SECURITY
ASSESSMENT
REPORT

PREPARED FOR

BFF Gram

@astrobiatech

TABLE OF CONTENTS

⊕ astrobiatech.in

SCOPE OF AUDIT

The scope of this audit was to analyze and document the BFF GRAM smart contract codebase for quality, security, and correctness.

CHECKED VULNERABILITIES

We have scanned the smart contract for commonly known and more specific vulnerabilities. Here are some of the commonly known vulnerabilities that we considered:

- Re-entrancy
- Timestamp Dependence
- Gas Limit and Loops
- DoS with Block Gas Limit
- Transaction-Ordering Dependence
- Use of tx.origin
- Exception disorder
- Gasless send
- Balance equality
- Byte array
- Transfer forwards all gas
- ERC20 API violation
- Malicious libraries
- Compiler version not fixed
- Redundant fallback function
- Send instead of transfer
- Style guide violation
- Unchecked external call
- Unchecked math
- Unsafe type inference
- Implicit visibility level

TECHNIQUES & METHODS

Throughout the audit of smart contract, care was taken to ensure:
- The overall quality of code.
- Use of best practices.
- Code documentation and comments match logic and expected behaviour.
- Token distribution and calculations are as per the intended behaviour mentioned in the whitepaper.
- Implementation of ERC-20 token standards.
- Efficient use of gas.
- Code is safe from re-entrancy and other vulnerabilities.

The following techniques, methods and tools were used to review all the smart contracts.

Static Analysis

Static Analysis of Smart Contracts was done to identify contract vulnerabilities. In this step a series of automated tools are used to test security of smart contracts.

Code Review / Manual Analysis

Manual Analysis or review of code was done to identify new vulnerability or verify the vulnerabilities found during the static analysis. Contracts were completely manually analyzed, their logic was checked and compared with the one described in the whitepaper. Besides, the results of automated analysis were manually verified.

ISSUE CATEGORIES

Every issue in this report has been assigned with a severity level. There are four levels of severity and each of them has been explained below.

- ## HIGH SEVERITY ISSUES

  A high severity issue or vulnerability means that your smart contract can be exploited. Issues on this level are critical to the smart contract's performance or functionality and we recommend these issues to be fixed before moving to a live environment.

- ## MEDIUM SEVERITY ISSUES

  The issues marked as medium severity usually arise because of errors and deficiencies in the smart contract code. Issues on this level could potentially bring problems and they should still be fixed.

- ## LOW SEVERITY ISSUES

  Low level severity issues can cause minor impact and or are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future.

- ## INFORMATIONAL

  These are severity four issues which indicate an improvement request, a general question, a cosmetic or documentation error, or a request for information. There is low-to-no impact.

ISSUES TABLE

TYPE	HIGH	MEDIUM	LOW	INFORMATIONAL
OPEN	-	-	-	3
ACKNOWLWDGENT	-	-	-	-
CLOSED	-	-	-	-

INTRODUCTION

During the period of April 22 , 2023 to April 23 , 2023 – Astrobiatech Blockchain Security Team performed a security audit for COREDOGE smart contracts.

CONTRACT NAME	BFF GRAM
CONTRACT ADDRESS	0x5DF8335Ea6d77a3534A84E4D387BB0fAbCcC6883
BLOCKCHAIN	Binance
TOTAL SUPPLY	2,000,000,000 BFFG
COMPILER VERSION	v0.8.19+commit.7dd6d404
DECIMALS	9

OVERVIEW

CONTRACT ADDRESS
0x5DF8335Ea6d77a3534A84E4D387BB0fAbCcC6883

TOKEN TRACKER
BFF Gram (BFFG)

CONTRACT CREATOR
0x0d306035889b00b94d155cc8edd65a62e4e2c153

OWNER ADDRESS
0x0d306035889b00b94d155cc8edd65a62e4e2c153

SOURCE CODE
Contract Source Code Verified at Bscscan

CONTRACT NAME
BFFG

OTHER SETTINGS
default evmVersion, Unlicense license

COMPILER VERSION
v0.8.19+commit.7dd6d404

OPTIMIZATION ENABLED
Yes with 500 runs

Code is truncated to fit the constraints of this document.
The code in its entirety can be viewed here.

astrobiatech.in

ISSUES

Informational

1. ### Unlocked Compiler Version

   Description:-

   The contract has unlocked compiler version. An unlocked compiler version in the source code of the contract permits the user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to different compiler versions.

   Recommendation:-

   We advise that the compiler version is instead locked at the lowest version possible that the contract can be compiled at.

   Status :- Not Fixed

2. ### DoS with block gas limit

   Description: -

   If the gas requirement of a function is higher than the block gas limit, it cannot be executed.

   Recommendation: -

   We advise avoid loops in your functions or actions that modify large areas of storage.

   Status :- Not Fixed

3. ### Function name must be in mixedCase

   Description :-

   The used function name contains some only capital letters

   Recommendation :-

   We advise to make all funtions name in mixed letter.

   Status :- Not Fixed

FUNCTIONAL TEST

FUNCTIONS NAME	TESTING RESULT
approve	Passed
burn	Passed
changeOwnership	Found
mint	Passed
release	Passed
transfer	Passed
transferFrom	Passed

astrobiatech.in

FEES

BUY FEES	4%
Marketing	1%
Team	1%
Development	1%
Auto Liquidity	1%

SELL FEES	5%
Marketing	1%
Team	1%
Development	1%
Auto Liquidity	2%

⊕ astrobiatech.in

HOLDERS

A total of 1 token holder

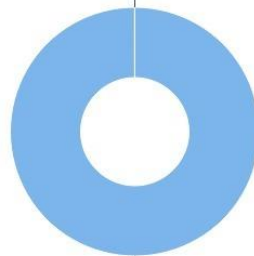| Rank	Address	Quantity	Percentage	Analytics
1	0x0d306035889b00b94d155cc8edd65a62e4e2c153	2,000,000,000	100.0000%	

The top 100 holders collectively own 100.00% (2,000,000,000.00 Tokens) of BFF Gram   Token Total Supply: 2,000,000,000.00 Token | Total Token Holders: 1

BFF Gram Top 100 Token Holders

Source: BscScan.com

OTHER ACCOUNTS

0x0d306035889b00b94d155cc8edd65a62e4e2c153

(A total of 2,000,000,000.00 tokens held by the top 100 accounts from the total supply of 2,000,000,000.00 token)
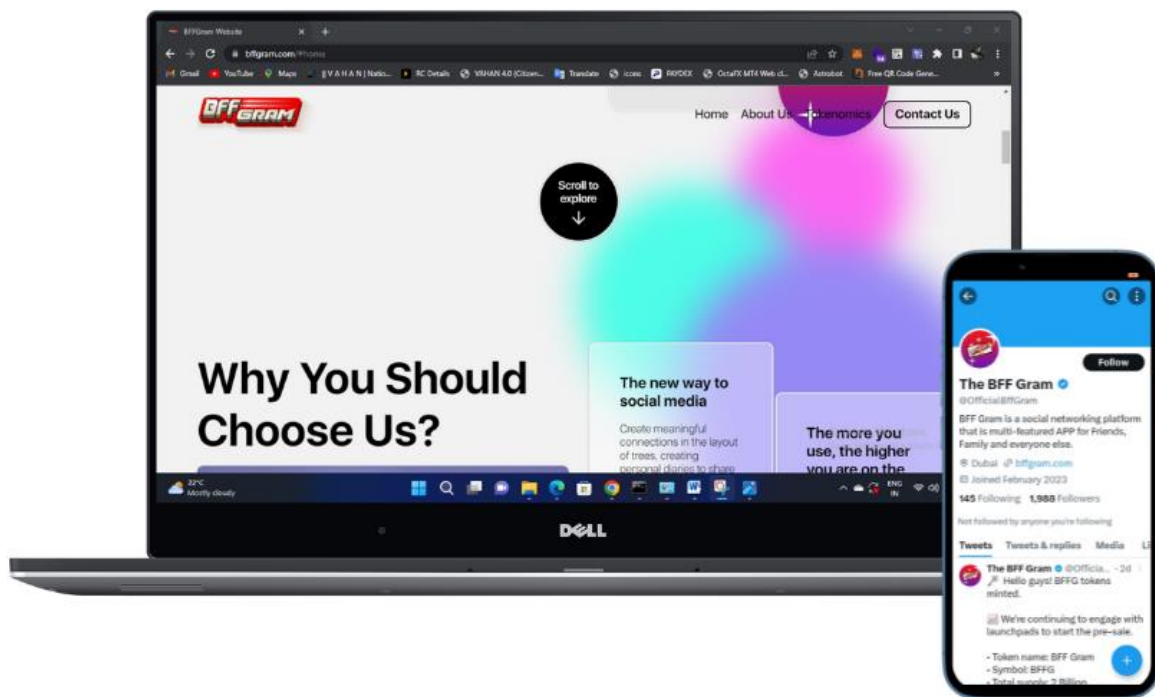
⊕ astrobiatech.in

SUMMARY

In this report, we have considered the security of the BFF GRAM platform. We performed our audit according to the procedure described above. 0 high , 0 medium, 0 low, and 3 informational severity were discovered during the audit.

⊕ astrobiatech.in

SOCIAL PROFILES

WEBSITE	https://www.bffgram.com/
EMAIL	contactus@bffgram.com
TELEGRAM	https://t.me/bffgramofficial
TWITTER	https://twitter.com/OfficialBffGram
SNAPCHAT	https://t.snapchat.com/UCf6B9na
LINKEDIN	https://www.linkedin.com/company/the-bff-gram/

astrobiatech.in

DISCLAIMER

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and Astrobiatech Blockchain Security and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Astrobiatech Blockchain Security) owe no duty of care towards you or any other person, nor does Astrobiatech Blockchain Security make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and Astrobiatech Blockchain Security hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, Astrobiatech Blockchain Security hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Astrobiatech Blockchain Security, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

⊕ astrobiatech.in

Proofed by Astrobiatech

ASTROBIATECH
BLOCKCHAIN SECURITY

https://astrobiatech.in

@astrobiatech