

HEGUNINJA AUDITS



Security Assessment

GAFA Token

April 19, 2022

Table of Contents

1 Audit Summary

2 Project Overview

2.1 Token Summary

2.2 Main Contract Assessed

3 Smart Contract Vulnerability Checks

3.1 Mint Check

3.2 Fees Check

3.3 MaxTx Check

3.4 Pause Trade Check

4 Contract Ownership

5 Liquidity Ownership

6 Important Notes To The Users

7 Social Media Check(Informational)

8 Disclaimer



Audit Summary

This report has been prepared for GAFA Token on the Binance Smart Chain network. CFGNINJA provides both client-centered and user-centered examination of the smart contracts and their current status when applicable. This report represents the security assessment made to find issues and vulnerabilities on the source code along with the current liquidity and token holder statistics of the protocol.

A comprehensive examination has been performed, utilizing Cross Referencing, Static Analysis, In-House Security Tools, and line-by-line Manual Review.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Inspecting liquidity and holders statistics to inform the current status to both users and client when applicable.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Verifying contract functions that allow trusted and/or untrusted actors to mint, lock, pause, and transfer assets.



Project Overview

Token Summary

Parameter	Result
Address	0x495205d4c6307A73595C5C11B44Bee9B3418Ac69
Name	GAFA
Token Tracker	GAFA (GAFA)
Decimals	9
Supply	1,000,000,000
Platform	Binance Smart Chain
compiler	v0.8.13+commit.abaa5c0e
Contract Name	Gafa
Optimization	Yes with 200 runs
LicenseType	Unlicense
Language	Solidity
Codebase	https://bscscan.com/ token/0x495205d4c6307A73595C5C11B44Bee9B3418Ac69
Url	https://www.gafa.co/



Main Contract Assessed

Contract Name

Name	Contract	Live
GAFA	0x495205d4c6307A73595C5C11B44Bee9B3418Ac69	Yes

TestNet Contract Assessed

Contract Name

Name	Contract	Live
GAFA	0x1c476ca333Dc65D386Bd808C320c5e1B2B3D1423	Yes

Solidity Code Provided

SolID	FileNameMD5	FileName
Gafa	1e7fab51d91b73967f65f6816feb6100	Gafa.sol



Smart Contract Vulnerability Checks

Vulnerability	Automatic Scan	Manual Scan	Result
Unencrypted Private Data On-Chain	Complete	Complete	Low / No Risk
Code With No Effects	Complete	Complete	Low / No Risk
Message call with hardcoded gas amount	Complete	Complete	Low / No Risk
Hash Collisions With Multiple Variable Length Arguments	Complete	Complete	Low / No Risk
Unexpected Ether balance	Complete	Complete	Low / No Risk
Presence of unused variables	Complete	Complete	Low / No Risk
Right-To-Left-Override control character (U+202E)	Complete	Complete	Low / No Risk
Typographical Error	Complete	Complete	Low / No Risk
DoS With Block Gas Limit	Complete	Complete	Low / No Risk
Arbitrary Jump with Function Type Variable	Complete	Complete	Low / No Risk
Insufficient Gas Griefing	Complete	Complete	Low / No Risk
Incorrect Inheritance Order	Complete	Complete	Low / No Risk
Write to Arbitrary Storage Location	Complete	Complete	Low / No Risk
Requirement Violation	Complete	Complete	Low / No Risk
Missing Protection against Signature Replay Attacks	Complete	Complete	Low / No Risk



Mint Check

The Project Owners of GAFA does not have a mint function in the contract, owner cannot mint tokens after initial deploy

..

The Project has a Total Supply of 1,000,000,000 and cannot mint any more than the Max Supply.



Owner can't mint new coins



Fees Check

The Project Owners of GAFA does not have the ability to set fees higher than 25% .

Team May have fees defined, however they dont have the ability to set those fees higher than 25%.

 Fees can be changed up to a maximum of 25%



MaxTx Check

The Project Onwers of GAFA does not has the ability to set max tx amount

The Team allow any investors to swap, transfer or sale their total amount if needed.

Project Has No MaxTX



Pause Trade Check

The Project Owners of GAFA Owner can pause trading but he can't move tokens (Owner can't pause trading)

The Team has done a great job to avoid stop trading, and investors has the ability to trade at any given time without any problems

Pause Trade Notes:

Auditor Notes:

Project Owner Notes: Project Owners Ack



Contract Ownership

The contract ownership of GAFA is not currently renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible ownable functions that may alter the state of the protocol.

The current owner is the address 0x17Ea9b241AA0C6cE365261FFd5Af16782751Ab05 which can be viewed from:

[HERE](#)

The owner wallet has the power to call the functions displayed on the privileged functions chart below, if the owner wallet is compromised this privileges could be exploited.

We recommend the team to renounce ownership at the right timing if possible, or gradually migrate to a timelock with governing functionalities in respect of transparency and safety considerations.

We recommend the team to use a Multisignature Wallet if contract is not going to be renounced, this will give the ability to the team to have more control over the contract.

Liquidity Ownership

Most of the liquidity is currently locked, the lock can be seen here:

Liquidity Locker Link can be viewed from:

[HERE](#)



KYC Information

The Project Owners of GAFA has provided KYC Documentation.

KYC Certificated can be found on the Following:
[KYC Data](#)

KYC Information Notes:

Auditor Notes: Auditor asked project owner if there was any plans to KYC.

Project Owner Notes: Customer already KYC with Pinksale.



Mythx Security Summary Checks

ID	Severity	Name	File	location
SWC-100	Pass	Function .	Gafa.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	Gafa.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.		L: 0 C: 0
SWC-103	Low	A floating pragma is set.	Gafa.sol	L: 9 C: 0
SWC-103	Low	A floating pragma is set.	Gafa.sol	L: 79 C: 0
SWC-103	Low	A floating pragma is set.	Gafa.sol	L: 106 C: 0
SWC-103	Low	A floating pragma is set.	Gafa.sol	L: 184 C: 0
SWC-103	Low	A floating pragma is set.	Gafa.sol	L: 409 C: 0
SWC-103	Low	A floating pragma is set.	Gafa.sol	L: 439 C: 0
SWC-103	Low	A floating pragma is set.	Gafa.sol	L: 467 C: 0
SWC-103	Low	A floating pragma is set.	Gafa.sol	L: 498 C: 0
SWC-103	Low	A floating pragma is set.	Gafa.sol	L: 643 C: 0
SWC-103	Low	A floating pragma is set.	Gafa.sol	L: 672 C: 0



ID	Severity	Name	File	location
SWC-104	Pass	Unchecked Call Return Value.		L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.		L: 0 C: 0
SWC-106	Pass	Unprotected SE LFDESTRUCT Instruction		L: 0 C: 0
SWC-107	Low	Read of persistent state following external call.	Gafa.sol	L: 1120 C: 0
SWC-107	Low	Read of persistent state following external call.	Gafa.sol	L: 1187 C: 8
SWC-107	Low	Read of persistent state following external call.	Gafa.sol	L: 1190 C: 8
SWC-107	Low	Read of persistent state following external call.	Gafa.sol	L: 1191 C: 8
SWC-107	Low	Write to persistent state following external call.	Gafa.sol	L: 1180 C: 8
SWC-108	Low	State variable visibility is not set..	Gafa.sol	L: 1131 C: 14
SWC-108	Low	State variable visibility is not set.	Gafa.sol	L: 1132 C: 12



ID	Severity	Name	File	location
SWC-108	Low	State variable visibility is not set.	Gafa.sol	L: 1157 C: 33
SWC-109	Pass	Uninitialized Storage Pointer.		L: 0 C: 0
SWC-110	Pass	Assert Violation.		L: 0 C: 0
SWC-111	Pass	Use of Deprecated Solidity Functions.		L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.		L: 0 C: 0
SWC-113	Low	Multiple calls are executed in the same transaction.	Gafa.sol	L: 1180 C: 8
SWC-114	Pass	Transaction Order Dependence.		L: 0 C: 0
SWC-115	Pass	Authorization through tx.origin.		L: 0 C: 0
SWC-116	Low	A control flow decision is made based on The block.timestamp environment variable.	Gafa.sol	L: 1205 C: 8
SWC-117	Pass	Signature Malleability.		L: 0 C: 0



ID	Severity	Name	File	location
SWC-118	Pass	Incorrect Constructor Name.		L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.		L: 0 C: 0
SWC-120	Pass	Weak Sources of Randomness from Chain Attributes.		L: 0 C: 0
SWC-121	Pass	Missing Protection against Signature Replay Attacks.		L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.		L: 0 C: 0
SWC-123	Pass	Requirement Violation.		L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.		L: 0 C: 0
SWC-125	Pass	Incorrect Inheritance Order.		L: 0 C: 0
SWC-126	Pass	Insufficient Gas Griefing.		L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.		L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.		L: 0 C: 0



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

We scan the contract for additional security issues using MYTHX and industry standard security scanning tool



Privileged Functions (onlyOwner)

Function Name	Parameters	Visibility
renounceOwnership	none	public
transferOwnership	address newOwner	public
setEnableAntiBot	(bool _enable)	external
excludeFromFee	address account	public
includeInFee	address account	public
setAllFeePercent	uint256 liquidityFee, uint256 gameRewardFee	external
lock	uint256 time	external
setSaleFeePercent	uint256 liquidityFee, uint256 gameRewardFee	external
setSaleLiquidityFeePercent	uint256 liquidityFee	external
setNumTokensSellToAddToLiquidity	uint256 _minimumTokensBeforeSwap	external
setpinkAntiBotAddress	address _AntiBotAddress	external
setSwapAndLiquifyEnabled	bool _enabled	public
setgameRewardWalletAddresses	address _gameRewardWallet	external



Important Notes To The Users:

- The team has not provided a KYC Link during the time of assessment and can be found in the Audit.
- No mint function found, owner cannot mint tokens after initial deploy.
- Smart contract uses Rebase. With Rebase, the circulating token supply adjusts (increases or decreases) automatically or manually according to defined parameters in the contract.
- Owner can't change fees up to 25%.
- Owner can't set max tx amount.
- Owner can't pause trading.
- No high-risk Exploits/Vulnerabilities Were Found in the Source Code.
-

Audit Passed



Social Media Checks

Social Media	URL	Result
Twitter	https://twitter.com/gafaexperience	Pass
Instagram	https://www.instagram.com/gafacoin	Pass
Website	https://www.gafa.co/	Pass
Telegram	https://t.me/+1Nzvi4LJ2lw4ZTYy	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:



Disclaimer

CFGNINJA has conducted an independent audit to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the codes that were provided for the scope of this audit. This audit report does not constitute agreement, acceptance or advocacy for the Project that was audited, and users relying on this audit 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 may be pursued by the Project in question, and that 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 completely free of exploits, bugs, vulnerabilities or depreciation 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 in this report. Information is provided 'as is', and CFGNINJA is under no covenant to the completeness, accuracy or solidity of the contracts audited. 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 and/or actions with regards to the information provided in this audit report.

The assessment services provided by CFGNINJA is subject to dependencies and under continuing development. You agree that your access and/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 and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

