Quick Audit Report

For **BonusUSDT**

0xF914BC1Cc1A4529E2B17Ed1B7694306d9F94637e

CHECK POINT

Instruments:

Smart Contract Weakness Classification and Test Cases [SWC-[100:136]]
Common Weakness Enumeration [CWE]
OWASP Risk Rating Methodology

Audit Results

Risk Level:

○	○	○	●	○
Weakness	Low	Medium	**High**	Critical

1

The owner of contract can grant any wallet address Admin rights, which allows users to set various variables in the ecosystem

2

Any authorized admin can to modify a 'liquidity fee', a 'dev fee', a 'market fee' and a 'reflect fee' to any percentage at any time

3

The owner can blacklist wallets from purchasing or selling the coins they hold. This might deter investors from purchasing the coin

4

This essentially makes the token become a honeypot to that address, and makes transferring any native tokens impossible

We strongly recommend that BonusUSDT conduct Full Token Security Audit to ensure trust in the team as they have notable control within the ecosystem

www.checkpoint.report
Telegram: @checkpointreport
Github: @checkpointreport