



Building the Futuristic **Blockchain** Ecosystem

SECURITY AUDIT REPORT

FELINE

TOKEN OVERVIEW

Risk Findings

Severity	Found
● High	1
● Medium	0
● Low	1
● Informational	2

Centralization Risks

Owner Privileges	Description
● Can Owner Set Taxes >25% ?	Not Detected
● Owner needs to enable trading ?	Yes, owner needs to enable trades
● 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

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 Trees	
10	Static analysis	
11	Testnet Version	
12	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	10 Feb 2024

CONTRACT DETAILS

Token Address: 0x1c32911A82A11c0AA20CAC38e46F3fBe2EB47639

Name: FELINE

Symbol: FLN

Decimals: 18

Network: BscScan

Token Type: BEP-20

Owner: 0x238e0E10e2727D397641A91237DbAF2e47C4Db3A

Deployer: 0x238e0E10e2727D397641A91237DbAF2e47C4Db3A

Token Supply: 10000000

Checksum: A17acbefe2a12642d388659dff20732

Testnet:

<https://testnet.bscscan.com/address/0xd4b39e426566b84c76918340512481612999b8ed#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 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.

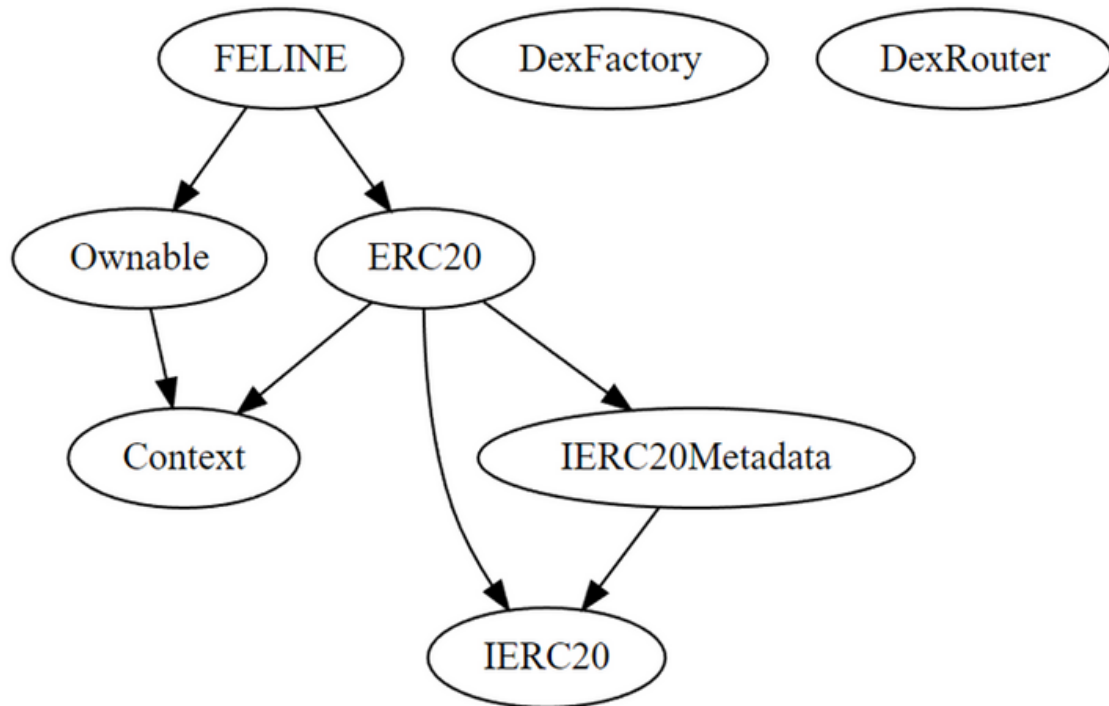
Low Risk

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

Informational

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

INHERITANCE TREE



STATIC ANALYSIS

```
INFO:Detectors:
Reentrancy in FELINE.internalSwap() (FELINE.sol#813-828):
  External calls:
    - swapToETH(balanceOf(address(this))) (FELINE.sol#819)
      - uniswapRouter.swapExactTokensForETHSupportingFeeOnTransferTokens(_amount,0,path,address(this),block.timestamp) (FELINE.sol#835-841)
    - (success) = marketingWallet.call{value: address(this).balance}() (FELINE.sol#820)
  External calls sending eth:
    - (success) = marketingWallet.call{value: address(this).balance}() (FELINE.sol#820)
  State variables written after the call(s):
    - isSwapping = false (FELINE.sol#826)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-2
INFO:Detectors:
Reentrancy in FELINE._transfer(address,address,uint256) (FELINE.sol#784-811):
  External calls:
    - internalSwap() (FELINE.sol#807)
      - uniswapRouter.swapExactTokensForETHSupportingFeeOnTransferTokens(_amount,0,path,address(this),block.timestamp) (FELINE.sol#835-841)
      - (success) = marketingWallet.call{value: address(this).balance}() (FELINE.sol#820)
  External calls sending eth:
    - internalSwap() (FELINE.sol#807)
      - (success) = marketingWallet.call{value: address(this).balance}() (FELINE.sol#820)
  Event emitted after the call(s):
    - Transfer(from,to,amount) (FELINE.sol#470)
      - super._transfer(_from,_to,toTransfer) (FELINE.sol#810)
Reentrancy in FELINE.internalSwap() (FELINE.sol#813-828):
  External calls:
    - swapToETH(balanceOf(address(this))) (FELINE.sol#819)
      - uniswapRouter.swapExactTokensForETHSupportingFeeOnTransferTokens(_amount,0,path,address(this),block.timestamp) (FELINE.sol#835-841)
    - (success) = marketingWallet.call{value: address(this).balance}() (FELINE.sol#820)
  External calls sending eth:
    - (success) = marketingWallet.call{value: address(this).balance}() (FELINE.sol#820)
  Event emitted after the call(s):
    - TransferFailed(marketingWallet,address(this).balance) (FELINE.sol#823)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-3
INFO:Detectors:
Context._msgData() (FELINE.sol#20-22) is never used and should be removed
ERC20._burn(address,uint256) (FELINE.sol#510-526) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Pragma version^0.8.0 (FELINE.sol#3) allows old versions
Pragma version^0.8.0 (FELINE.sol#30) allows old versions
Pragma version^0.8.0 (FELINE.sol#115) allows old versions
Pragma version^0.8.0 (FELINE.sol#200) allows old versions
Pragma version^0.8.0 (FELINE.sol#230) allows old versions
Pragma version0.8.19 (FELINE.sol#621) necessitates a version too recent to be trusted. Consider deploying with 0.8.18.
solc-0.8.19 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Low level call in FELINE.internalSwap() (FELINE.sol#813-828):
  - (success) = marketingWallet.call{value: address(this).balance}() (FELINE.sol#820)
Low level call in FELINE.withdrawStuckETH() (FELINE.sol#844-849):
  - (success) = address(msg.sender).call{value: address(this).balance}() (FELINE.sol#845-847)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
INFO:Detectors:
Function DexRouter.WETH() (FELINE.sol#633) is not in mixedCase
Event FELINE.marketingWalletChanged(address) (FELINE.sol#688) is not in CapWords
Parameter FELINE.setmarketingWallet(address)._newmarketing (FELINE.sol#708) is not in mixedCase
Parameter FELINE.setBuyTaxes(uint256)._marketingTax (FELINE.sol#723) is not in mixedCase
Parameter FELINE.setSellTaxes(uint256)._marketingTax (FELINE.sol#729) is not in mixedCase
Parameter FELINE.setSwapTokensAtAmount(uint256)._newAmount (FELINE.sol#734) is not in mixedCase
Parameter FELINE.setWhitelistStatus(address,bool)._wallet (FELINE.sol#748) is not in mixedCase
Parameter FELINE.setWhitelistStatus(address,bool)._status (FELINE.sol#749) is not in mixedCase
Parameter FELINE.checkWhitelist(address)._wallet (FELINE.sol#755) is not in mixedCase
Parameter FELINE.swapToETH(uint256)._amount (FELINE.sol#830) is not in mixedCase
Parameter FELINE.withdrawStuckTokens(address).BEP20_token (FELINE.sol#851) is not in mixedCase
Constant FELINE._totalSupply (FELINE.sol#661) is not in UPPER_CASE_WITH_UNDERSCORES
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
FELINE.slitherConstructorVariables() (FELINE.sol#656-862) uses literals with too many digits:
  - swapTokensAtAmount = _totalSupply / 100000 (FELINE.sol#676)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
INFO:Slither:FELINE.sol analyzed (8 contracts with 93 detectors), 31 result(s) found
```

TESTNET VERSION

1- Approve (passed):

<https://testnet.bscscan.com/tx/0xb0cc163fe6426c30e9159a03b4ba950cfb079343da13646a670983a15b9e1722>

2- Set Buy Taxes (passed):

<https://testnet.bscscan.com/tx/0xf9234e9f6317c7f6d77be57bc2e40da2608abaed616190df30f3396ca5e4ae8e>

3- Set Sell Taxes (passed):

<https://testnet.bscscan.com/tx/0x95d7f7fdb77d9ce03bc7442c66f227444cb7a22d6c1bf056f013391c4492233>

4- Enable Trading (passed):

<https://testnet.bscscan.com/tx/0x8b961bfbb0b64e22453fe06ec8f1a922bf525ede4cd1984a7eb63d9f1b276153>

5- Set Marketing Wallet (passed):

<https://testnet.bscscan.com/tx/0x71cedbc3916877e1999313514aa481d8985edfca5f4f16a784608331890b1f61>

MANUAL REVIEW

Severity Criteria

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

Vulnerabilities are divided into three primary risk categories:

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

Centralization – Enabling Trades

Severity: High

function: EnableTrading

Status: Open

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() external onlyOwner {  
    require(!tradingEnabled, "Trading is already enabled");  
    tradingEnabled = true;  
    startTradingBlock = block.number;  
}
```

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.

LOW RISK FINDING

Centralization – Missing Events

Severity: **Low**

subject: Missing Events

Status: Open

Overview:

They serve as a mechanism for emitting and recording data onto the blockchain, making it transparent and easily accessible.

```
function enableTrading() external onlyOwner {
  require(!tradingEnabled, "Trading is already enabled");
  tradingEnabled = true;
  startTradingBlock = block.number;
}

function setWhitelistStatus(
  address _wallet,
  bool _status
) external onlyOwner {
  whitelisted[_wallet] = _status;
  emit Whitelist(_wallet, _status);
}
```


INFORMATIONAL & OPTIMIZATIONS

Optimization

Severity: Informational

Subject: Floating Pragma.

Status: Open

Overview:

It is considered best practice to pick one compiler version and stick with it. With a floating pragma, contracts may accidentally be deployed using an outdated.

pragma solidity ^0.8.19;

Suggestion:

Adding the latest constant version of solidity is recommended, as this prevents the unintentional deployment of a contract with an outdated compiler that contains unresolved bugs.

INFORMATIONAL & OPTIMIZATIONS

Optimization

Severity: Optimization

subject: Remove unused code.

Status: Open

Overview:

Unused variables are allowed in Solidity, and they do. not pose a direct security issue. It is the best practice. though to avoid them

```
function _msgData() internal view virtual returns (bytes calldata) {  
    return msg.data;  
}
```


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](https://twitter.com/expeleeofficial)

 [expelee](https://medium.com/expelee)

 [Expelee](https://t.me/Expelee)

 [expelee](https://in.linkedin.com/company/expelee)

 [expelee_official](https://www.instagram.com/expelee_official)

 [expelee-co](https://github.com/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.

The logo for Expelee, featuring the word "expelee" in a stylized font. The "ex" is in white, and "pelee" is in orange. The letters are bold and modern.

Building the Futuristic **Blockchain Ecosystem**