expelee

Building the Futuristic Blockchain Ecosystem

SECURITY AUDIT REPORT

BONKI

TOKEN OVERVIEW

Risk Findings

Severity	Found
High	1
Medium	0
Low	0
Informational	0

Centralization Risks

Owner Privileges	Description
Can Owner Set Taxes >25% ?	Not Detected
Owner Can enable trading ?	Detected
Can Owner Disable Trades ?	Not Detected
Can Owner Mint ?	Not Detected
Can Owner Blacklist ?	Not Detected
Can Owner set Max Wallet amount ?	Not Detected
Can Owner Set Max TX amount ?	Not Detected

expelee

TABLE OF CONTENTS

02 Token Overview
03 Table of Contents
04 Overview
05 Contract Details
06 Audit Methodology
07 Vulnerabilities Checklist
08 Risk Classification
09 Inheritance Tree
10 Static Analysis
13 Testnet Version
14 Manual Review
17 About Expelee
18 Disclaimer

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 high risk**
KYC Verification	**-**
Audit Date	**03 Jan 2024**

CONTRACT DETAILS

Token Name: BONKI

Token Address: 0x90e4d3321288a7260A206DA769c28ea1BAF2918a

Symbol: BONKI

Network: BscScan

Token Type: BEP - 20

Language: Solidity

Total Supply: 100,000,000,000,000

Owner's Wallet:
0x6E5c933bD0d57368B9959fd48e1ED2BF11cD00FD

Deployer's Wallet:
0x4AC8cb73913a9A7e34f82Fac6877af647673210b

Checksum:
a2032c616934aeb47e6039f76b20d2F5

Testnet
https://testnet.bscscan.com/address/0xf9963cbd4be362414ff2978b04ec3995dab09d0e#code

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
- Compiler
- Hardhat

VULNERABILITY CHECKS

Design Logic	Passed
Compiler warnings	Passed
Private user data leaks	Passed
Timestamps 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 Zepplin module	Passed

RISK CLASSIFICATION

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and acces 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

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

expelee

INHERITANCE TREES

expelee

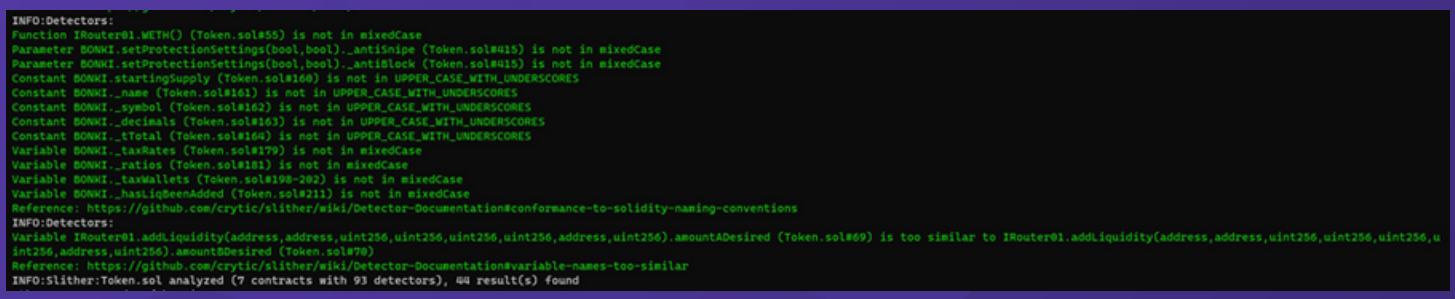
STATIC ANALYSIS

A static analysis of the code was performed using Slither. No issues were found.

```
INFO:Detectors:
BONKI.contractSwap(uint256) (Token.sol#571-631) performs a multiplication on the result of a division:
        - toLiquify = ((contractTokenBalance * ratios.liquidity) / ratios.totalSwap) / 2 (Token.sol#581)
        - liquidityBalance = (amtBalance * toLiquify) / swapAmt (Token.sol#601)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#divide-before-multiply
INFO:Detectors:
Reentrancy in BONKI.enableTrading() (Token.sol#647-666):
        External calls:
        - initializer.setLaunch(lpPair,uint32(block.number),uint64(block.timestamp),_decimals) (Token.sol#653-655)
        - (initThreshold,initSwapAmount) = initializer.getInits(balanceOf(lpPair)) (Token.sol#656-662)
        State variables written after the call(s):
        - tradingEnabled = true (Token.sol#663)
        BONKI.tradingEnabled (Token.sol#210) can be used in cross function reentrancies:
        - BONKI._transfer(address,address,uint256) (Token.sol#527-569)
        - BONKI.enableTrading() (Token.sol#647-666)
        - BONKI.renounceOwnership() (Token.sol#274-280)
        - BONKI.tradingEnabled (Token.sol#210)
Reentrancy in BONKI.finalizeTransfer(address,address,uint256,bool,bool,bool) (Token.sol#689-729):
        External calls:
        - check = initializer.checkUser(from,to,amount) (Token.sol#699-703)
        State variables written after the call(s):
        - _checkLiquidityAdd(from,to) (Token.sol#717)
                - _liquidityHolders[from] = true (Token.sol#636)
        BONKI._liquidityHolders (Token.sol#154) can be used in cross function reentrancies:
        - BONKI._checkLiquidityAdd(address,address) (Token.sol#633-645)
        - BONKI._hasLimits(address,address) (Token.sol#513-525)
        - BONKI.constructor() (Token.sol#225-240)
        - BONKI.excludePresaleAddresses(address,address) (Token.sol#493-511)
        - _checkLiquidityAdd(from,to) (Token.sol#717)
                - initializer = Initializer(address(this)) (Token.sol#640)
        BONKI.initializer (Token.sol#212) can be used in cross function reentrancies:
        - BONKI._checkLiquidityAdd(address,address) (Token.sol#633-645)
        - BONKI._hasLimits(address,address) (Token.sol#513-525)
        - BONKI.enableTrading() (Token.sol#647-666)
        - BONKI.finalizeTransfer(address,address,uint256,bool,bool,bool) (Token.sol#689-729)
        - BONKI.removeSniper(address) (Token.sol#411-413)
        - BONKI.setInitializer(address) (Token.sol#376-389)
        - BONKI.setLpPair(address,bool) (Token.sol#361-374)
        - BONKI.setProtectionSettings(bool,bool) (Token.sol#415-417)
        - BONKI.takeTaxes(address,uint256,bool,bool) (Token.sol#731-752)
Reentrancy in BONKI.transferOwner(address) (Token.sol#256-272):
        External calls:
        - finalizeTransfer(_owner,newOwner,balanceOf(_owner),false,false,true) (Token.sol#266)
                - check = initializer.checkUser(from,to,amount) (Token.sol#699-703)
        State variables written after the call(s):
        - _owner = newOwner (Token.sol#270)
        BONKI._owner (Token.sol#248) can be used in cross function reentrancies:
        - BONKI._hasLimits(address,address) (Token.sol#513-525)
        - BONKI.constructor() (Token.sol#225-240)
```

```
INFO:Detectors:
BONKI.setInitializer(address).constructorLP (Token.sol#379) lacks a zero-check on :
        - lpPair = constructorLP (Token.sol#381)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation
INFO:Detectors:
BONKI.finalizeTransfer(address,address,uint256,bool,bool,bool) (Token.sol#689-729) has external calls inside a loop: check = initializer.checkUser(from,to,amount) (Token.sol#699-703)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation/#calls-inside-a-loop
INFO:Detectors:
Reentrancy in BONKI.enableTrading() (Token.sol#647-666):
        External calls:
        - initializer.setLaunch(lpPair,uint32(block.number),uint64(block.timestamp),_decimals) (Token.sol#653-655)
        - (initThreshold,initSwapAmount) = initializer.getInits(balanceOf(lpPair)) (Token.sol#656-662)
        State variables written after the call(s):
        - allowedPresaleExclusion = false (Token.sol#664)
        - launchStamp = block.timestamp (Token.sol#665)
        - swapAmount = initSwapAmount (Token.sol#661)
        - swapThreshold = initThreshold (Token.sol#660)
Reentrancy in BONKI.finalizeTransfer(address,address,uint256,bool,bool,bool) (Token.sol#689-729):
        External calls:
        - check = initializer.checkUser(from,to,amount) (Token.sol#699-703)
        State variables written after the call(s):
        - _checkLiquidityAdd(from,to) (Token.sol#717)
                - _hasLiqBeenAdded = true (Token.sol#638)
        - _checkLiquidityAdd(from,to) (Token.sol#717)
                - _isExcludedFromFees[from] = true (Token.sol#637)
        - _tOwned[from] -= amount (Token.sol#712)
        - _tOwned[to] += amountReceived (Token.sol#714)
        - amountReceived = takeTaxes(from,amount,buy,sell) (Token.sol#713)
                - _tOwned[address(this)] += feeAmount (Token.sol#748)
        - _checkLiquidityAdd(from,to) (Token.sol#717)
                - contractSwapEnabled = true (Token.sol#642)
Reentrancy in BONKI.setInitializer(address) (Token.sol#376-389):
        External calls:
        - (router,constructorLP) = initializer.getConfig() (Token.sol#379-387)
        State variables written after the call(s):
        - _approve(_owner,address(dexRouter),type()(uint256).max) (Token.sol#383)
                - _allowances[sender][spender] = amount (Token.sol#326)
        - _approve(address(this),address(dexRouter),type()(uint256).max) (Token.sol#384)
                - _allowances[sender][spender] = amount (Token.sol#326)
        - dexRouter = IRouter02(router) (Token.sol#380)
        - lpPair = constructorLP (Token.sol#381)
        - lpPairs[lpPair] = true (Token.sol#382)
Reentrancy in BONKI.setNewRouter(address) (Token.sol#346-359):
        External calls:
        - lpPair = IFactoryV2(_newRouter.factory()).createPair(address(this),_newRouter.WETH()) (Token.sol#352)
        State variables written after the call(s):
        - _approve(address(this),address(dexRouter),type()(uint256).max) (Token.sol#358)
                - _allowances[sender][spender] = amount (Token.sol#326)
        - dexRouter = _newRouter (Token.sol#356)
```

```
INFO:Detectors:
Reentrancy in BONKI._transfer(address,address,uint256) (Token.sol#527-569):
        External calls:
        - contractSwap(contractTokenBalance) (Token.sol#563)
                - dexRouter.swapExactTokensForETHSupportingFeeOnTransferTokens(swapAmt,0,path,address(this),block.timestamp) (Token.sol#588-598)
                - dexRouter.addLiquidityETH{value: liquidityBalance}(address(this),toLiquify,0,0,DEAD,block.timestamp) (Token.sol#604-617)
                - (success,None) = _taxWallets.marketing.call{gas: 55000,value: marketingBalance}() (Token.sol#626)
                - (success,None) = _taxWallets.buyback.call{gas: 55000,value: buybackBalance}() (Token.sol#629)
        - finalizeTransfer(from,to,amount,buy,sell,other) (Token.sol#568)
                - check = initializer.checkUser(from,to,amount) (Token.sol#699-703)
        External calls sending eth:
        - contractSwap(contractTokenBalance) (Token.sol#563)
                - dexRouter.addLiquidityETH{value: liquidityBalance}(address(this),toLiquify,0,0,DEAD,block.timestamp) (Token.sol#604-617)
                - (success,None) = _taxWallets.marketing.call{gas: 55000,value: marketingBalance}() (Token.sol#626)
                - (success,None) = _taxWallets.buyback.call{gas: 55000,value: buybackBalance}() (Token.sol#629)
        Event emitted after the call(s):
        - ContractSwapEnabledUpdated(true) (Token.sol#643)
                - finalizeTransfer(from,to,amount,buy,sell,other) (Token.sol#568)
        - Transfer(from,address(this),feeAmount) (Token.sol#749)
                - finalizeTransfer(from,to,amount,buy,sell,other) (Token.sol#568)
        - Transfer(from,to,amountReceived) (Token.sol#715)
                - finalizeTransfer(from,to,amount,buy,sell,other) (Token.sol#568)
Reentrancy in BONKI.contractSwap(uint256) (Token.sol#571-631):
        External calls:
        - dexRouter.swapExactTokensForETHSupportingFeeOnTransferTokens(swapAmt,0,path,address(this),block.timestamp) (Token.sol#588-598)
        - dexRouter.addLiquidityETH{value: liquidityBalance}(address(this),toLiquify,0,0,DEAD,block.timestamp) (Token.sol#604-617)
        External calls sending eth:
        - dexRouter.addLiquidityETH{value: liquidityBalance}(address(this),toLiquify,0,0,DEAD,block.timestamp) (Token.sol#604-617)
        Event emitted after the call(s):
        - AutoLiquify(liquidityBalance,toLiquify) (Token.sol#614)
Reentrancy in BONKI.finalizeTransfer(address,address,uint256,bool,bool,bool) (Token.sol#689-729):
        External calls:
        - check = initializer.checkUser(from,to,amount) (Token.sol#699-703)
        Event emitted after the call(s):
        - ContractSwapEnabledUpdated(true) (Token.sol#643)
                - _checkLiquidityAdd(from,to) (Token.sol#717)
        - Transfer(from,address(this),feeAmount) (Token.sol#749)
                - amountReceived = takeTaxes(from,amount,buy,sell) (Token.sol#713)
        - Transfer(from,to,amountReceived) (Token.sol#715)
Reentrancy in BONKI.setInitializer(address) (Token.sol#376-389):
        External calls:
        - (router,constructorLP) = initializer.getConfig() (Token.sol#379-387)
        Event emitted after the call(s):
        - Approval(sender,spender,amount) (Token.sol#327)
                - _approve(address(this),address(dexRouter),type()(uint256).max) (Token.sol#384)
        - Approval(sender,spender,amount) (Token.sol#327)
                - _approve(_owner,address(dexRouter),type()(uint256).max) (Token.sol#383)
        - SetInitializer(init) (Token.sol#388)
Reentrancy in BONKI.setNewRouter(address) (Token.sol#346-359):
```


INFO:Detectors:
Function IRouter01.WETH() (Token.sol#55) is not in mixedCase
Parameter BONKI.setProtectionSettings(bool,bool)._antiSnipe (Token.sol#415) is not in mixedCase
Parameter BONKI.setProtectionSettings(bool,bool)._antiBlock (Token.sol#415) is not in mixedCase
Constant BONKI.startingSupply (Token.sol#160) is not in UPPER_CASE_WITH_UNDERSCORES
Constant BONKI._name (Token.sol#161) is not in UPPER_CASE_WITH_UNDERSCORES
Constant BONKI._symbol (Token.sol#162) is not in UPPER_CASE_WITH_UNDERSCORES
Constant BONKI._decimals (Token.sol#163) is not in UPPER_CASE_WITH_UNDERSCORES
Constant BONKI._tTotal (Token.sol#164) is not in UPPER_CASE_WITH_UNDERSCORES
Variable BONKI._taxRates (Token.sol#179) is not in mixedCase
Variable BONKI._ratios (Token.sol#181) is not in mixedCase
Variable BONKI._taxWallets (Token.sol#198-202) is not in mixedCase
Variable BONKI._hasLiqBeenAdded (Token.sol#211) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
Variable IRouter01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountADesired (Token.sol#69) is too similar to IRouter01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountBDesired (Token.sol#70)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar
INFO:Slither:Token.sol analyzed (7 contracts with 93 detectors), 44 result(s) found

TESTNET VERSION

1- Approve (passed):
https://testnet.bscscan.com/tx/0x73a5289fb713e99a86a715047bf694edd6f8e1e968e384ea3bbe05f1863c97a6

2- Multi Send Tokens (passed):
https://testnet.bscscan.com/tx/0xf463225e642a124ee966df4938d1ae630049fa9a3acdc0e95bc4aa189a04f5d7

3- Set Contract Swap Enable (passed):
https://testnet.bscscan.com/tx/0xe45f5f3fd7aaa457a2c828ee159e16a233a8c3b0821fc5f488090a7b2484aa85

4- Set Taxes (passed):
https://testnet.bscscan.com/tx/0x47f14c2963001e4ad5597341e27df0f924013139d39e0db162f4490ef23bc25f

5- Set Wallets (passed):
https://testnet.bscscan.com/tx/0x7cd698f8b17079421e600437aaef5dcc9b59d90d1014e6c45997b4c4df2146c0

6- Set Ratios (passed):
https://testnet.bscscan.com/tx/0x3eee303632da4bb94130cbd9050cfd2e1de80c2749a9a64cdeac5c05e7d68b25

7- Transfer (passed):
https://testnet.bscscan.com/tx/0x5b9cb25b6d4746db6e6f3b4d5a695343700fb4f702c29c8ef909b89575914ba3

MANUAL REVIEW

Severity Criteria

Expelee assesses the severity of disclosed vulnerabilities according to methodology based on OWASP standarts.

Vulnerabilities are dividend into three primary risk categroies:
High
Medium
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			

HIGH RISK FINDING

Enabling Trades

Category: Centralization
Category: Enable Trading
Status: Open
Severity: High

Overview:
The EnableTrading function permits only the contract owner to activate trading capabilities. Until this function is executed, no investors can buy, sell, or transfer their tokens. This places a high degree of control and centralization in the hands of the contract owner.

```
function enableTrading() public onlyOwner {
require(!tradingEnabled, "Trading already enabled!");
require(_hasLiqBeenAdded, "Liquidity must be added.");
if (address(initializer) == address(0)){
    initializer = Initializer(address(this));
  }
try initializer.setLaunch(lpPair, uint32(block.number),
uint64(block.timestamp), _decimals) {} catch {}
try initializer.getInits(balanceOf(lpPair)) returns (uint256
initThreshold, uint256 initSwapAmount) {
    swapThreshold = initThreshold;
    swapAmount = initSwapAmount;
  } catch {}
 tradingEnabled = true;
```

```
    allowedPresaleExclusion = false;
    launchStamp = block.timestamp;
}
```

Suggestion:

To reduce centralization and potential manipulation, consider one of the following approaches:

1. Automatically enable trading after a specified condition, such as the completion of a presale, is met.

2. If manual activation is still desired, consider transferring the ownership of the contract to a trustworthy, third-party entity like a certified "PinkSale Safu" developer. This can give investors more confidence in the eventual activation of trading capabilities, mitigating concerns of potential bad-faith actions by the original owner.

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 guarantess against the sale of team tokens or the removal of liquidity by the project audited in this document.

Always do your own research and project 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. Alway 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.