Original audit

https://www.certik.com/projects/doxy-finance

Medium severity issues

- ## CENTRALIZING RISK ON MANY FUNCTIONS

In the functions shown below, there is centralization risk because only the owner can access them and make changes.

whitelistAddress;

rescueBNBFromContract;

setRouterAddress;

rescueBEPTokenFromContract;

rescueTokenFromContract;

transferOwnership;

Remediation

The risk describes the current project design and potentially makes iterations to improve in the securityoperation and level of decentralization, which in most cases cannot be resolved entirely at the presentstage. We advise the client to carefully manage the privileged account's private key to avoid any potentialrisks of being hacked. In general, we strongly recommend centralized privileges or roles in the protocol beimproved via a decentralized mechanism or smart-contract-based accounts with enhanced securitypractices, e.g., multisignature wallets.

Low severity issues

- ## VARIABLES THAT COULD BE DECLARED AS IMMUTABLE

The below variables can be set as immutable because don't get a change in contract.

uint256 public burnPercent = 10;

address public strategicSalesWallet = payable(0x7E3265C0EA866880fc841dFC0FdAcB9cAfcC1Eec);

address public liquidityWallet = payable(0xEed053faa4Ca68080214C39dD865f061778b2DA8) ;

address public marketingWallet = payable(0x0cF2238c9a7de47230BEC4D43374E9ef40Fb9044) ;

address public gameOperationsWallet = payable(0x20299F7Ca816fB9e93772ECb0590E3fAf4138835) ;

address public teamWallet = payable(0x8427854b5d433e7b858607D06089E3062BEb838B) ;

address public communityAirdropWallet = payable(0xFD2b59E77ddAF0153034D378257057391cF0A04C) ;

address stakingAddress = payable(0x658DB9eC9B452c6eEbAa4b248B34bf62B6B92981) ;

Remediation

We advise using the constructor function and adding these variables as immutable in the contract. Immutable state variables can be assigned during contract creation but will remain constant throughout the lifetime of a deployed contract. A big advantage of immutable variables is that reading them is significantly cheaper than reading from regular state variables since they will not be stored in storage.

- ## MISSING EMIT EVENTS

There should always be events emitted in the sensitive functions that are controlled by centralization roles.

Remediation

It is recommended emitting events for the sensitive functions that are controlled by centralization roles.

- ## IMPROPER USAGE OF PUBLIC AND EXTERNAL TYPE

public functions that are never called by the contract could be declared as external. external functions are more efficient than public functions.

Remediation

Consider using the external attribute for public functions that are never called within the contract.

- **UNCHECKED RETURNS VALUE IN TRANSFER / TRANSFERFROM**

in the functions below there is not any check for the returned value.

rescueBNBFromContract;

setRouterAddress;

rescueBEPTokenFromContract;

Remediation

Use require to check returned value or use safeERC20.