题目四

pragma solidity ^0.4.23;

contract Token4 {

struct Investment { #基金

uint256 amount; #余额

uint256 deposit\_term; #收益期

address owner; #所有者

}

Investment[] balances;

uint256 head;

address private owner;

bytes16 private secret;

function BelluminarBank(bytes16 \_secret, uint256 deposit\_term) public {

secret = \_secret;

owner = msg.sender;

if(msg.value > 0) {

balances.push(Investment(msg.value, deposit\_term, msg.sender));

}

}

function bankBalance() public view returns (uint256) {

return address(this).balance;

}

function invest(uint256 account, uint256 deposit\_term) public payable {

if (account >= head && account < balances.length) {

Investment storage investment = balances[account];

investment.amount += msg.value;

} else {

if(balances.length > 0) {

require(deposit\_term >= balances[balances.length - 1].deposit\_term + 1 years);

}

investment.amount = msg.value;

investment.deposit\_term = deposit\_term;

investment.owner = msg.sender;

balances.push(investment);

}

}

function withdraw(uint256 account) public {

require(now >= balances[account].deposit\_term);

require(msg.sender == balances[account].owner);

msg.sender.transfer(balances[account].amount);

}

function confiscate(uint256 account, bytes16 \_secret) public {

require(msg.sender == owner);

require(secret == \_secret);

require(now >= balances[account].deposit\_term + 1 years);

uint256 total = 0;

for (uint256 i = head; i <= account; i++) {

total += balances[i].amount;

delete balances[i];

}

head = account + 1;

msg.sender.transfer(total);

}

}

题目说明：

请找出代码中的漏洞，提交攻击合约代码，获取合约中所有资金。