Coinsult

Advanced Manual Smart Contract Audit

Project: Lebicat
Website: https://www.lebicat.com

🟢 **Low-risk**
5 low-risk code issues found

🟡 **Medium-risk**
0 medium-risk code issues found

🔴 **High-risk**
0 high-risk code issues found

Contract address

0xc95816EA0C4E2ab4a4A7F4Bc4e899d36aA4aeFE5

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	Null Address: 0x000...dEaD	500,000,000	50.0000%
2	0xec631a5ab463f4401bfeb4501c40a174e229b18a	443,598,700	44.3599%
3	0x0c6a47d78514512a512a5770107291e4eb040b59	56,401,300	5.6401%

Source code

Coinsult was commissioned by Lebicat to perform an audit based on the following smart contract:

https://bscscan.com/address/0xc95816ea0c4e2ab4a4a7f4bc4e899d36aa4aefe5#code

Manual Code Review

🟢 Low-risk

5 low-risk code issues found.
Could be fixed, will not bring problems.

- Contract contains Reentrancy vulnerabilities:
    Additional information: This combination increases risk of malicious intent. While it
    may be justified by some complex mechanics (e.g. rebase, reflections, buyback).
    More information: Slither

```solidity
    function transferFrom(
        address sender,
        address recipient,
        uint256 amount
    ) external override returns (bool) {
        if (_allowances[sender][msg.sender] != _totalSupply) {
            _allowances[sender][msg.sender] =
_allowances[sender][msg.sender]
                .sub(amount, "Insufficient Allowance");
        }

        return _transferFrom(sender, recipient, amount);
    }
```

- Avoid relying on block.timestamp
    block.timestamp can be manipulated by miners.

```solidity
if (
        buybackMultiplierTriggeredAt.add(buybackMultiplierLength) >
        block.timestamp
    ) {
```

- Missing zero address validation
    Check that the new address is not the zero address.

```solidity
    address _autoLiquidityReceiver,
    address _marketingFeeReceiver
```

- The return value of an external transfer/transferFrom call is not checked

   Use SafeERC20, or ensure that the transfer/transferFrom return value is checked.

```solidity
function distributeDividend(address shareholder) internal {
      if (shares[shareholder].amount == 0) {
          return;
      }

      uint256 amount = getUnpaidEarnings(shareholder);
      if (amount > 0) {
          totalDistributed = totalDistributed.add(amount);
          rewardToken.transfer(shareholder, amount);
          shareholderClaims[shareholder] = block.timestamp;
          shares[shareholder].totalRealised = shares[shareholder]
              .totalRealised
              .add(amount);
          shares[shareholder].totalExcluded = getCumulativeDividends(
              shares[shareholder].amount
          );
      }
  }
```

- Literals with many digits are difficult to read and review.

   Recommendation: Use Ether suffix, Time suffix, or The scientific notation

```solidity
require(gas < 750000, "Gas must be lower than 750000");
```

🟡 **Medium-risk**

0 medium-risk code issues found.
Should be fixed, could bring problems.

🔴 **High-risk**

0 high-risk code issues found
Must be fixed, and will bring problems.

Extra notes by the team

🟡 Owner can stop autobuyback.

🟡 Fees can be set up to 100% for both buy and sell fees.

🟡 Owner can exclude addresses from dividends.

🟡 Owner can exclude addresses from fees.

🟡 The ownership of the contract isn't renounced.

🔴 Owner is able to disable swap and liquify

Contract Snapshot

```solidity
contract BuybackBabyToken is IERC20Extended, Auth, BaseToken {
    using SafeMath for uint256;

    uint256 public constant VERSION = 1;

    address private constant DEAD = address(0xdead);
    address private constant ZERO = address(0);
    uint8 private constant _decimals = 9;

    string private _name;
    string private _symbol;
    uint256 private _totalSupply;

    address public rewardToken;
    IUniswapV2Router02 public router;
    address public pair;
    address public autoLiquidityReceiver;
    address public marketingFeeReceiver;

    uint256 public liquidityFee; // default: 200
    uint256 public buybackFee; // default: 300
    uint256 public reflectionFee; // default: 800
    uint256 public marketingFee; // default: 100
    uint256 public totalFee;
    uint256 public feeDenominator; // default: 10000

    uint256 public targetLiquidity; // default: 25
    uint256 public targetLiquidityDenominator; // default: 100

    uint256 public buybackMultiplierNumerator; // default: 200
    uint256 public buybackMultiplierDenominator; // default: 100
    uint256 public buybackMultiplierTriggeredAt;
    uint256 public buybackMultiplierLength; // default: 30 mins
```
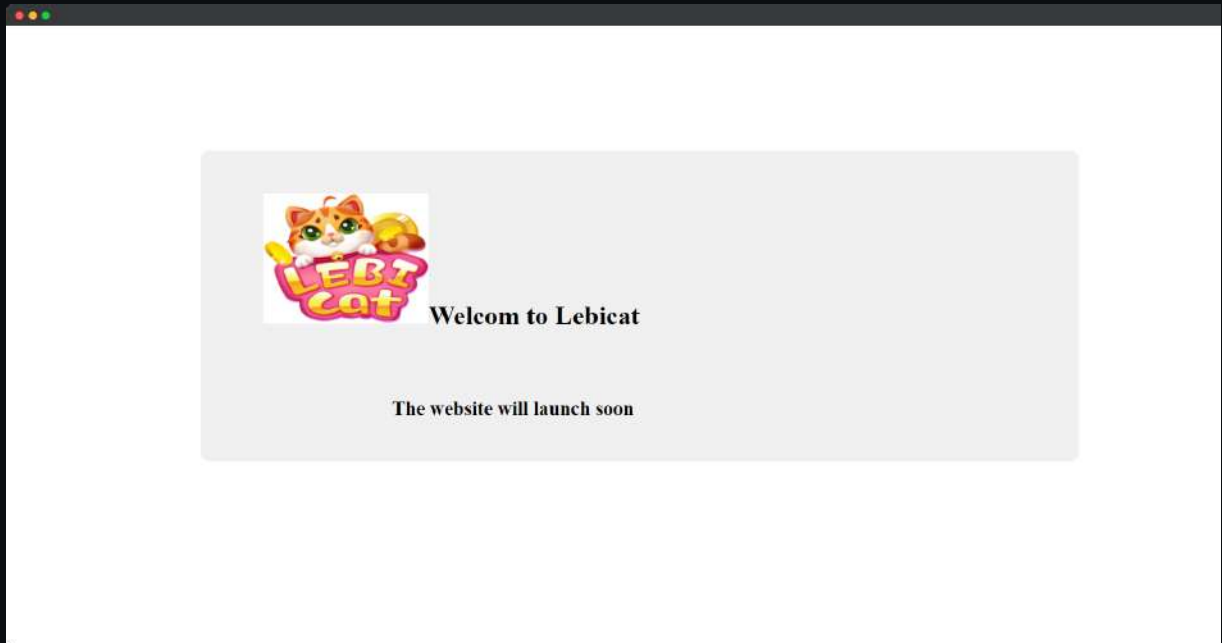
Website Review

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.

Note: The website will launch soon

Rug-pull Review

Based on the available information analyzed by us, we come to the following conclusions:

🟢 Locked Liquidity (no liquidity yet)

🟡 Large unlocked wallets
   - Note: Tokens not distributed yet

🔴 No doxxed Team

Honeypot Review

Based on the available information analyzed by us, we come to the following conclusions:

🟢 Ability to sell

🔴 Owner is not able to pause the contract

🟢 Router cannot be changed

Note: Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by the project owner.