CFG NINJA

SECURITY ASSESSMENT

SFW Token

December 14, 2023

Audit Status: Fail

BLADE POOL

RISK ANALYSIS | SFW.

Classifications of Manual Risk Results

Classification	Description
🔴 Critical	Danger or Potential Problems.
🔴 High	Be Careful or Fail test.
🟠 Medium	Improve is needed.
🟢 Low	Pass, Not-Detected or Safe Item.
i Informational	Function Detected

Manual Code Review Risk Results

Contract Security	Description
🔴 Buy Tax	95%
🟢 Sale Tax	2.17%
🟢 Cannot Buy	Pass
🟢 Cannot Sale	Pass
🟢 Max Tax	5%
🟢 Modify Tax	Yes
🟢 Fee Check	Fail
🟢 Is Honeypot?	Not Detected
🟢 Trading Cooldown	Not Detected

Contract Security	Description
🟢 Enable Trade?	Pass
🟢 Pause Transfer?	Not Detected
🟢 Max Tx?	Pass
🟢 Is Anti Whale?	Not Detected
🟢 Is Anti Bot?	Not Detected
🟢 Is Blacklist?	Not Detected
🟢 Blacklist Check	Pass
ℹ is Whitelist?	Detected
🟢 Can Mint?	Pass
🟢 Is Proxy?	Not Detected
🟢 Can Take Ownership?	Not Detected
🟢 Hidden Owner?	Not Detected
ℹ Owner	No
🟢 Self Destruct?	Not Detected
🟢 External Call?	Not Detected
🟢 Other?	Not Detected
🟢 Holders	3
🟠 Audit Confidence	Medium

The summary section reveals the strengths and weaknesses identified during the assessment, including any vulnerabilities or potential risks that may exist. It serves as a valuable snapshot of the overall security status of the audited project. However, it is highly recommended to read the entire security assessment report for a comprehensive understanding of the findings. The full report provides detailed insights into the assessment process, methodology, and specific recommendations for addressing the identified issues.

CFG Ninja Verified on December 14, 2023

SFW

SECURITY CERTIFICATE · VERIFIED BY CFG NINJA

Executive Summary

TYPES	ECOSYSTEM	LANGUAGE
DeFi	BNBCHAIN	Solidity

Timeline

Audit Request	Onboarding Process	Audit Preview	Audit Release
2022-12-12	2022-12-12	2022-12-12	2022-12-12

Vulnerability Summary

4	0	4	4
Total Findings	Resolved	Pending	Unresolved

● 1 Critical	0 Resolved, 1 Pending	Critical risks are the most severe and can have a significant impact on the smart contracts functionality, security, or the entire system. These vulnerabilities can lead to the loss of user funds, unauthorized access, or complete system compromise.
● 0 High		High-risk vulnerabilities have the potential to cause significant harm to the smart contract or the system. While not as severe as critical risks, they can still result in financial losses, data breaches, or denial of service attacks.
● 1 Medium	0 Resolved, 1 Pending	Medium-risk vulnerabilities pose a moderate level of risk to the smart contracts security and functionality. They may not have an immediate and severe impact but can still lead to potential issues if exploited. These risks should be addressed to ensure the contracts overall security.
● 1 Low	0 Resolved, 1 Pending	Low-risk vulnerabilities have a minimal impact on the smart contracts security and functionality. They may not pose a significant threat, but it is still advisable to address them to maintain a robust security posture.
ⓘ 1 Informational	0 Resolved, 1 Pending	Informational risks are not actual vulnerabilities but provide useful information about potential improvements or best practices. These findings may include suggestions for code optimizations, documentation enhancements, or other non-critical areas for improvement.

PROJECT OVERVIEW | SFW.

Token Summary

Parameter	Result
Address	0x63B8e2109fA2E5ec8D26A19632E50560DbF310bf
Name	SFW
Token Tracker	SFW (SFW)
Decimals	18
Supply	1,000,000,000,000
Platform	BNBCHAIN
compiler	v0.8.19+commit.7dd6d404
Contract Name	XToken
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://bscscan.com/ token/0x63B8e2109fA2E5ec8D26A19632E50560DbF310bf#code

Main Contract Assessed

Name	Contract	Live
SFW	0x63B8e2109fA2E5ec8D26A19632E50560DbF310bf	Yes

TestNet Contract Assessed

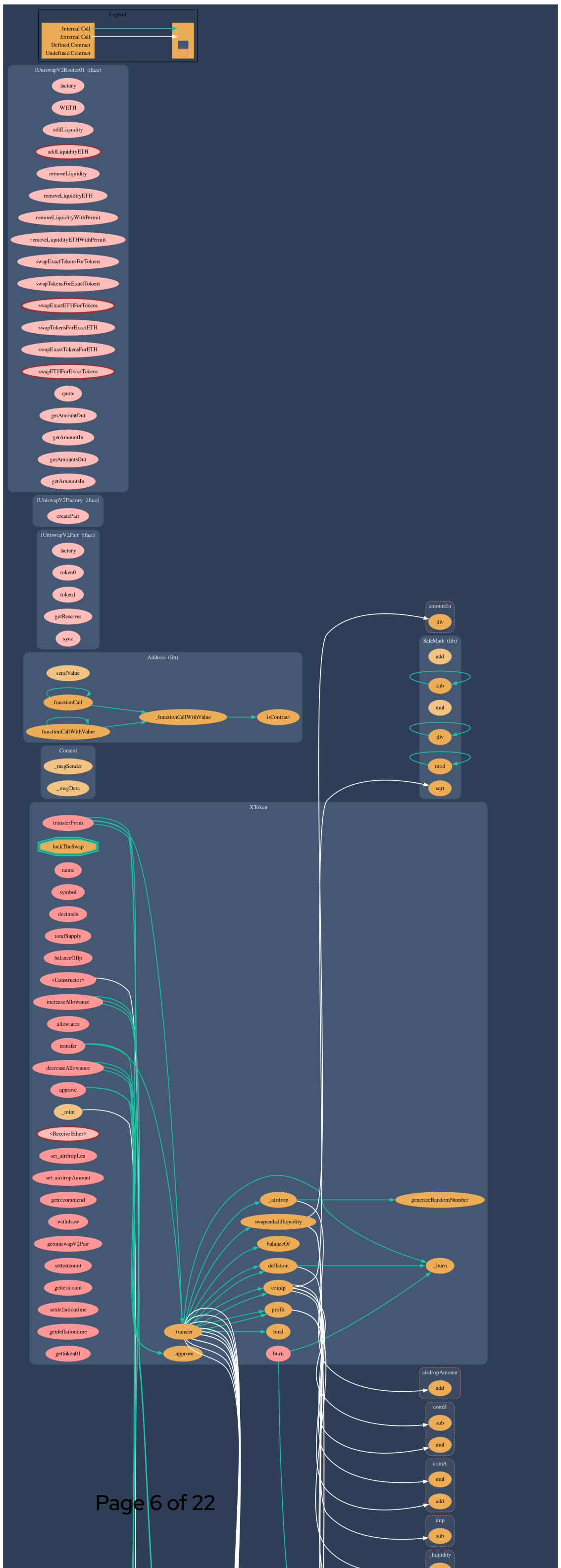
Name	Contract	Live
SFW	0x99a9487b8Bbe777987981b57AA990951A84A72B2	Yes

Solidity Code Provided

SolID	File Sha-1	FileName
SFW	a36bef7dc9e5fbf1ab302fd28d1a86f9c8fd9f99	SFW.sol

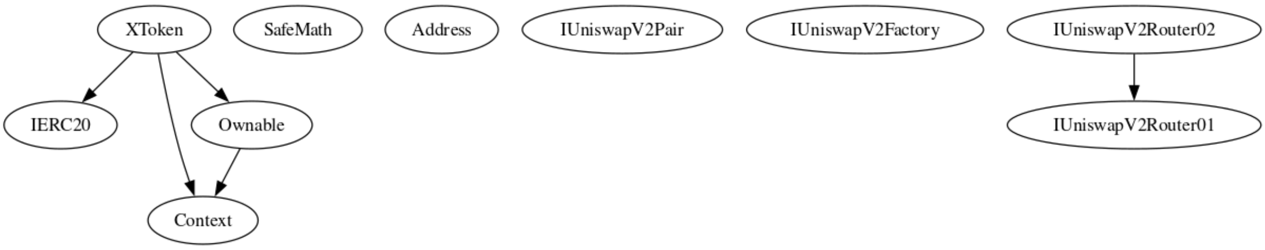
Call Graph

The Smart Contract Graph is a visual representation of the interconnectedness and relationships between smart contracts within a blockchain network. It provides a comprehensive view of the interactions and dependencies between different smart contracts, allowing developers and users to analyze and understand the flow of data and transactions within the network. The Smart Contract Graph enables better transparency, security, and efficiency in decentralized applications by facilitating the identification of potential vulnerabilities, optimizing contract execution, and enhancing overall network performance.



Inheritance Check

Smart contract inheritance is a concept in blockchain programming where one smart contract can inherit properties and functionalities from another existing smart contract. This allows for code reuse and modularity, making the development process more efficient and scalable. Inheritance enables the child contract to access and utilize the variables, functions, and modifiers defined in the parent contract, thereby inheriting its behavior and characteristics. This feature is particularly useful in complex decentralized applications (dApps) where multiple contracts need to interact and share common functionalities. By leveraging smart contract inheritance, developers can create more organized and maintainable code structures, promoting code reusability and reducing redundancy.



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	SFW.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	SFW.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	SFW.sol	L: 0 C: 0
SWC-103	Low	A floating pragma is set.	SFW.sol	L: 10 C: 0
SWC-104	Pass	Unchecked Call Return Value.	SFW.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	SFW.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	SFW.sol	L: 0 C: 0
SWC-107	Pass	Read of persistent state following external call.	SFW.sol	L: 0 C: 0
SWC-108	Low	State variable visibility is not set..	SFW.sol	L: 311 C: 13, L: 315 C: 12
SWC-109	Pass	Uninitialized Storage Pointer.	SFW.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	SFW.sol	L: 0 C: 0
SWC-111	Pass	Use of Deprecated Solidity Functions.	SFW.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	SFW.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	SFW.sol	L: 0 C: 0
SWC-114	Pass	Transaction Order Dependence.	SFW.sol	L: 0 C: 0
SWC-115	Pass	Authorization through tx.origin.	SFW.sol	L: 0 C: 0
SWC-116	Pass	A control flow decision is made based on The block.timestamp environment variable.	SFW.sol	L: 0 C: 0
SWC-117	Pass	Signature Malleability.	SFW.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	SFW.sol	L: 0 C: 0

ID	Severity	Name	File	location
SWC-119	Pass	Shadowing State Variables.	SFW.sol	L: 0 C: 0
SWC-120	Low	Potential use of block.number as source of randonmness.	SFW.sol	L: 601 C: 54
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	SFW.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	SFW.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	SFW.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	SFW.sol	L: 0 C: 0
SWC-125	Pass	Incorrect Inheritance Order.	SFW.sol	L: 0 C: 0
SWC-126	Pass	Insufficient Gas Griefing.	SFW.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	SFW.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	SFW.sol	L: 0 C: 0
SWC-129	Pass	Typographical Error.	SFW.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U+202E).	SFW.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	SFW.sol	L: 0 C: 0
SWC-132	Pass	Unexpected Ether balance.	SFW.sol	L: 0 C: 0
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	SFW.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	SFW.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/ Dead Code).	SFW.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	SFW.sol	L: 0 C: 0

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

Smart Contract Vulnerability Details | SWC-103 - Floating Pragma.

CWE-664: Improper Control of a Resource Through its Lifetime.

References:

Description:

Contracts should be deployed with the same compiler version and flags that they have been tested with thoroughly. Locking the pragma helps to ensure that contracts do not accidentally get deployed using, for example, an outdated compiler version that might introduce bugs that affect the contract system negatively.

Remediation:

Lock the pragma version and also consider known bugs (https://github.com/ethereum/solidity/releases) for the compiler version that is chosen.

Pragma statements can be allowed to float when a contract is intended for consumption by other developers, as in the case with contracts in a library or EthPM package. Otherwise, the developer would need to manually update the pragma in order to compile locally.

References:

Ethereum Smart Contract Best Practices - Lock pragmas to specific compiler version.

SMART CONTRACT VULNERABILITY DETAILS | SFW.

SWC-108 - State Variable Default Visibility.

CWE-710: Improper Adherence to Coding Standards

Description:

Labeling the visibility explicitly makes it easier to catch incorrect assumptions about who can access the variable.

Remediation:

Variables can be specified as being public, internal or private. Explicitly define visibility for all state variables.

References:

Ethereum Smart Contract Best Practices - Explicitly mark visibility in functions and state variables

Smart Contract Vulnerability Details | SWC-120 - Weak Sources of Randomness from Chain Attributes.

CWE-330: Use of Insufficiently Random Values

Description:

Solidity allows for ambiguous naming of state variables when inheritance is used. Contract A with a variable x could inherit contract B that also has a state variable x defined. This would result in two separate versions of x, one of them being accessed from contract A and the other one from contract B. In more complex contract systems this condition could go unnoticed and subsequently lead to security issues.

Shadowing state variables can also occur within a single contract when there are multiple definitions on the contract and function level.

Remediation:

Using commitment scheme, e.g. RANDAO. Using external sources of randomness via oracles, e.g. Oraclize. Note that this approach requires trusting in oracle, thus it may be reasonable to use multiple oracles. Using Bitcoin block hashes, as they are more expensive to mine.

References:

How can I securely generate a random number in my smart contract?)

When can BLOCKHASH be safely used for a random number? When would it be unsafe?

The Run smart contract.

TECHNICAL FINDINGS | SFW.

Smart contract security audits classify risks into several categories: Critical, High, Medium, Low, and Informational. These classifications help assess the severity and potential impact of vulnerabilities found in smart contracts.

Classification of Risk

Severity	Description
● Critical	Critical risks are the most severe and can have a significant impact on the smart contracts functionality, security, or the entire system. These vulnerabilities can lead to the loss of user funds, unauthorized access, or complete system compromise.
● High	High-risk vulnerabilities have the potential to cause significant harm to the smart contract or the system. While not as severe as critical risks, they can still result in financial losses, data breaches, or denial of service attacks.
● Medium	Medium-risk vulnerabilities pose a moderate level of risk to the smart contracts security and functionality. They may not have an immediate and severe impact but can still lead to potential issues if exploited. These risks should be addressed to ensure the contracts overall security.
● Low	Low-risk vulnerabilities have a minimal impact on the smart contracts security and functionality. They may not pose a significant threat, but it is still advisable to address them to maintain a robust security posture.
i Informational	Informational risks are not actual vulnerabilities but provide useful information about potential improvements or best practices. These findings may include suggestions for code optimizations, documentation enhancements, or other non-critical areas for improvement.

By categorizing risks into these classifications, smart contract security audits can prioritize the resolution of critical and high-risk vulnerabilities to ensure the contract's overall security and protect user funds and data.

SFW-13 | Extra Gas Cost For User.

Category	Severity	Location	Status
Logical Issue	ⓘ Informational	SFW.sol: L: 340 C: 14	Detected

Description

The user may trigger a tax distribution during the transfer process, which will cost a lot of gas and it is unfair to let
a single user bear it.

Recommendation

We advise the client to make the owner responsible for the gas costs of the tax distribution.

Mitigation

References:

Writing Clean Code for Solidity: Best Practices for Solidity Development

SFW-14 | Unnecessary Use Of SafeMath.

Category	Severity	Location	Status
Logical Issue	● Medium	SFW.sol: L: 0 C: 0	Detected

Description

The SafeMath library is used unnecessarily. With Solidity compiler versions 0.8.0 or newer, arithmetic operations
will automatically revert in case of integer overflow or underflow.
library SafeMath {
An implementation of SafeMath library is found.
using SafeMath for uint256;
SafeMath library is used for uint256 type in contract.

Recommendation

We advise removing the usage of SafeMath library and using the built-in arithmetic operations provided by the
Solidity programming language.

Mitigation

References:

Writing Clean Code for Solidity: Best Practices for Solidity Development

SFW-16 | Taxes can be up to 100%.

Category	Severity	Location	Status
Logical Issue	● Medium	SFW.sol: L: 0 C: 0	Detected

Description

The current definition of taxes can be set up to 100% for specific wallets, we suggest to modify the function not to be dynamic but to be a static resolution.

due to the logic written in here may results in a honeypot.

Recommendation

We advise the team to review the following logic..

Mitigation

References:

Writing Clean Code for Solidity: Best Practices for Solidity Development

FINDINGS

In this document, we present the findings and results of the smart contract security audit. The identified vulnerabilities, weaknesses, and potential risks are outlined, along with recommendations for mitigating these issues. It is crucial for the team to address these findings promptly to enhance the security and trustworthiness of the smart contract code.

Severity	Found	Pending	Resolved
● Critical	1	1	0
● High	0	0	0
● Medium	1	1	0
● Low	0	1	0
ⓘ Informational	1	1	0
Total	3	4	0

In a smart contract, a technical finding summary refers to a compilation of identified issues or vulnerabilities discovered during a security audit. These findings can range from coding errors and logical flaws to potential security risks. It is crucial for the project owner to thoroughly review each identified item and take necessary actions to resolve them. By carefully examining the technical finding summary, the project owner can gain insights into the weaknesses or potential threats present in the smart contract. They should prioritize addressing these issues promptly to mitigate any risks associated with the contract's security. Neglecting to address any identified item in the security audit can expose the smart contract to significant risks. Unresolved vulnerabilities can be exploited by malicious actors, potentially leading to financial losses, data breaches, or other detrimental consequences. To ensure the integrity and security of the smart contract, the project owner should engage in a comprehensive review process. This involves understanding the nature and severity of each identified item, consulting with experts if needed, and implementing appropriate fixes or enhancements. Regularly updating and maintaining the smart contract's codebase is also essential to address any emerging security concerns. By diligently reviewing and resolving all identified items in the technical finding summary, the project owner can significantly reduce the risks associated with the smart contract and enhance its overall security posture.

SOCIAL MEDIA CHECKS SFW.

Social Media	URL	Result
Website		Fail
Telegram		Fail
Twitter		Fail
Facebook		N/A
Reddit	N/A	N/A
Instagram		N/A
CoinGecko	N/A	N/A
Github		N/A
CMC	N/A	N/A
Other		Fail

From a security assessment standpoint, inspecting a project's social media presence is essential. It enables the evaluation of the project's reputation, credibility, and trustworthiness within the community. By analyzing the content shared, engagement levels, and the response to any security-related incidents, one can assess the project's commitment to security practices and its ability to handle potential threats.

Social Media Information Notes:

Auditor Notes: Website need improvements.

Project Owner Notes:

ASSESSMENT RESULTS | SFW.

Score Rsesults

Review	Score
Overall Score	73/100
Auditor Score	60/100

Review by Section	Score
Manual Scan Score	20
SWC Scan Score	31
Advance Check Score	22

Our security assessment or audit score system for the smart contract and project follows a comprehensive evaluation process to ensure the highest level of security. The system assigns a score based on various security parameters and benchmarks, with a passing score set at 80 out of a total attainable score of 100.The assessment process includes a thorough review of the smart contracts codebase, architecture, and design principles. It examines potential vulnerabilities, such as code bugs, logical flaws, and potential attack vectors. The evaluation also considers the adherence to best practices and industry standards for secure coding. Additionally, the system assesses the projects overall security measures, including infrastructure security, data protection, and access controls. It evaluates the implementation of encryption, authentication mechanisms, and secure communication protocols. To achieve a passing score, the smart contract and project must attain a minimum of 80 points out of the total attainable score of 100. This ensures that the system has undergone a rigorous security assessment and meets the required standards for secure operation.

AUDIT FAILED

Important Notes for SFW

- Since the VM version paris, "difficulty" was replaced by "prevrandao", which now returns a random number based on the beacon chain.

Auditor Score =60
Audit Fail

AUDIT
FAILED

Appendix

Finding Categories

Centralization / Privilege

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

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimalEVM 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 howblock.timestamp works.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functionsbeing 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 mayresult in a vulnerability.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to makethe 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 require statements on the input variables than a setterfunction.

Coding Best Practices

ERC 20 Conding 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

The purpose of this disclaimer is to outline the responsibilities and limitations of the security assessment and smart contract audit conducted by Bladepool/CFG NINJA. By engaging our services, the project owner acknowledges and agrees to the following terms:

1. Limitation of Liability: Bladepool/CFG NINJA shall not be held liable for any damages, losses, or expenses incurred as a result of any contract malfunctions, vulnerabilities, or exploits discovered during the security assessment and smart contract audit. The project owner assumes full responsibility for any consequences arising from the use or implementation of the audited smart contract. 2. No Guarantee of Absolute Security: While Bladepool/CFG NINJA employs industry-standard practices and methodologies to identify potential security risks, it is important to note that no security assessment or smart contract audit can provide an absolute guarantee of security. The project owner acknowledges that there may still be unknown vulnerabilities or risks that are beyond the scope of our assessment. 3. Transfer of Responsibility: By engaging our services, the project owner agrees to assume full responsibility for addressing and mitigating any identified vulnerabilities or risks discovered during the security assessment and smart contract audit. It is the project owner s sole responsibility to ensure the proper implementation of necessary security measures and to address any identified issues promptly. 4. Compliance with Applicable Laws and Regulations: The project owner acknowledges and agrees to comply with all applicable laws, regulations, and industry standards related to the use and implementation of smart contracts. Bladepool/CFG NINJA shall not be held responsible for any non-compliance by the project owner. 5. Third-Party Services: The security assessment and smart contract audit conducted by Bladepool/CFG NINJA may involve the use of third-party tools, services, or technologies. While we exercise due diligence in selecting and utilizing these resources, we cannot be held liable for any issues or damages arising from the use of such third-party services. 6. Confidentiality: Bladepool/CFG NINJA maintains strict confidentiality regarding all information and data obtained during the security assessment and smart contract audit. However, we cannot guarantee the security of data transmitted over the internet or through any other means. 7. Not a Financial Advice: Bladepool/CFG NINJA please note that the information provided in the security assessment or audit should not be considered as financial advice. It is always recommended to consult with a financial professional or do thorough research before making any investment decisions.

By engaging our services, the project owner acknowledges and accepts these terms and releases Bladepool/CFG NINJA from any liability, claims, or damages arising from the security assessment and smart contract audit. It is recommended that the project owner consult legal counsel before entering into any agreement or contract.