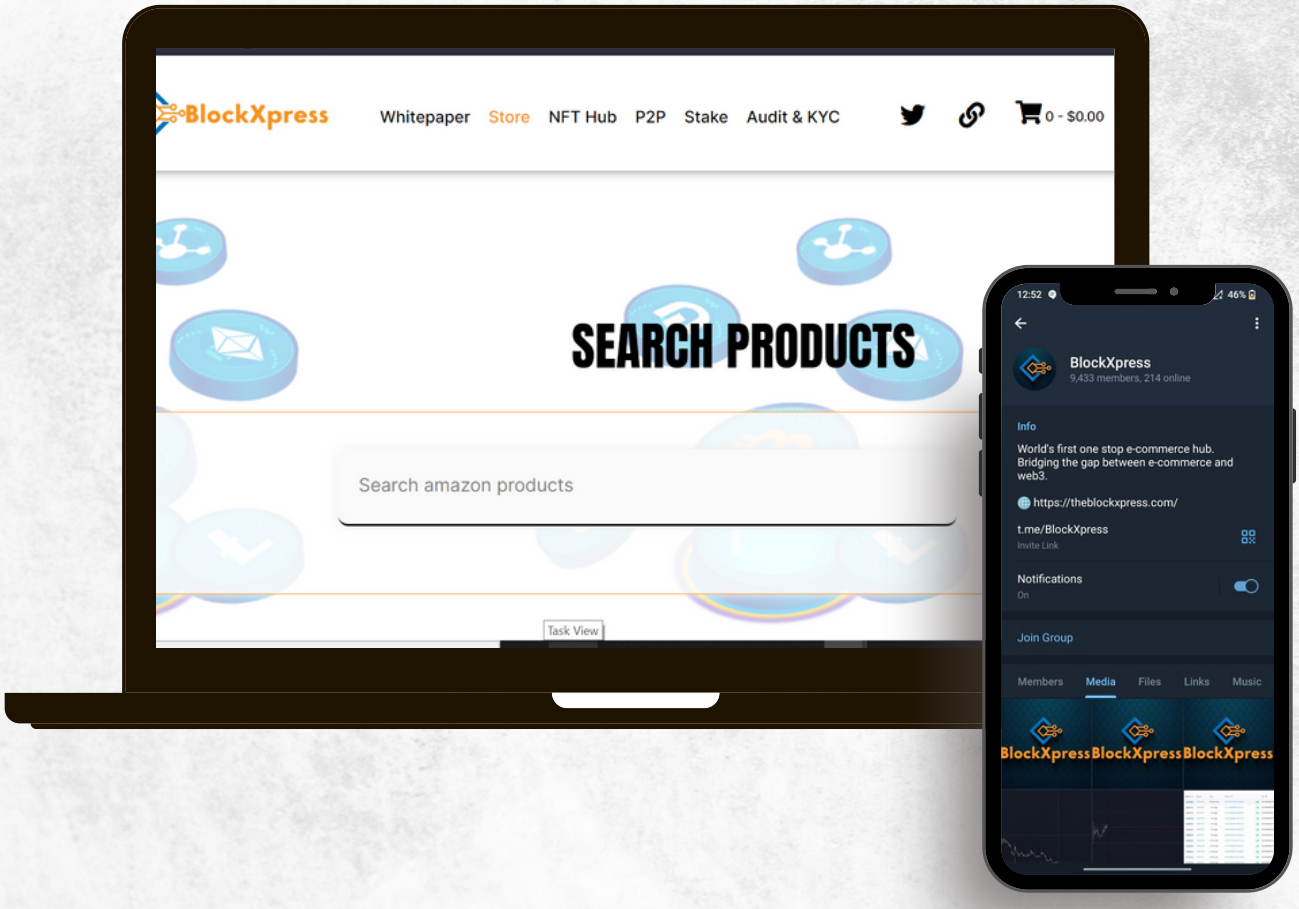
Bridging decentralisation and commerce in one platform at the ease of convenience to every userbase is our main focus. In the era of progression and innovation, time is the most valuable resources people have. Our goal is to make things easier for every userbase to bridge blockchain and commerce in the most efficient and reliable way

expelee

expelee.com

Social Media Profiles

Block Express



https://theblockxpress.com/stake/

https://t.me/BlockXpress

https://twitter.com/blockxpress

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

-Team Expelee

CONTRACT DETAILS

Contract Type
STAKING CONTRACT

Symbol
-

Network
BSC

Language
Solidity

Contract Address (Verified)
0x8Af63fbc8d680cEC25c6E5Ca5C90e788d2D74406

Token Type
ERC 20

Total Supply
-

Compiler
v0.8.17+commit.8df45f5f

License
None

Contract SHA-256 Checksum:
cd6be33fa0976b3820e1ffbbdcb38dd8c8daf0fb726dab5adb2eab9c68205f53

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

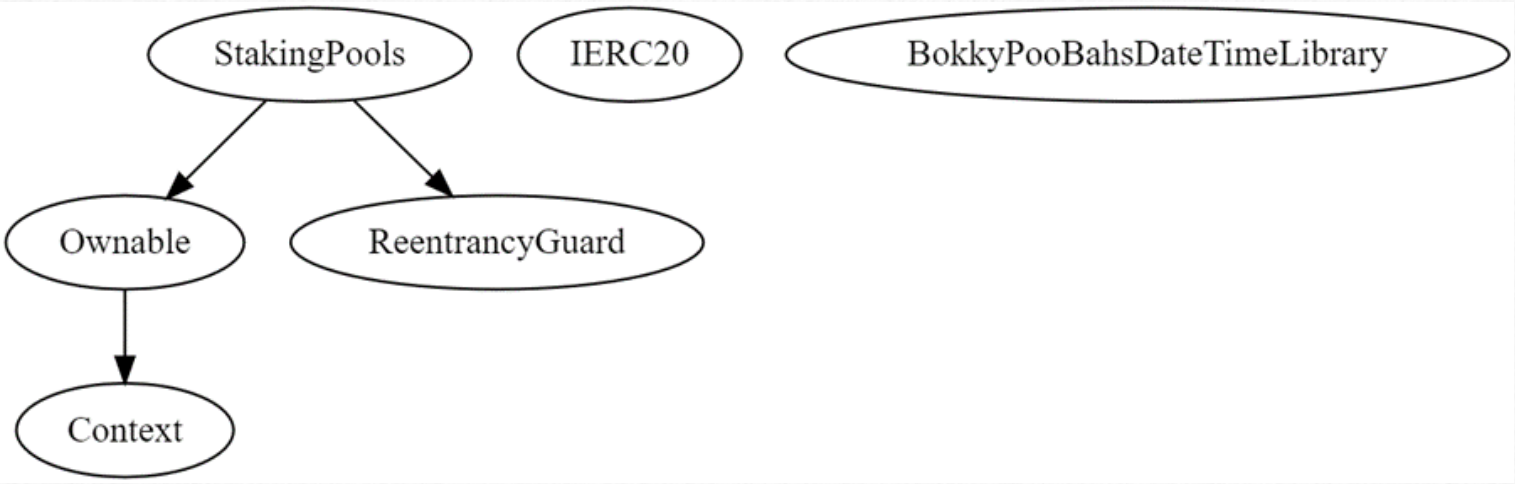
Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

AUDIT SUMMARY

Audit Scope:

StakingPools.sol is in this audit scope
Ownable, Context, IERC20 and ReentrancyGuard are standard openzeppelin contracts which are not in this audit scope, BokkyPooBahsDateTimeLibrary is a date & time library which is also not in this audit scope.

Contracts & Inheritance Tree:



Summary

- there are 3 Pools, with 15%, 35%, 75% APY each.
- lock times are 14, 30, 60 days for each Pool.

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:2
- Suggestions & discussion: 0
- Gas Optimizations : 0

Medium Risk Findings

Logical - **withdrawing can be reverted for some users:**
this is issue is met when there is not enough tokens in the contract, i.e, owner should deposit some amount of staking tokens to the contract to cover rewards, otherwise rewards will be paid from staking amounts, and this means there wont be enough tokens in the contract for some users to withdraw.

Low Risk Findings

Centralization - **owner is able to withdraw all staked tokens after end of staking period (6 monthes):**

```
function withdrawERC20(address _tokenContract, uint256 _amount)
        external
        onlyOwner
    {
        if (_tokenContract == address(tokenToStake)) {
require(
block.timestamp >= stakingEndingDate(),
"You cannot withdraw stake tokens untill stake has ended"
            );
        }
        IERC20 tokenContract = IERC20(_tokenContract);
tokenContract.transfer(msg.sender, _amount);
}
```

Suggestion : make sure that owner is not able to withdraw staking tokens from the contract but only able to withdraw other tokens.

Centralization - Owner is able to set fees up to 30% for rewards.

```
function changeFee(uint256 _newFee) public onlyOwner {
    fee = _newFee;
}
```

this fees are deducted from accumolated rewards at time of unstaking

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.