题目一

pragma solidity ^0.4.18;

contract Token1 {

mapping(address => uint) balances;

uint public totalSupply;

function Token(uint \_initialSupply) public {

balances[msg.sender] = totalSupply = \_initialSupply;

}

function transfer(address \_to, uint \_value) public returns (bool) {

require(balances[msg.sender] - \_value >= 0);

balances[msg.sender] -= \_value;

balances[\_to] += \_value;

return true;

}

function balanceOf(address \_owner) public view returns (uint balance) {

return balances[\_owner];

}

}

题目说明：

本题为攻击一个简单的token合约。初始合约时你有20个token，找出代码中包含的漏洞，提交合约调用方式，增加你的token数量。