CFG NINJA AUDITS

Security Assessment
PAPI Token

May 28, 2023

Audit Status: Pass

Audit Edition: Pinksale

Risk Analysis

Classifications of Manual Risk Results

Classification	Description
🔴 Critical	Danger or Potential Problems.
🟠 Major	Be Careful or Fail test.
🟢 Minor	Pass, Not-Detected or Safe Item.
ℹ️ Informational	Function Detected

Manual Code Review Risk Results

Contract Priviledge	Description
🟢 Buy Tax	0
🟢 Sale Tax	0
🟢 Cannot Sale	Pass
🟢 Cannot Sale	Pass
ℹ️ Max Tax	0
ℹ️ Modify Tax	Not Detected
🟢 Fee Check	Pass
🟢 Is Honeypot?	Not Detected
🟢 Trading Cooldown	Not Detected
🟢 Can Pause Trade?	Pass
🟢 Pause Transfer?	Not Detected

Contract Priviledge	Description
🟢 Max Tx?	Pass
🟢 Is Anti Whale?	Not Detected
🟢 Is Anti Bot?	Not Detected
🟢 Is Blacklist?	Not Detected
ℹ️ Blacklist Check	Pass
🟢 is Whitelist?	Detected
🟢 Can Mint?	Pass
🟢 Is Proxy?	Not Detected
🟢 Can Take Ownership?	Not Detected
🟢 Hidden Owner?	Not Detected
ℹ️ Owner	0x1dc45dff134ff4138192f06b23fc84fc73d9d8ba
🟢 Self Destruct?	Not Detected
ℹ️ Other?	Detected
🟢 Other?	Not Detected
🟢 Holders	1
🟢 Auditor Confidence	Low

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	0x09Fa77BA4683F22475Ae5ce976d9bE65648a2462
Name	PAPI
Token Tracker	PAPI (PAPI)
Decimals	18
Supply	1,000,000,000
Platform	Binance Smart Chain
compiler	v0.8.4+commit.c7e474f2
Contract Name	StandardToken
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://bscscan.com/token/0x09fa77ba4683f22475ae5ce976d9be65648a2462#code
Payment Tx	0x635380d660decad0ca8c630c6647a48d14c5f964d905f67a362220c809600eff

Main Contract Assessed
Contract Name

Name	Contract	Live
PAPI	0x09Fa77BA4683F22475Ae5ce976d9bE65648a2462	Yes

TestNet Contract was Not Assessed

Solidity Code Provided

SolID	File Sha-1	FileName
Homer3D	68c8a59250f3173c0a20804ad2e550bdf04f9385	Homer3D.sol
Homer3D		
Homer3D		
Homer3D		

Call Graph

The contract for PAPI has the following call graph structure.
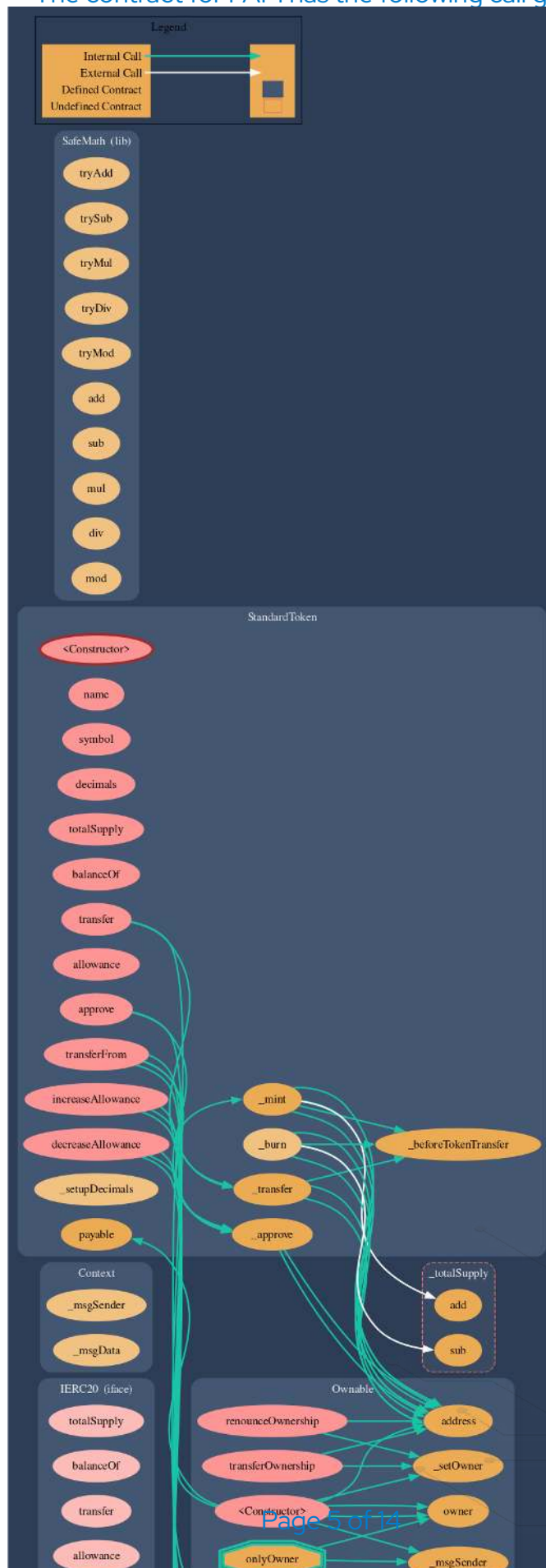
Smart Contract Vulnerability Checks

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SWC-102	Pass	Outdated Compiler Version file.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

CFG NINJA

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

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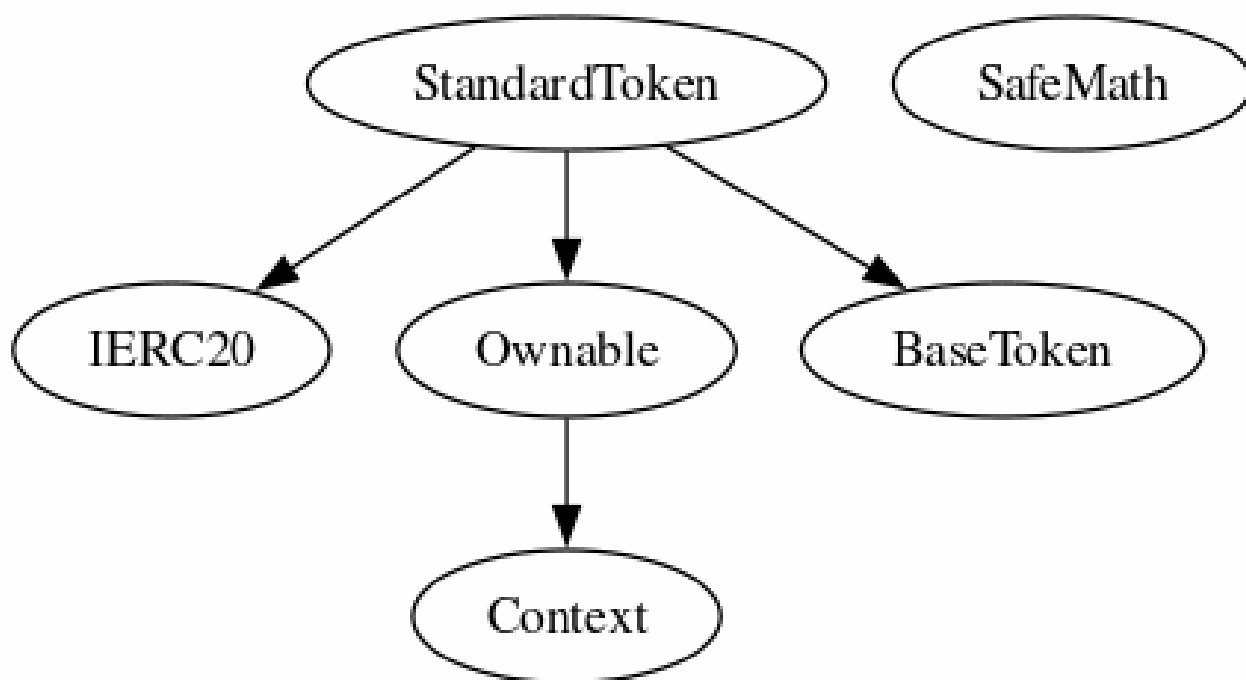
Social Media Checks

Social Media	URL	Result
Twitter	https://twitter.com/papitokenbsc	Pass
Other		Fail
Website	https://papicoin.xyz/	Pass
Telegram	https://t.me/papi_bsc	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:

Audit Result

Final Audit Score

Review	Score
Security Score	85
Auditor Score	80

The Following Score System Has been Added to this page to help understand the value of the audit, the maximun score is 100, however to attain that value the project most 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:

- No issues or vulnerabilities were found.

- This is a pinksale-generated standard token.

Auditor Score =80
Audit Passed

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

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 advocation 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.