



WagyuSwap BEP20 Token Audit V1

Prepared by:

Jorge Martinez
Walther Villatoro

Version: 1

Date: Oct 9, 2021



Table of Contents

1. Project Information.....	3
1.1 Project Scope.....	3
1.2 Issue Classification.....	4
2. Process Details.....	5
2.1 Analysis	5
2.2 Auditing Process.....	5
2.3 Test Results	6



1. Project Information

1.1 Project Scope

We were tasked with auditing the WagyuSwap smart contract platform. This audit process pertains to the \$WAG BEP20 Token provided to us by the WagyuSwap development team on October 1st, 2021. The files within scope of this audit are:

File	MD5
./contracts/WAG.sol	8805b92c78aac652686e8fc7c8455f89

And can be found at here <https://github.com/TheBlockchainAuditor/WAG-audit> on git commit 761f025e4dc339a002b150fcf4fa37648d84d78f.

We modularized the code into separate contracts to ease the testing of the code.



1.2 Issue Classification

Informational

This issue relates to style and security best practices but does not pose an immediate risk.

Low

An issue classified as informational does not pose an immediate threat to disruption of functionality and could not be exploited on a recurring basis, however, it should be considered for security best practices or code integrity.

Medium

An issue classified as medium has relatively small risk and isn't exploitable to circumvent desired functionality and could not have financial consequences but could put user's sensitive information at risk.

Critical

These issues in the smart contract can have catastrophic implications that could ruin your reputation, disrupt the contract's functionality, and impact the client and your user's sensitive information.





2. Process Details

2.1 Analysis

This audit is a review of security best practices of the \$WAG BEP20 contract. The contract was shared with us on the Binance Smart Chain Testnet at the following url <https://bscscan.com/address/0x8a113d475664dd68fb827498d599853835097db0>.

The \$WAG token inherits the ERC20.sol, Ownable.sol, and LGEWhitelisted contracts from [@openzeppelin/contracts-ethereum-package3.0.0](https://github.com/OpenZeppelin/contracts-ethereum-package) which is code that has been thoroughly audited and battle tested time and time again.

As part of our auditing process we tested and verified the behavior of the \$WAG BEP20 and antibot whitelisting smart contracts. Through the process we found:



In this analysis, we did not find any issues in the provided contract.

2.2 Auditing Process

This section describes the auditing process that was followed to test the \$WAG BEP Token. We deployed a local instance of the PancakeSwap protocol to develop a testing environment that most realistically simulates the live environment. We created a pair and added liquidity to it so that simulated traders can swap tokens from the simulated liquidity pool. This allowed for proper testing of the antibot whitelist. In addition, we also verified that the \$WAG token is BEP20 compliant. With the environment properly simulated we developed a custom test suite that covered the attack space. The requirements and specifications were inspected thoroughly while constructing the test suite to verify its intended functionality. The results of the tests are detailed below in section 2.3.



2.3 Test Results

WagyuSwap BEP20 Contract Test Suite

Deployment

- ✓ should be called WAGYUSWAP.app
- ✓ Should have the symbol WAG
- ✓ Should have a total supply of 500000000
- ✓ Should have 18 decimals
- ✓ Should give allowance to a spender of approved amount (59ms)
- ✓ Should increase the allowance of a spender (51ms)
- ✓ Should decrease the allowance of a spender (86ms)

Trading

- ✓ should take a 10% fee when selling tokens on pancakeswap (336ms)

allowance

- ✓ allowance works as expected (223ms)

approve

- ✓ cannot approve the zero address to move your tokens (46ms)

transferFrom

- ✓ allows you transfer an address' tokens to another address (71ms)

Ownership

- ✓ only the owner can transfer ownership to another address (94ms)

- ✓ owner cannot transfer ownership to the zero address

- ✓ the owner can renounce ownership of the contract (51ms)

Whitelist

- ✓ creating the LGE whitelist requires duration and amountsMax of equal length (63ms)
- ✓ Adding liquidity activates the whitelist (676ms)
- ✓ transferring tokens reverts if you're not on the whitelist (113ms)
- ✓ whitelisters cannot buy more than the specified amount max (144ms)
- ✓ whitelist admin can add whitelist addresses using modifyLGEWhitelist (75ms)
- ✓ whitelist admin can modify the whitelist duration (80ms)
- ✓ whitelist admin can modify the max tokens that can be bought during the whitelist (74ms)
- ✓ whitelist admin can call the modifyLGEWhitelist and not change anything (57ms)
- ✓ when the whitelist round is over, getLGEWhitelistRound returns 0 (105ms)
- ✓ whitelist admin cannot modify a whitelist that doesn't exist (39ms)
- ✓ whitelist admin can renounce their whitelister permissions (84ms)
- ✓ whitelist admin can tranfer their whitelisting permission to another address (166ms)
- ✓ whitelist admin cannot transfer their whitelisting permission to the zero address (89ms)

Configuration

- ✓ Should allow owner to change the router
- ✓ Should not let the fees be greater than 20%
- ✓ Should not let fee reward address be the zero address (57ms)

30 passing (6s)

File	% Stmt	% Branch	% Funcs	% Lines	Uncovered Lines
contracts\LGWhitelisted.sol	93.97	76.79	96.77	94.07	
WagyuToken.sol	100	85.29	100	100	
All files	93.97	76.79	96.77	94.07	... 219,220,221

Since its successful launch, WagyuSwap has seen millions of dollars in daily volume. Our audit has found no security vulnerabilities and we are proud to have been a part of making the WagyuSwap smart contract platform safer and more reliable.





The Blockchain Auditor
