

expelee

Building the Futuristic **Blockchain Ecosystem**

Security Audit Report FOR



XAI CORP

XAI Corp

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:

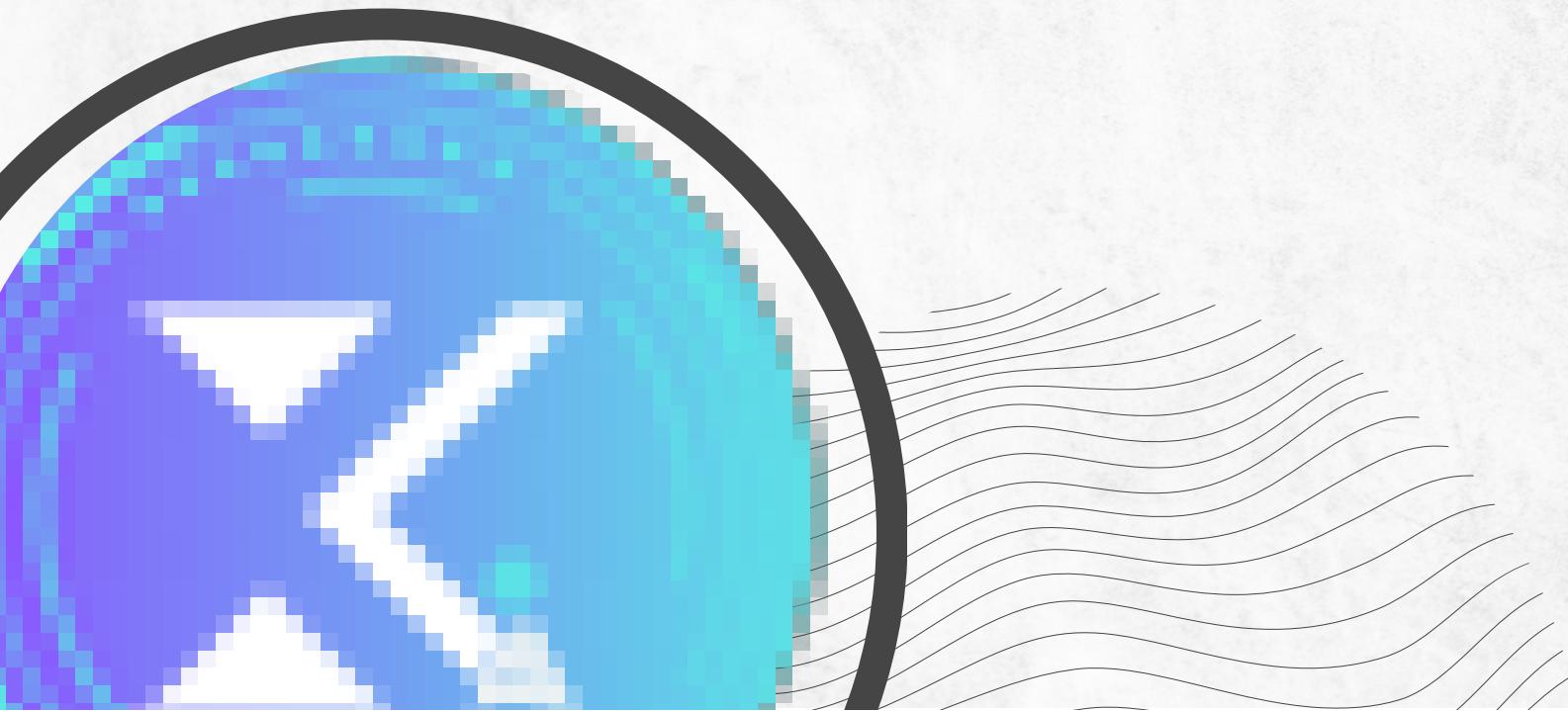
 Audit Result	Passed
 KYC Verification	Not Done
 Audit Date	16 April 2023

PROJECT DESCRIPTION

XAI Corp

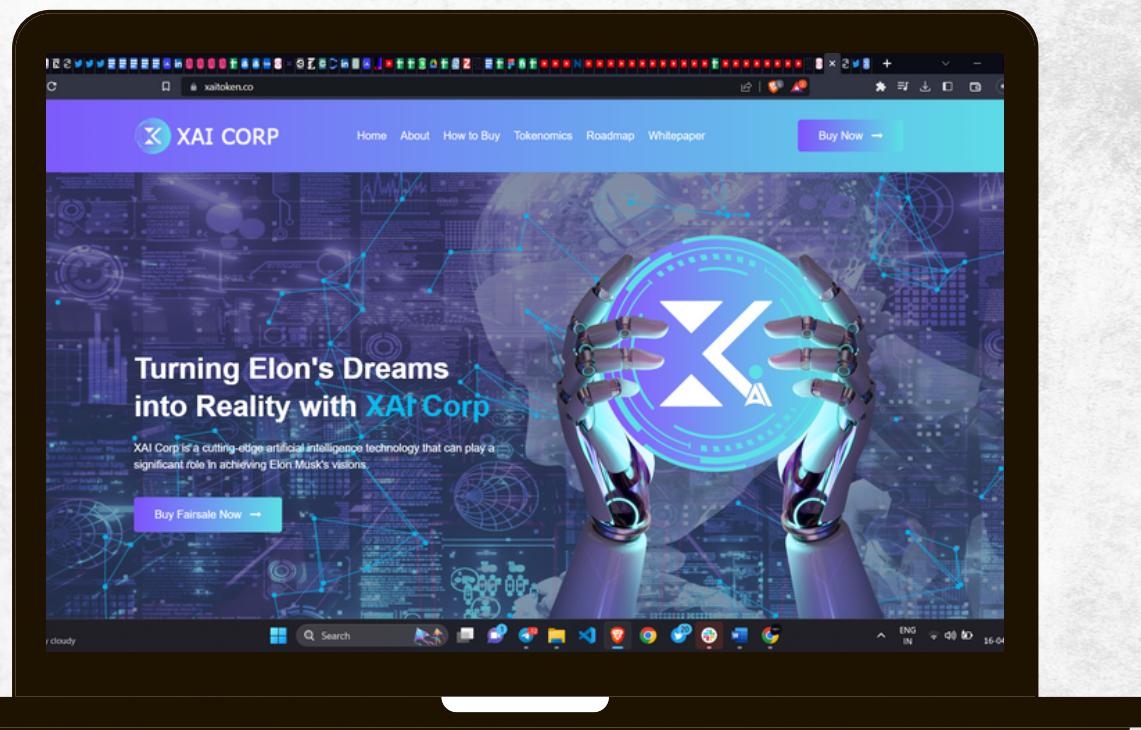
XAI Corp is introducing a cutting-edge AI-based crypto trading platform that is designed to help traders make informed and profitable trading decisions in the dynamic and fast-paced world of cryptocurrency trading.

Our AI technology uses advanced algorithms and machine learning to analyze market data, identify trends, and make predictions about future price movements. With real-time analysis and actionable insights.



Social Media Profiles

XAI Corp



-  <https://xaitoken.co/>
-  https://t.me/xaicorp_official
-  https://twitter.com/xaicorp_elon

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

-Team Expelee

CONTRACT DETAILS

Token Name	Symbol
XAI Corp	XAI
Network	Language
Binance Smart Chain	Solidity
Contract Address (Verified)	
0xdf727caE79B396C32aa86614B62436A63262AEAf	
Token Type	Total Supply
BEP20	1,000,000,000,000
Contract SHA-256 Checksum:	
633af0857339c96ce1006177a5864f189c6de7a6	
Owner Wallet	
0x1E921C2d9e3bB8F3350e2E22759ddA2F237b140D	
Deployer Wallet	
0x1E921C2d9e3bB8F3350e2E22759ddA2F237b140D	

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.

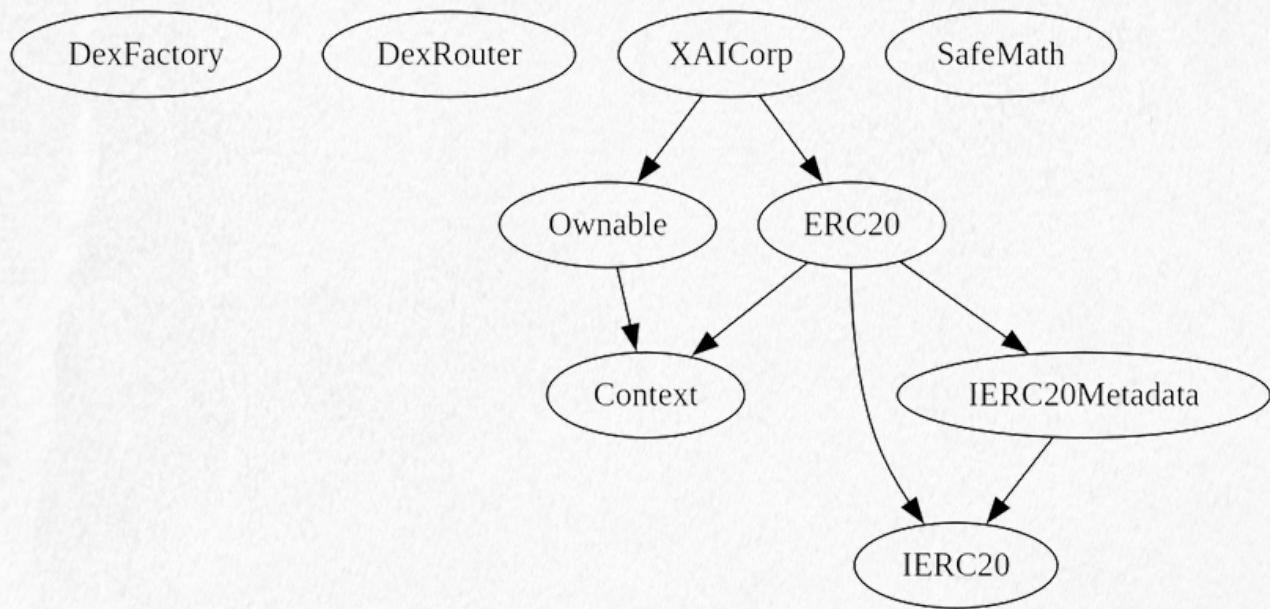
AUDIT SUMMARY

Used Tools:

- 1. Manual Review:** The code underwent a thorough review process by the Expelee team, which involved analyzing the code line by line. This review helped to identify any potential issues or bugs that could impact the performance of the code.
- 2. BSC Test Network:** The code was tested extensively on the BSC Test network to ensure that it functions as intended. All tests were conducted using the BSC Test network, and each test has a corresponding transaction attached to it. These tests can be accessed in the "Functional Tests" section of the report.

Overall, these tools were instrumental in identifying any potential issues and ensuring that the code functions as expected.

Inheritance Trees:



Summary:

- Contract owner is not able to set buy/sell taxes more than 5% each
- Contract owner is not able to set transfer fee (0% transfer fee)
- Contract owner is not able to set limits for buy/sell/transfer amounts
- Contract owner is not able to blacklist an arbitrary wallet
- Contract owner is not able to disable trades/transfers
- Contract owner is not able to mint new tokens

Testnet Version:

Adding Liquidity

Tx:

<https://testnet.bscscan.com/tx/0x4f8728f0f3e9627bfda980fbe6a8fb3f862131a8ff898f954b3508d15d9e11f>

Buying from a fee excluded wallet

Tx (0% tax):

<https://testnet.bscscan.com/tx/0x536400d13ab7b63711af1bdd8a7d95f89692a1b89b8ba6dc856494d484824bb0>

Selling from a fee excluded wallet

Tx (0% tax):

<https://testnet.bscscan.com/tx/0x318d544bd2eb80060c02f93f6e8251beadab8c019aaba97897e668ee3506d6e1>

Transferring using a fee excluded wallet

Tx (0% tax):

<https://testnet.bscscan.com/tx/0x982a6e6d7252e658b85cc81cdbae0d07eca6730ebd5dc5d57b390849f3d31ca9>

Testnet Version:

Buying from a regular wallet 

Tx (max 5% tax):

<https://testnet.bscscan.com/tx/0xc929f9a89be63a281a97761fa5587c4e936958ceb38512977738c0cbee9f498d>

Selling from a regular wallet 

Tx (max 5% tax):

<https://testnet.bscscan.com/tx/0x0e74115cf4141d819f75edfe730843ae412c2a1b9e2047265a1eec6251db145>

Transferring using a regular wallet 

Tx (0% tax):

<https://testnet.bscscan.com/tx/0x08c3ab4d6b863458d1f7f9516f930e84a7c96a2c1d7f346cf9947113e2c838c3>

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				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
Likelihood				

FINDINGS

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

High Risk Finding

Category: Centralization

Impact: High

Subject: Enabling trades is not guaranteed

Overview:

The owner of the contract must enable trades for public, otherwise no one would be able to buy/sell/transfer their tokens except whitelisted wallets.

```
function enableTrading(address _pairAddress) external onlyOwner {  
    pairAddress = _pairAddress;  
    tradingStatus = true;  
}
```

Suggestion

To mitigate this issue there are several options:

- Temporary transfer ownership of the contract to a pinksale safu developer (**suggested**)
- Enable tradings before presale
- Allowing enabling of the trades after a specifiec time by any token holder

Example:

```
function enableTrading(address _pairAddress) external {  
    require(msg.sender == owner || elapsedTimeSincePresale >  
threshold, "Caller  
must be owner, or threshold must be  
passed");  
    pairAddress = _pairAddress;  
    tradingStatus = true;  
}
```

Issue Status: Open

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.