Coinsult

Advanced Manual Smart Contract Audit

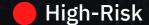**Project:** Reynverse Metaverse
Website: Https://ReynVerse.com

🟢 **Low-Risk**

2 low-risk code
issues found

🟡 **Medium-Risk**

0 medium-risk code
issues found

🔴 **High-Risk**

0 high-risk code
issues found

Contract Address

0x3AAC5fd5A7fEbe7b868155956fA77498a3AD98C0

Disclaimer

Tokenomics

Rank	Address	Quantity (Token)	Percentage
1	0xafc2f29d00d72ec09ea6db707c0b4829a4445627	1,000,000,000	100.0000%

Source Code

Coinsult was comissioned by Reynverse Metaverse to perform an audit based on the following smart contract:

https://bscscan.com/address/0x3AAC5fd5A7fEbe7b868155956fA77498a3AD98C0#code

Manual Code Review

In this audit report we will highlight all these issues:

🟢 **Low-Risk**

2 low-risk code
issues found

🟡 **Medium-Risk**

0 medium-risk code
issues found

🔴 **High-Risk**

0 high-risk code
issues found

The detailed report continues on the next page...

🟢 **Low-Risk:** Could be fixed, will not bring problems.

No zero address validation for some functions

Detect missing zero address validation.

```
payable(feeReceiver_).transfer(msg.value);
```

Recommendation

Check that the new address is not zero.

Exploit scenario

```
contract C {

  modifier onlyAdmin {
    if (msg.sender != owner) throw;
    _;
  }

  function updateOwner(address newOwner) onlyAdmin external {
    owner = newOwner;
  }
}
```

Bob calls updateOwner without specifying the newOwner, soBob loses ownership of the contract.

● **Low-Risk:** Could be fixed, will not bring problems.

Redundant Statements

Detect the usage of redundant statements that have no effect.

```solidity
function _msgData() internal view virtual returns (bytes calldata) {
    this; // silence state mutability warning without generating bytecode - see https://github.com/e
    return msg.data;
}
```

Recommendation

Remove redundant statements if they congest code but offer no value.

Exploit scenario

```solidity
contract RedundantStatementsContract {

    constructor() public {
        uint; // Elementary Type Name
        bool; // Elementary Type Name
        RedundantStatementsContract; // Identifier
    }

    function test() public returns (uint) {
        uint; // Elementary Type Name
        assert; // Identifier
        test; // Identifier
        return 777;
    }
}
```

Each commented line references types/identifiers, but performs no action with them, so no code will be generated for such statements and they can be removed.

Owner privileges

- Owner cannot set fees higher than 25%

- Owner cannot pause trading

- Owner cannot change max transaction amount

Extra notes by the team

No notes

Contract Snapshot

```solidity
contract CoinToken is ERC20 {
    constructor(
        string memory name_,
        string memory symbol_,
        uint256 decimals_,
        uint256 initialBalance_,
        address tokenOwner_,
        address payable feeReceiver_
    ) payable ERC20(name_, symbol_,initialBalance_,decimals_,tokenOwner_) {
        payable(feeReceiver_).transfer(msg.value);
    }
}
```

Website Review

Coinsult checks the website completely manually and looks for visual, technical and textual errors. We also look at the security, speed and accessibility of the website. In short, a complete check to see if the website meets the current standard of the web development industry.

- ● Mobile Friendly

- ● Does not contain jQuery errors

- ● SSL Secured

- ● No major spelling errors

Project Overview

🟡 Not KYC verified by Coinsult