Coinsult

Advanced Manual Smart Contract Audit

Project: STE
Website: http://www.startour.pro/

Low-risk	Medium-risk	High-risk
6 low-risk code issues found	2 medium-risk code issues found	0 high-risk code issues found

Contract address
0x186ae6d98c48f8dee117e57cd473dcb220456ee9

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	0x0d6c3c00451ea77b69f00e3a9ae7a71e827ad66a	438,730.852820926350338112	12.2942%
2	0x1d3d9ffc0e2fc0608edbea3b17fd38858fe2fe11	371,951.891404262534777978	10.4229%
3	0xec9e6645dab7c02a5db3bfe79a4e456c7a976a2a	315,345.430750077808901335	8.8367%
4	Null Address: 0x000...dEaD	280,672.7	7.8651%
5	0xb32b8a21c22bc66a58be4257469712944c3507d0	261,531.969260878804383683	7.3287%

Source code

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

https://bscscan.com/address/0x186ae6d98c48f8dee117e57cd473dcb220456ee9#code

Manual Code Review

🟢 Low-risk

6 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

```
function redeem(uint256 i) public{
  miner storage me=aminer[_msgSender()];
  uint256 starttime=me.sStore[i].stime;
  require(starttime>0,'something wrong!');
  uint256 amount;
  uint256 amonth=30*86400;
  if(starttime+(amonth*2)<block.timestamp){
      amount=me.sStore[i].tokenNum;
  }else{
      if(starttime+amonth < block.timestamp){
          amount=me.sStore[i].tokenNum*95/100;
          }else{
          amount=me.sStore[i].tokenNum*90/100;
          }
  }
  if(me.sStore[i].tokenIndex==0){//bnb
      payable(_msgSender()).transfer(amount);//*****/
  }else{
      IERC20(supportToken[me.sStore[i].tokenIndex]).transfer(_msgSender(),amount);
  }
  me.myU-=me.sStore[i].tokenNum;
  doClaim();
  if(me.node && me.myU<usdtCost){
      me.realnode=false;
  }

  miner storage boss=aminer[me.boss];

  uint256 laststakeCount=me.sStore.length;

  if(laststakeCount==1) {
      me.mine=false;
      miners--;
      V[me.me]=0;
      if(boss.team1workerCount<=9 && boss.team1workerCount>1){
          boss.allU-=getTeamU(boss.me,boss.team1workerCount);
```

```
            }
            boss.team1workerCount--;
        }
        uint8 ii=0;
        while(boss.me!=address(0) && ii<9){
            if( boss.node){
                if( boss.team1workerCount<10) boss.realnode=false;
            }
            if(ii<boss.team1workerCount) {
                boss.allU-=me.sStore[i].usdt;
                }
            if(boss.allU<v1Cost){
                V[boss.me]=0;
            }else{
                V[boss.me]=1;
            }
            calcV(boss.me);
            boss=aminer[boss.boss];
            ii++;
        }
        usdtAmount-=me.sStore[i].usdt;

        stakeStore[] memory oldstore=me.sStore;
        delete me.sStore;
        for (uint256 index = 0; index < oldstore.length; index++) {
            if(index<i) {
                me.sStore.push(oldstore[index]);
            }
            if(index>i) {
                 me.sStore.push(oldstore[index]);
            }
        }

    }
```

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

```
function df23c9c7(uint256 value) public onlyOwner{
        price=value;
        priceList.push(price);
        pricetimestampList.push(block.timestamp);
    }
```

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

```
      function f7d090d6(address recipient, uint256 amount)
       public onlyOwner
       returns (bool)
    {
       payable(recipient).transfer(amount);
       return true;
    }
```

- The return value of an external transfer/transferFrom call is not checked
  Use SafeERC20, or ensure that the transfer/transferFrom return value is checked.

```
function dde81bde(address conaddr,address addr, uint256 amount)
       public onlyOwner
       returns (bool)
    {
       IERC20(conaddr).transfer(addr, amount);
       return true;
    }
```

- Literals with many digits are difficult to read and review.
  Recommendation: Use Ether suffix, Time suffix, or The scientific notation

```
uint256 etime=s.stime+90*86400;
```

- Costly operations inside a loop might waste gas, so optimizations are justified.
  Recommended : Use a local variable to hold the loop computation result.

```
 function _mint(address account, uint256 amount) internal virtual {
       require(account != address(0), "ERC20: mint to the zero
address");

       _totalSupply += amount;
       _balances[account] += amount;
       emit Transfer(address(0), account, amount);
    }
```

🟡 Medium-risk

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

- Owner can mint tokens

```
function b823f49b(address to, uint256 amount) public onlyOwner{
        _mint(to, amount);
    }
```

- Owner able to send tokens from contract address to address.

```
function dde81bde(address conaddr,address addr, uint256 amount)
        public onlyOwner
        returns (bool)
    {
        IERC20(conaddr).transfer(addr, amount);
        return true;
    }
```

🔴 High-risk

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

Extra notes by the team

🟡 Owner can change the router address.

🟡 The ownership of the contract isn’t renounced.

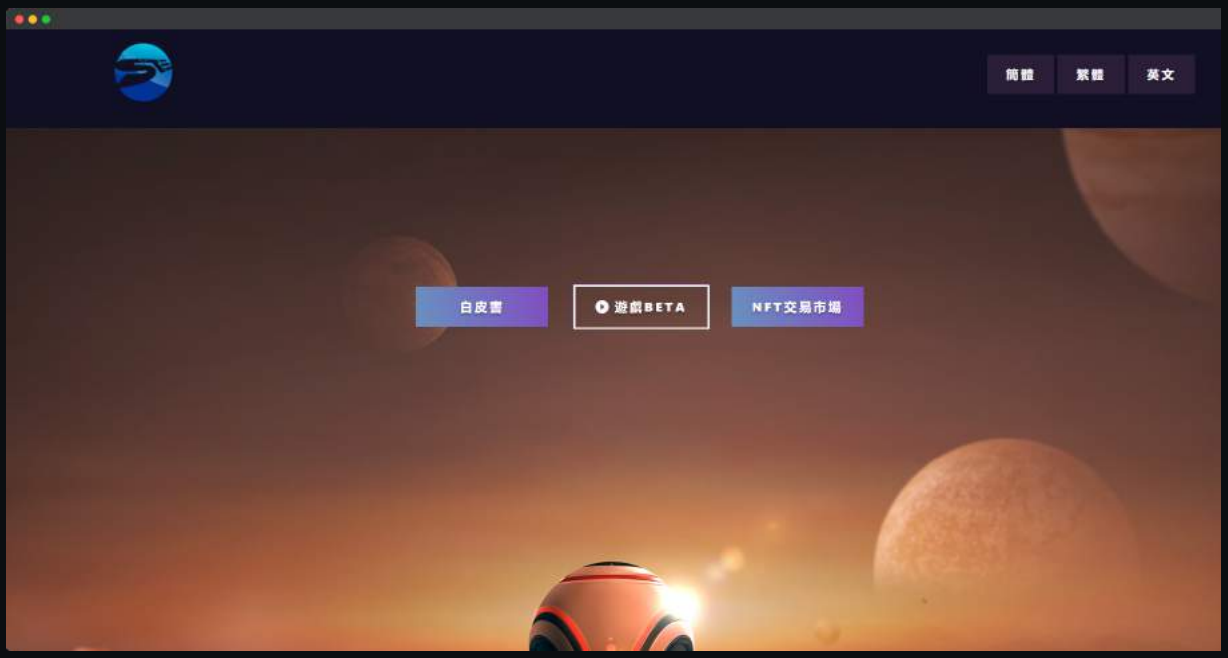
🔴 Owner can mint tokens

Contract Snapshot

```
contract StarTour is ERC20 {
    uint8[9] private power = [50, 10, 10, 5, 5, 5, 5, 5, 5];
    uint256 private maxnum = 500 * 10**26;
    uint256 private miners = 0;
    uint256 private usdtAmount = 0;

    address private backAddr;
    address private dexAddr;
    address private tokenAddr;
    address private nftAddr;
    address private wethAddr =
0xbb4CdB9CBd36B01bD1cBaEBF2De08d9173bc095c; //mainnet eth
    address private usdtAddr =
0x55d398326f99059fF775485246999027B3197955; //mainnet usdt
    address[20] private supportToken;
    address[] private nodeList;
    uint256[] public priceList;
    uint256[] public pricetimestampList;
    struct stakeStore {
        uint8 tokenIndex;
        uint256 stime;
        uint256 ctime;
        uint256 usdt;
        uint256 tokenNum;
    }
    struct stakeBurn {
        uint256 stime;
        uint256 ctime;
        uint256 stakeNum;
        uint256 claimed;
    }
```

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
- 🟢 Contains no jQuery errors
- 🔴 Not SSL Secured
- 🟢 No major spelling errors

Note: Website loading speed is very low.

Loading speed: 20%

Rug-pull Review

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

🟢 Locked Liquidity

🔴 Large unlocked wallets

- Note: Wallet contains 12.2% of the total supply

🔴 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 can 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.