



Coinsult

Advanced Manual Smart Contract Audit



Project: Richer Inu

Website: <https://richerinubsc.com>

Low-Risk

3 low-risk code
issues found

Medium-Risk

0 medium-risk code
issues found

High-Risk

0 high-risk code
issues found

Contract Address

0x601d28012cdC13F32D9d737bc75d9145967da1fb

Disclaimer: Coinsult is not responsible for any financial losses. Nothing in this contract audit is financial advice, please do your own research.

Disclaimer

Coinsult is not responsible if a project turns out to be a scam, rug-pull or honeypot. We only provide a detailed analysis for your own research.

Coinsult is not responsible for any financial losses. Nothing in this contract audit is financial advice, please do your own research.

The information provided in this audit is for informational purposes only and should not be considered investment advice. Coinsult does not endorse, recommend, support or suggest to invest in any project.

Coinsult can not be held responsible for when a project turns out to be a rug-pull, honeypot or scam.

Tokenomics

Rank	Address	Quantity (Token)	Percentage
1	0x2d66bf3f3571731cf477d9a246e1ed04f1f94208	50,000,000	100.0000%

Source Code

Coinsult was comissioned by Richer Inu to perform an audit based on the following smart contract:

<https://bscscan.com/address/0x601d28012cdC13F32D9d737bc75d9145967da1fb#code>

Manual Code Review

In this audit report we will highlight all these issues:

Low-Risk

3 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.

takeTaxes contains unused parameter (bool other)

```
function takeTaxes(address from, address to, uint256 tAmount, bool takeFee, bool buy, bool sell, bool other) {
    ExtraValues memory values;
    Ratios memory ratios = _ratios;
    values.currentRate = _getRate();

    values.rAmount = tAmount * values.currentRate;

    if (_hasLimits(from, to)) { bool checked;
        try antiSnipe.checkUser(from, to, tAmount) returns (bool check) {
            checked = check; } catch { revert(); }
        if(!checked) { revert(); }
    }

    if (takeFee) {
        uint256 currentFee;

        if (buy) {
            currentFee = _taxRates.buyFee;
        } else if (sell) {
            currentFee = _taxRates.sellFee;
        } else {
            currentFee = taxRates.transferFee;
        }
    }
}
```

Recommendation

remove unused parameters

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

Avoid relying on `block.timestamp`

`block.timestamp` can be manipulated by miners.

```
function setLpPair(address pair, bool enabled) external onlyOwner {
    if (!enabled) {
        lpPairs[pair] = false;
        antiSnipe.setLpPair(pair, false);
    } else {
        if (timeSinceLastPair != 0) {
            require(block.timestamp - timeSinceLastPair > 3 days, "3 Day cooldown!");
        }
        lpPairs[pair] = true;
        timeSinceLastPair = block.timestamp;
        antiSnipe.setLpPair(pair, true);
    }
}
```

Recommendation

Do not use `block.timestamp`, now or `blockhash` as a source of randomness

Exploit scenario

```
contract Game {

    uint reward_determining_number;

    function guessing() external{
        reward_determining_number = uint256(block.blockhash(10000)) % 10;
    }
}
```

Eve is a miner. Eve calls `guessing` and re-orders the block containing the transaction. As a result, Eve wins the game.

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

No zero address validation for some functions

Detect missing zero address validation.

```
function setWallets(address payable marketing, address payable treasury) external onlyOwner {
    _taxWallets.marketing = payable(marketing);
    _taxWallets.treasury = payable(treasury);
}
```

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, so Bob loses ownership of the contract.

Owner privileges

- Owner cannot set fees higher than 25%
- Owner cannot pause trading
- Owner cannot change max transaction amount
- Owner can exclude from fees
- ⚠ Owner can exclude address from limits
- ⚠ Owner can change max transaction amount but this has to be higher than 0.5% of total supply
- ⚠ Owner can change max wallet amount but this has to be higher than 1% of total supply
- ⚠ Owner can exclude addresses from reward

Extra notes by the team

No notes

Contract Snapshot

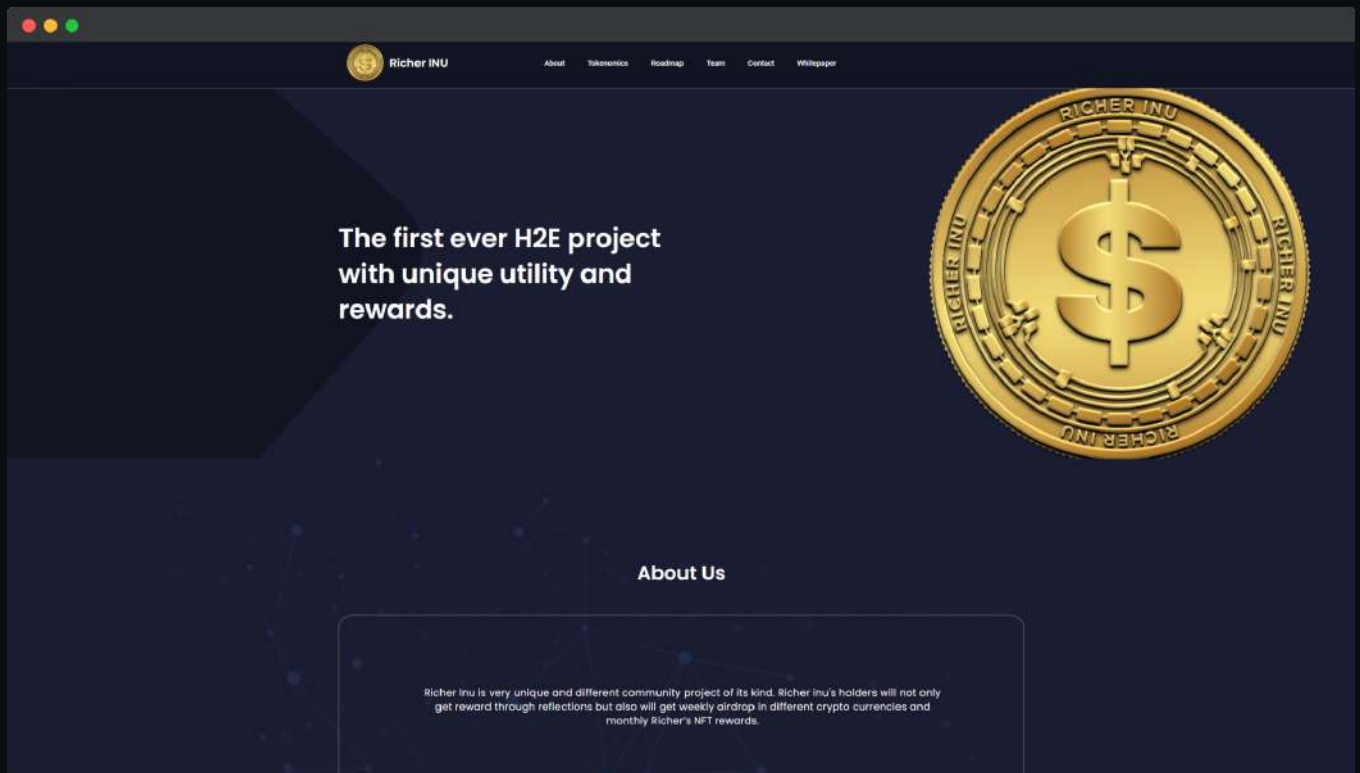
```
contract RicherInu is IERC20 {
    // Ownership moved to in-contract for customizability.
    address private _owner;

    mapping (address => uint256) private _rOwned;
    mapping (address => uint256) private _tOwned;
    mapping (address => bool) lpPairs;
    uint256 private timeSinceLastPair = 0;
    mapping (address => mapping (address => uint256)) private _allowances;

    mapping (address => bool) private _liquidityHolders;
    mapping (address => bool) private _isExcludedFromProtection;
    mapping (address => bool) private _isExcludedFromFees;
    mapping (address => bool) private _isExcludedFromLimits;
    mapping (address => bool) private _isExcluded;
    address[] private _excluded;
```


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
- Not SSL Secured
- No major spelling errors

Project Overview

● KYC verified by Coinsult partner

● Not KYC verified by Coinsult

Richer Inu

Completed KYC Verification at a Coinsult partner



✓ Project Owner Identified

✓ Contract: 0x601d28012cdC13F32D9d737bc75d9145967da1fb

Richer Inu

Audited by Coinsult.net



Date: 4 August 2022

✓ Advanced Manual Smart Contract Audit