



CFG NINJA AUDITS

Security Assessment

Wojakpot Token

July 9, 2023

Audit Status: Pass





Audit Edition: Advance













POWERED BY
BLADE POOL

Risk Analysis


















Classifications of Manual Risk Results

Classification	Description
 Critical	Danger or Potential Problems.
 High	Be Careful or Fail test.
 Low	Pass, Not-Detected or Safe Item.
 Informational	Function Detected

Manual Code Review Risk Results

Contract Privilege	Description
 Buy Tax	3%
 Sale Tax	3%
 Cannot Sale	Pass
 Cannot Sale	Pass
 Max Tax	5%
 Modify Tax	Yes
 Fee Check	Pass
 Is HoneyPot?	Not Detected
 Trading Cooldown	Not Detected
 Can Pause Trade?	Pass



Contract Priviledge	Description
 Pause Transfer?	Detected, already enabled.
 Max Tx?	Pass
 Is Anti Whale?	Not Detected
 Is Anti Bot?	Not Detected
 Is Blacklist?	Not Detected
 Blacklist Check	Pass
 is Whitelist?	Not Detected
 Can Mint?	Pass
 Is Proxy?	Not Detected
 Can Take Ownership?	Not Detected
 Hidden Owner?	Not Detected
 Owner	0xa9a72d15842A239B0D2fD62009239D77abCb7857
 Self Destruct?	Not Detected
 External Call?	Detected
 Other?	Detected
 Holders	1
 Auditor Confidence	Medium

The following quick summary it's added to the project overview; however, there are more details about the audit and its results. Please read every detail.



Project Overview

Token Summary

Parameter	Result
Address	0x066D75d3c0fA22c3819b2Bb4c096480b1C557DCF
Name	Wojakpot
Token Tracker	Wojakpot (WJP)
Decimals	18
Supply	1,000,000,000
Platform	Ethereum
compiler	v0.8.19+commit.7dd6d404
Contract Name	WojakpotToken
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://etherscan.io/address/0x066d75d3c0fa22c3819b2bb4c096480b1c557dcf#code
Payment Tx	Corporate



Project Overview

Simulation Summary

Parameter	Result
Transfer From Owner	Pass
Transfer From Holder	Pass
Add Liquidity	Pass
RemoveLiquidity	Pass
Buy from Owner	Pass
Buy from Holder	Pass
Sale from Owner	Pass
Sale from Holder	Pass
Remove Liquidity	Pass
SwapAndLiquify	Pass
SwapAndSale w/Fee	Pass
SwapAndSale TX	
SwapAndSaleNoFee	Pass
SwapAndSale No/Fee TX	
ExcludeFromFees	Pass
LaunchPad	N/A



Parameter	Result
Pool Creation	Pass
Pool Creation TX	
Pool Finalize	Pass
Pool Finalize TX	
Enable	Pass

The following quick summary it's added to the project overview; however, there are more details about the audit and its results. Please read every detail.



Main Contract Assessed

Contract Name

Name	Contract	Live
Wojakpot	0x066D75d3c0fA22c3819b2Bb4c096480b1C557DCF	Yes

TestNet Contract Assessed

Contract Name

Name	Contract	Live
Wojakpot	0xaDDF1F899098331C3ef5b5CeE6dcd13fC136e4eB	Yes

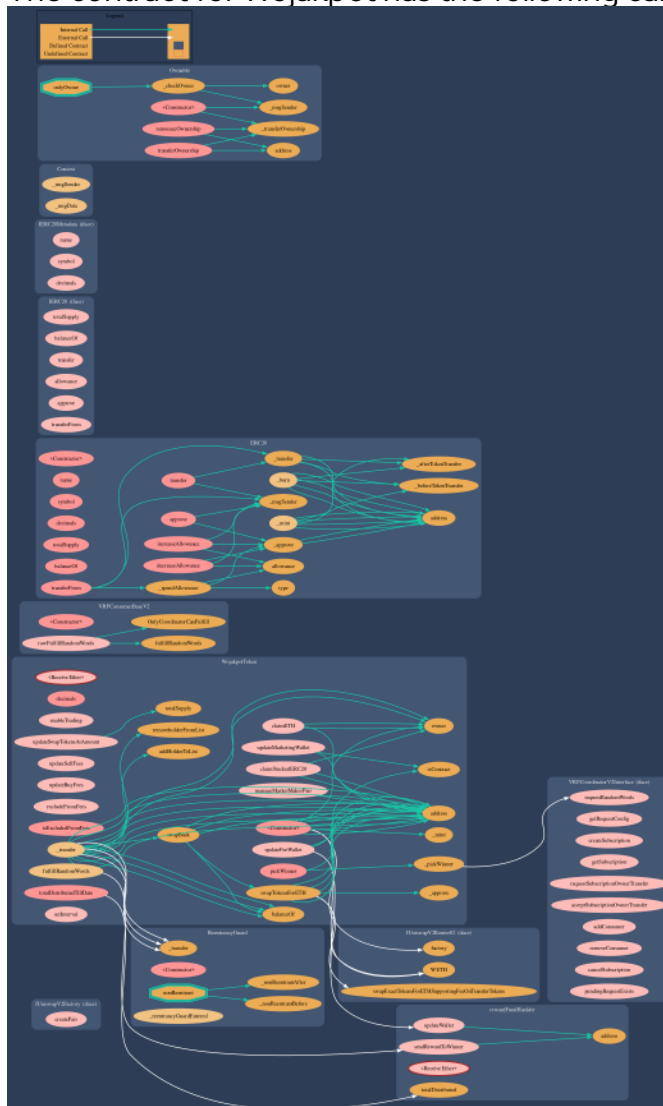
Solidity Code Provided

SolidID	File Sha-1	FileName
ELONMARK	aca27f38db0787295ae73e4bd8263bf3df62d704	wojakpotmainnet.sol
ELONMARK	3278ce43fda58736ad264cb8f121c7242d3a5838	VRFCoordinatorV2Interface.sol
ELONMARK	bde2c0e650a551d206abbc21ef3912e0c602d22e	VRFConsumerBaseV2.sol
ELONMARK	a9a540d525b9f251de46254a794eb2843a5113f7	ReentrancyGuard.sol



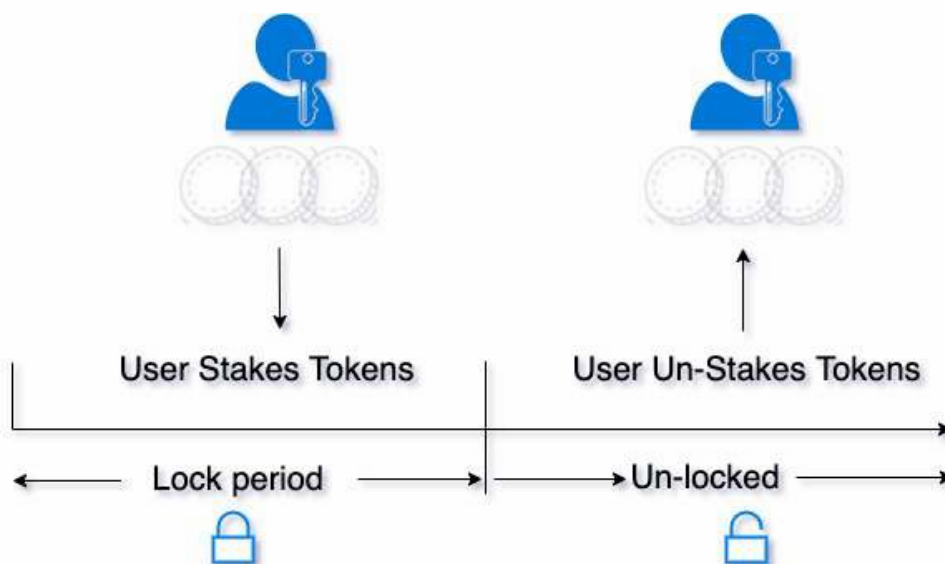
Call Graph

The contract for Wojakpot has the following call graph structure.



What is a Staking Contract

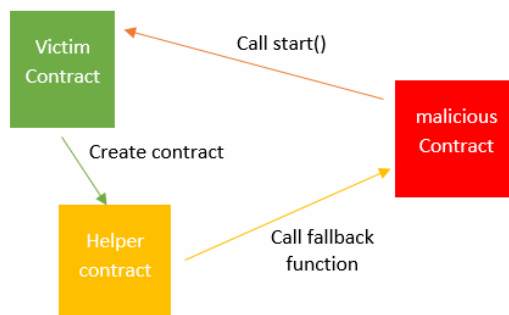
A smart contract which allows users to stake and un-stake a specified ERC20 token. Staked tokens are locked for a specific length of time (set by the contract owner at the outset). Once the time period has elapsed, the user can remove their tokens again.



The Project Owners of Wojakpot have implemented Reentrancy Guard Library

The Team has done a great job to avoid potential reentrancy issues in the contract.

You can read more about the reentrancy library used.
[ReentrancyGuard](#)



Smart Contract Vulnerability Checks

The Smart Contract Weakness Classification Registry (SWC Registry) is an implementation of the weakness classification scheme proposed in EIP-1470. It is loosely aligned to the terminologies and structure used in the Common Weakness Enumeration (CWE) while overlaying a wide range of weakness variants that are specific to smart contracts.

ID	Severity	Name	File	location
SWC-100	Pass	Function Default Visibility	wojakpotmainnet.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	wojakpotmainnet.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	wojakpotmainnet.sol	L: 0 C: 0
SWC-103	Pass	A floating pragma is set.	wojakpotmainnet.sol	L: 0 C: 0
SWC-104	Pass	Unchecked Call Return Value.	wojakpotmainnet.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	wojakpotmainnet.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	wojakpotmainnet.sol	L: 0 C: 0
SWC-107	Pass	Read of persistent state following external call.	wojakpotmainnet.sol	L: 0 C: 0
SWC-108	Pass	State variable visibility is not set..	wojakpotmainnet.sol	L: 0 C: 0
SWC-109	Pass	Uninitialized Storage Pointer.	wojakpotmainnet.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	wojakpotmainnet.sol	L: 0 C: 0



ID	Severity	Name	File	location
SWC-111	Pass	Use of Deprecated Solidity Functions.	wojakpotmainnet.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	wojakpotmainnet.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	wojakpotmainnet.sol	L: 0 C: 0
SWC-114	Pass	Transaction Order Dependence.	wojakpotmainnet.sol	L: 0 C: 0
SWC-115	Pass	Authorization through tx.origin.	wojakpotmainnet.sol	L: 0 C: 0
SWC-116	Pass	A control flow decision is made based on The block.timestamp environment variable.	wojakpotmainnet.sol	L: 0 C: 0
SWC-117	Pass	Signature Malleability.	wojakpotmainnet.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	wojakpotmainnet.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	wojakpotmainnet.sol	L: 0 C: 0
SWC-120	Pass	Potential use of block.number as source of randommness.	wojakpotmainnet.sol	L: 0 C: 0
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	wojakpotmainnet.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	wojakpotmainnet.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	wojakpotmainnet.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	wojakpotmainnet.sol	L: 0 C: 0
SWC-125	Pass	Incorrect Inheritance Order.	wojakpotmainnet.sol	L: 0 C: 0



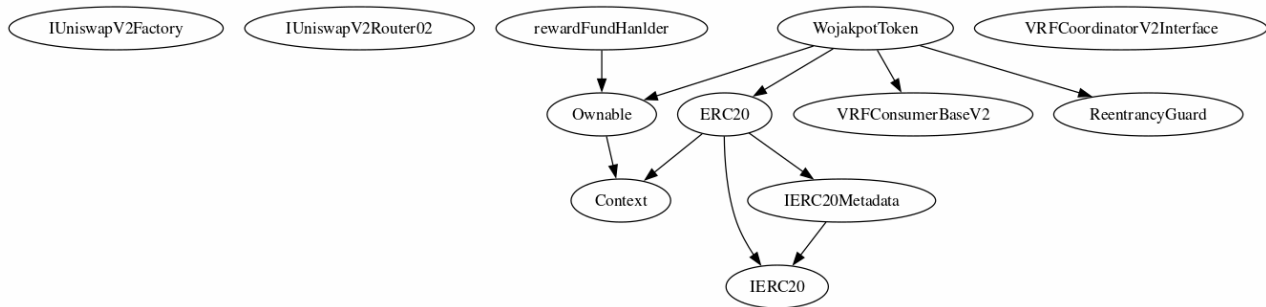
ID	Severity	Name	File	location
SWC-126	Pass	Insufficient Gas Griefing.	wojakpotmainnet.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	wojakpotmainnet.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	wojakpotmainnet.sol	L: 0 C: 0
SWC-129	Pass	Typographical Error.	wojakpotmainnet.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U +202E).	wojakpotmainnet.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	wojakpotmainnet.sol	L: 0 C: 0
SWC-132	Pass	Unexpected Ether balance.	wojakpotmainnet.sol	L: 0 C: 0
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	wojakpotmainnet.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	wojakpotmainnet.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/Dead Code).	wojakpotmainnet.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	wojakpotmainnet.sol	L: 0 C: 0

We scan the contract for additional security issues using MYTHX and industry-standard security scanning tools.



Inheritance

The contract for Wojakpot has the following inheritance structure.



Privileged Functions (onlyOwner)

Please Note if the contract is Renounced none of this functions can be executed.

Function Name	Parameters	Visibility
renounceOwnership		Public
transferOwnership	address newOwner	Public
setInterval		External
claimETH		External
claimStuckedERC20		External
updateFeeWallet		External
updateMarketingWallet		External
excludeFromFees		External
updateBuyFees		External
updateSellFees		External
updateSwapTokensAmount		External
enableTrading		External



Function Name	Parameters	Visibility
updateWallet		External
sendRewardToWinner		External



Smart Contract Advance Checks



ID	Severity	Name	Result	Status
WJP-01	Low	Potential Sandwich Attacks.	Pass	Not Detected
WJP-02	Informational	Function Visibility Optimization	Pass	Not Detected
WJP-03	Low	Lack of Input Validation.	Pass	Resolved
WJP-04	High	Centralized Risk In addLiquidity.	Pass	Not Detected
WJP-05	Low	Missing Event Emission.	Pass	Not Detected
WJP-06	Low	Conformance with Solidity Naming Conventions.	Pass	Not Detected
WJP-07	Low	State Variables could be Declared Constant.	Pass	Not Detected
WJP-08	Low	Dead Code Elimination.	Pass	Not Detected
WJP-09	High	Third Party Dependencies.	Fail	Detected
WJP-10	High	Initial Token Distribution.	Pass	Not Detected
WJP-11	Critical	pickWinner makes external call.	Fail	Detected
WJP-12	High	Centralization Risks In The X Role	Pass	Not Detected
WJP-13	Informational	Extra Gas Cost For User..	Pass	Not Detected
WJP-14	Medium	Unnecessary Use Of SafeMath	Pass	Not Detected
WJP-15	Medium	Symbol Length Limitation due to Solidity Naming Standards.	Pass	Not Detected



ID	Severity	Name	Result	Status
WJP-16	Medium	Taxes can be up to 100%	Pass	Not Detected
WJP-17	Logical Issue	Highly Permissive Role Access,	Pass	Not Detected
WJP-18	Critical	Stop Transactions by using Enable Trade.	Pass	Resolved



WJP-09 | Third Party Dependencies.

Category	Severity	Location	Status
Volatile Code	 High	wojakpotmainnet.sol: L: 168, C: 14	 Detected

Description

The contract is serving as the underlying entity to interact with third party `0x2Ca8E0C643bDe4C2E08ab1fA0da3401AdAD7734D` protocols. The scope of the audit treats 3rd party entities as black boxes and assume their functional correctness. However, in the real world, 3rd parties can be compromised and this may lead to lost or stolen assets. In addition, upgrades of 3rd parties can possibly create severe impacts, such as increasing fees of 3rd parties, migrating to new LP pools, etc.

Remediation



We understand that the business logic of Wojakpot requires interaction with `0x2Ca8E0C643bDe4C2E08ab1fA0da3401AdAD7734D`, etc. We encourage the team to constantly monitor the statuses of 3rd parties to mitigate the side effects when unexpected activities are observed.

Project Action

Ensure account has enough funds or vrf may fail.



WJP-11 | pickWinner makes external call..

Category	Severity	Location	Status
Security	 Critical	wojakpotmainnet.sol: L: 458 C: 14	 Detected

Description

pickWinner function makes external call to VRT Chainlink, this call depends on the owner subscription. if subscription runs out of funds this function may not work.

Remediation






ensure chainlink subscription has enough funds to pick the winner.

Project Action








Technical Findings Summary

Classification of Risk

Severity	Description
 Critical	Risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.
 High	Risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.
 Medium	Risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform
 Low	Risks can be any of the above but on a smaller scale. They generally do not compromise the overall integrity of the Project, but they may be less efficient than other solutions.
 Informational	Errors are often recommended to improve the code's style or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

Findings

Severity	Found	Pending	Resolved
 Critical	1	0	1
 High	1	0	0
 Medium	0	0	0
 Low	0	0	1
 Informational	0	0	0
Total	2	0	2



Social Media Checks

Social Media	URL	Result
Twitter	https://twitter.com/wojakpot	Pass
Other	https://www.instagram.com/wojakpot/	Pass
Website	https://wojakpot.vip/	Pass
Telegram	https://t.me/Wojakpot	Pass

We recommend to have 3 or more social media sources including a completed working websites.

Social Media Information Notes:

Auditor Notes: undefined

Project Owner Notes:



Assessment Results

Score Results

Review	Score
Overall Score	86/100
Auditor Score	80/100
Review by Section	Score
Manual Scan Score	20/33
SWC Scan Score	37 /37
Advance Check Score	29 /30

The Following Score System Has been Added to this page to help understand the value of the audit, the maximum score is 100, however to attain that value the project must pass and provide all the data needed for the assessment. Our Passing Score has been changed to 80 Points, if a project does not attain 80% is an automatic failure. Read our notes and final assessment below.

Audit Passed



Assessment Results

Important Notes:

- The customer has developed a contract token with a library from ChainLink to pick a winner.
- The customer has enabled trade. <https://etherscan.io/tx/0x9874837f417755d86f028636cf4ab873a2f463da0774da44e80fc170f471cdde>
- Please do your DYOR, the audit is not a validation or confirmation of project success. The contract has been tested and reviewed, please note the risk associated with the chainlink integration.

Auditor Score =80

Audit Passed



Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that act against the nature of decentralization, such as explicit ownership or specialized access roles in combination with a mechanism to relocate funds.

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimal EVM opcodes resulting in a reduction on the total gas cost of a transaction.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on how block.timestamp works.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functions being invoke-able by anyone under certain circumstances.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that may result in a vulnerability.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to make the codebase more legible and, as a result, easily maintainable.

Inconsistency

Inconsistency findings refer to functions that should seemingly behave similarly yet contain different code, such as a constructor assignment imposing different requirements on the input variables than a setter function.



Coding Best Practices

ERC 20 Coding Standards are a set of rules that each developer should follow to ensure the code meet a set of creterias and is readable by all the developers.



Disclaimer

CFGNINJA has conducted an independent security assessment to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the reviewed code for the scope of this assessment. This report does not constitute agreement, acceptance, or advocacy for the Project, and users relying on this report should not consider this as having any merit for financial advice in any shape, form, or nature. The contracts audited do not account for any economic developments that the Project in question may pursue, and the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude, and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are entirely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence, regardless of the findings presented. Information is provided 'as is, and CFGNINJA is under no covenant to audited completeness, accuracy, or solidity of the contracts. In no event will CFGNINJA or its partners, employees, agents, or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions or actions with regards to the information provided in this audit report.

The assessment services provided by CFGNINJA are subject to dependencies and are under continuing development. You agree that your access or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies with high levels of technical risk and uncertainty. The assessment reports could include false positives, negatives, and unpredictable results. The services may access, and depend upon, multiple layers of third parties.

