Introduction to DeFi

10 / 4

CONTENT

0x00 Common Smart Contract Security Issue

0x01 Smart Contract Code Analysis Tools

0X02 Previous Attack Incident Reproduction

0X03 Assignment 2 Release Announcement

Common Attack Vector

Smart Contract Security

- This course focuses on solidity security, It’s important to remember that it’s not overly complex.
- Every DeFi protocol engineer strives to protect their project, and the responsibility for securing smart contracts doesn’t fall solely on the auditors.
- What we will cover today: (1) access control, (2) arbitrary call, (3) default visibility, (4) reentrancy issue, (5) bad randomness, (6) ecrecover issue, (7) signature replay.

Access Control

Case 1: Do not have `onlyOwner` modifier, allowing attack to set important parameter.

Protocol: GFOX

Problematic Function: `setMerkleRoot` function

- No `onlyOwner` modifier

Impact:

- Anyone can reset the Merkle root to include themself in the whitelist

<u>Transaction details</u>, we will discuss more about this case & merkle tree later in the course.

Access Control

Real-World Case Study: I accidentally kill it.

Problem: The owner does not init the wallet

(1) The initWallet is not invoke when creation

(2) There is arbitrary delegatecall issue in the contract.

(3) The user call the kill function that contains `kill`

(4) Not an attack incident, an user is just learning smart contract - A $280M lesson learned

Analysis Contract

Access Control

Case 2: Do not have `initializer` modifier, allowing attack to re-initialize the contract

Protocol: 88mph

Problematic Function: `init` function

- No `initializer` modifier for initialization
- No `onlyOwner` verification

Impact:

- Anyone can be the owner
- Able to reset system token

Access Control

Case 3: Do not verify the caller in flash loan receive function

Problematic Function: `executeOperation` function (Aave flash loan receiver function)

Uniswap: uniswapV2Call
Balancer: receiveFlashLoan
Aave: executeOperation

- Not verify `initiator` address - anyone can initiate flash loan to trigger the function
- Not verify the `msg.sender` - anyone can call the `executeOperation` directly.

Access Control

MEV Bot Case Study: Lack of Contract Verification Won't Protect You from Attacks

20221108	**MEV_0ad8**	**Unlimited external call**	**$282k**
20221014	MEVBOTa47b	Insufficient validation	$241 k
20220928	MEVBOT - Badc0de	Arbitrary call via callFunction	$94,304
20220913	MevBot private tx	Incorrect access control	$140 K
20231112	MEVBot_0xa247	Access Control	$150K
20231107	MEVbot	Access Control	$2M
20231112	MEVBot_0x8c2d	Access Control	$365K

Link

Access Control

Case 4: unprotected callback in ERC-721 and ERC-1155

Problematic Function: `onERC721Received` function

- The callback might contains some critical logics and not protected.
- Anyone can directly invoke the callback

Instance: ERC-721, ERC-1155

Default Function Visibility

Case 1: If you do not specify the function visibility, The default visibility is `public`, not `internal`.

Real World Case: CoinstoreNFT

- No protected `burn` function
- Not verify the token owner

Real World Case: The Sandbox

(1) No protected `_burn` function

Arbitrary Call

Case 1: Arbitrary call with `call` - calldata injection.

Some case study

MixedSwapRouter::algebraSwapCallback

MinterProxyV2::swap

SpectraRouter::_dispatch

It a common attack vector. But it does not mean this pattern should never be used.

For example: DAO, Multisig Wallet

Arbitrary Call

Case 1: Arbitrary call with `delegatecall` - Logic contract contains malicious operation

`selfdestruct` in implementation contract.

- For example, the UUPS vulnerability

Reentrancy Issue

What is reentrancy issue? Check your system programming slides.

Reentrant Functions

- **When interrupts occur, a function could be called twice and causes problems.**
- **Potential Problem**
  - In the signal handler, we can't tell where the process was executing when the signal was caught!
- **A function is described as reentrant if it can be safely called recursively**

Tei-Wei Kuo, Chi-Sheng Shih, Hao-Hua Chu, and Pu-Jen Cheng©2007
Department of Computer Science and Information Engineering
Graduate institute of Multimedia and Networking, National Taiwan University

Reference: SP from PJ

An example in C: malloc

Tei-Wei Kuo, Chi-Sheng Shih, Hao-Hua Chu, and Pu-Jen Cheng©2007
Department of Computer Science and Information Engineering
Graduate institute of Multimedia and Networking, National Taiwan University

Reentrancy Issue

Different Types of Reentrancy

- Single function reentrancy
- Cross function reentrancy
- Cross contract reentrancy
- Cross chain reentrancy
- Read only reentrancy

The problem lies in the function that changes the state - not pure, view function

Note: the problem is in the `view` function

Reentrancy Issue

Case 1: Single function reentrancy

Example

Reentrancy Issue

Case 1: Cross function reentrancy

DFX Finance Hack—Nov 10, 2022—Detailed Analysis

Overview On the 10th of November, 2022, DFX Finance, operating on an Ethereum-based protocol with the attack manifesting on the Polygon network, fell victim to a security breach involving a flash loan attack th...

ImmuneBytes / Dec 1, 2023

Reentrancy Issue

Case 1: reentrancy issue in IERC721Receiver / IERC1155Receiver

```
function _safeMint(
    address to,
    uint256 tokenId,
    bytes memory _data
) internal virtual {
    _mint(to, tokenId);
    require(
        _checkOnERC721Received(address(0), to, tokenId, _data),
        "ERC721: transfer to non ERC721Receiver implementer"
    );
}
```

When “SafeMint” Becomes Unsafe: Lessons from the HypeBears Security Incident

On the morning of Feb 3rd (+8 timezone), our system reported an attack transaction...

Medium / Feb 5, 2022

When `safeMint` become unsafe

Is ERC-20 safe? There are some variant: ERC 223, 677, 777, and 1363

Reentrancy Issue

Case 1: Read Only Reentrancy

The problem is in the `view` function

Reentrancy Issue

Exercise: Read Only Reentrancy

RareSkills/**solidity-riddles**

A collection of Solidity security exercises and puzzles to test your knowledge of Solidity's more esoteric features. Some are easy,...

10 Contributors | 1 Issue | 291 Stars | 90 Forks

solidity-riddles/contracts/ReadOnly.sol at main · RareSkills/solidity-riddles

A collection of Solidity security exercises and puzzles to test your knowledge of Solidity's more esoteric features. Some are easy, and some are exceptionally challenging. - RareSkills/soli...

GitHub

Simple Example

Reentrancy Issue

Case 1: Curve LP Oracle Manipulation

What is an oracle, what is Curve, and what is an LP (liquidity provider)?

Curve LP Oracle Manipulation: Post Mortem

What if you could manipulate Curve's oracles to exploit major DeFi protocols? Read about the...

chainsecurity.com

A Real-World Example

Reentrancy Issue

Protection 1: Use mutex lock

OpenZeppelin/
openzeppelin-contracts

OpenZeppelin Contracts is a library for secure smart contract development.

445 Contributors | 277 Used by | 25k Stars | 12k Forks

openzeppelin-contracts/contracts/utils/ReentrancyGuard.sol at maste...

OpenZeppelin Contracts is a library for secure smart contract development. - OpenZeppelin/openzeppelin-contracts

GitHub

Non upgradeable version

OpenZeppelin/
openzeppelin-contracts...

Upgradeable variant of OpenZeppelin Contracts, meant for use in upgradeable contracts.

216 Contributors | 2k Used by | 988 Stars | 426 Forks

openzeppelin-contracts-upgradeable/contracts/utils/ReentrancyGuardUpgradea...

Upgradeable variant of OpenZeppelin Contracts, meant for use in upgradeable contracts. - OpenZeppelin/openzeppelin-contracts-upgradeable

GitHub

Upgradeable version

Reentrancy Issue

Protection 2: Check-Effect-Interaction

- Check: validate all the input
- Effect: update the state variable
- Interaction: make external call

How to change our contract?

Bad Randomness

How do you get random number on the blockchain?

Bad Randomness in Solidity Smart Contracts

Introduction Bad randomness, often referred to as the "nothing is
attack, is a vulnerability in Solidity smart contracts deployed on th
Ethereum blockchain.

ImmuneBytes / Nov 1, 2023

SunWeb3Sec/
DeFiVulnLabs

To learn common smart contract vulnerabilities using Foundry!

12 Contributors | 2 Issues | 2k Stars | 275 Forks

DeFiVulnLabs/src/test/Randomness.sol at main · SunWeb3Sec/DeFiVulnLabs

To learn common smart contract vulnerabilities using Foundry! - SunWeb3Sec/DeFiVulnLabs

GitHub

Bad Randomness

Soluiton: Chainlink VRF

Generate Random Numbers for Smart Contracts using Chainlink VRF

Learn how to securely generate random numbers for your smart contract with Chainlink VRF (an RNG). This guide uses Solidity code examples.

Chainlink Documentation

Bad Randomness

Soluiton: Chainlink VRF

Signature Replay

What is a signature?

ECDSA: Elliptic Curve Cryptography

Message | Private Key | Public Key | Signature

user0 can sign the **message** using the **private key** and get the **signature**.

user1 can recover the **public key** given the **message** and the **signature**

A **public key** can be generated given a **private key**

Signature Replay

EVM Utils Demo

ERC 191 Signing

Sign typed data using ERC-191 | Personal message signing

Evm Tools

Signature Replay

What can be a digest / message? Any 32 bytes data

- How to sign? Use metamask / Foundry cheatcode
- How to recover? Use ecrecover precompile address. - **NOTE**: return zero address(0) when the recover process fail.

```
(address alice, uint256 alicePk) = makeAddrAndKey("alice");
emit log_address(alice);
bytes32 hash = keccak256("Signed by Alice");
(uint8 v, bytes32 r, bytes32 s) = vm.sign(alicePk, hash);
address signer = ecrecover(hash, v, r, s);
assertEq(alice, signer); // [PASS]
```

Signature Replay

What can this do?

Signature Replay

Multisig Wallet

Signature Replay

Multisig Wallet

What might be the potential problem in this implementation?

Signature Replay

Real World Usage - Safe Wallet

Safe{Wallet}— Secure Smart Account Management on Ethereum

Explore Safe, the leading Ethereum multisig wallet for secure and efficient Smart Account management. Experience advanced security and user-friendly features.

Signature Replay

Some signature can be reused for multiple times.

- Scenario 1: A proposal will deposit 5 ether to lending protocol, and if some signers want to deposit again, can they re-submit the same signature?

- Scenario 2: A proposal is created on another EVM-compatible chain, it has been executed. The same wallet is created on the Ethereum mainnet, can the signature be re-used again?

Signature Replay

Some signature can be reused for multiple times.

- Adding a *nonce* value to your message, and verify whether this signature is used before.
- Adding a *chain.id* value to your message, verify whether this signature is used on another chain before.

Signature Replay

EIP-191

ERC-191: Signed Data Standard

This ERC proposes a specification about how to handle signed data in Ethereum contracts.

Ethereum Improvement Proposals

0x19 <1 byte version> <version specific data> <data to sign>.

Signature Replay

EIP-712

ERC-191: Signed Data Standard

This ERC proposes a specification about how to handle signed data in Ethereum contracts.

Ethereum Improvement Proposals

0x19 <1 byte version> <version specific data> <data to sign>.

Signature Replay

ECDSA Oppenzeppelin Library

OpenZeppelin/
openzeppelin-contracts

OpenZeppelin Contracts is a library for secure smart contract development.

445 Contributors | 277 Used by | 25k Stars | 12k Forks

openzeppelin-contracts/contracts/utils/cryptography/ECDSA.sol at...

OpenZeppelin Contracts is a library for secure smart contract development. - OpenZeppelin/openzeppelin-contracts

GitHub

Smart Contract Analysis Tool

DEMO REPO

LouisTsai-Csie/**COSCUP-2024-Demo**

1 Contributor | 0 Issues | 0 Stars | 0 Forks

LouisTsai-Csie/COSCUP-2024-Demo

Contribute to LouisTsai-Csie/COSCUP-2024-Demo development by creating an account on GitHub.

GitHub

Tools Category

We categorize the smart contract code analysis tools into three categories.

STATIC ANALYZER

Scan smart contract code without executing it, identifying potential vulnerabilities and inefficiencies

FUZZING TOOLS

Generate and send random inputs to test the robustness and security of smart contracts.

FORMAL VERIFICATION

Mathematically prove the correctness of the logic against its specifications, ensuring it behaves as intended under all conditions.

Demo: Static Analyzer

Scan smart contract code without executing it, identifying potential vulnerabilities and inefficiencies

Slither / Slitherin

Aderyn

Mythril

NOTE: After the Dencun upgrade, `selfdestruct` can only eliminate bytecode deployed during the contract creation transaction.

Demo: Fuzzing Tools

Generate and send random inputs to test the robustness and security of smart contracts.

Medusa

Foundry

Echidna

Demo: Formal Verification

Mathematically prove the correctness of the logic against its specifications, ensuring it behaves as intended under all conditions.

ityFuzz

Certora

CERTORA

Halmos

Awesome list

LouisTsai-Csie/**awesome-smart-contract-analysis...**

A curated list of awesome smart contract analysis tools

1 Contributor | 0 Issues | 1 Discussion | 101 Stars | 13 Forks

LouisTsai-Csie/awesome-smart-contract-analysis-tools: A curated list of awesome smart contract analysis tools

A curated list of awesome smart contract analysis tools - LouisTsai-Csie/awesome-smart-contract-analysis-tools

GitHub

Awesome-Smart-Contract-Analysis-Tools

- Including 40+ Tools (focus on Solidity)
- Category: Static Analyzer, Fuzzing, formal verification tools, ...
- Keep adding new tools now!
- Submit your PR & Issues

Storage Collision

The inconsistency of the storage layout between proxy and implementation contract leads to storage collision vulnerability

Slither

Consistent Storage Layout: Ensure the storage layout of the proxy contract matches that of the implementation contract.

Slither-check-upgradeability

7	`order-vars-contracts`	Incorrect vars order with the v2	High
8	`order-vars-proxy`	Incorrect vars order with the proxy	High

Demo Time

Audius Attack &
Slither-check-upgradeability

Attack Incident Reproduction

DEMO REPO

LouisTsai-Csie/**TEM-2024-Demo**

1 Contributor | 0 Issues | 1 Star | 0 Forks

LouisTsai-Csie/TEM-2024-Demo

Contribute to LouisTsai-Csie/TEM-2024-Demo development by creating an account on GitHub.

GitHub

Tracking Current and Past Attack Incidents

Incident Database

Includes all past attack incidents and analyses

Postmortem Analysis

Recent Attack Incident Analysis and Postmortem

Real Time Alert

Reporting Ongoing Attack Incidents and Brief Analyses

Attack Incident Database

DeFiHackLabs

Rekt News

SlowMist

Phalcon

Postmortem Analysis

Rekt News : The dark web of DeFi journalism.

BlockThreat Intelligence : a weekly newsletter that provides the latest security updates, tools, events, vulnerabilities, and threats in the crypto landscape.

SlowMist Weekly Security Digest : Weekly attack incident overview in X (Twitter)

ChainLight Hack Digest : Weekly attack incident overview in X (Twitter).

BlockSec Monthly Security Review : Monthly attack incident overview.

Real Time Alert

Twitter is your good friend

0 PeckShield Alert

1 Phalcon Alert

2 Cyvers Alert

3 Certik Alert

4 Nic Franlin

5 Beosin Alert

6 MetaTrust Alert

7 SlowMist Alert

#security-alert channel in DeFiHackLabs discord

Transaction Analysis

ROLE

Attacker, Attack Contract, Victim Contract, ...

If the transaction is complicated:

1. There might be some duplicate pattern
2. Collapse the staticcall section first

Attack Preparation

Request Flash Loan, Create Helper Contracts, ...

Exploit Procedure

Interact with the victim / external contract, ...

Post Attack Handling

Repay flash loan, transfer to wallet, ...

Transaction Analysis Tools

Tenderly

AnyTx

Openchain

Transaction Tracer

View and trace EVM transactions

samczsun

Phalcon

BlockSec App Suite | Full-Stack Blockchain Security Service

Security suite for Protocols, Developers, LPs, & Traders - safeguarding your blockchain journey

blocksec.com

Demo!

Demo 0: FILX

Access Control

FLIX

Root Cause

The contract lacks a protected initialization function, allowing an attacker to reinitialize it, take over owner role, and subsequently withdraw all funds from the treasury.

Loss	~200K	PoC	Link
Chain	Ethereum	Transaction	Link

Attack Preparation

None

Exploit Procedure

Call the `init` function and take over the owner role

Post Attack Handling

swap FLIX token for USDT

FLIX

```
51      /**
52       * @dev constructor
53       * @param initToken The t
54       */
55      function init(
56          IERC20 initToken,
57          uint256 initPeriods,
58          uint256 initInterval
59      ) public {
60          token = initToken;
61          periods = initPeriods;
62          interval = initInterval;
63          owner = _msgSender();
64      }
```

```
function withdraw(
    IERC20 otherToken,
    uint256 amount,
    address receiver
) public virtual onlyOwner {
    uint256 currentBalance = otherToken.balanceOf(address(this));
    require(receiver != address(0), "receiver must not empty");
    require(currentBalance >= amount, "current balance insufficient");
    otherToken.safeTransfer(receiver, amount);
}
```

The owner has been reset, allowing the `onlyOwner` modifier to be bypassed

FLIX

Attack Procedure

```
[Sender] DN404 Exploiter
0  0 → CALL value: 0.000000000000079292 [Receiver] MEV BOT.CodeIsLawZ95677371 Calldata() ▸ ()
1    1 → CALL TransparentUpgradeableProxy.init Calldata(initToken=Wrapped Ether (WETH), initPeriods=1, initInterval=1,000,000,000,000,000,000) ▸ ()
3    1 → CALL TransparentUpgradeableProxy.withdraw Calldata(otherToken=FILX, amount=685,000,000,000,000,000,000,000, receiver=[Receiver]MEV BOT) ▸ ()
8    1 → CALL Uniswap V3: FILX-USDT 2.swap Calldata(recipient=[Receiver]MEV BOT, zeroForOne=true, amountSpecified=685,000,000,000,000,000,000,000, sqrtPric
17   1 → CALL Tether: USDT Stablecoin.transfer Calldata(_to=Uniswap V2: USDT, _value=169,577,736,489) ▸ ()
19   1 → CALL Uniswap V2: USDT.swap Calldata(amount0Out=67,645,684,730,046,434,621, amount1Out=0, to=[Receiver]MEV BOT, data="") ▸ ()
26   1 → CALL Wrapped Ether (WETH).withdraw Calldata(wad=67,645,684,730,046,434,621) ▸ ()
29   1 → CALL value: 67.645684730046641553 [Sender] DN404 Exploiter.fallback(raw data) ▸ ()
```

Post Attack Handling

Transaction

Demo 0: RICO

Arbitrary Call

RICO

Root Cause

An attacker can provide a target address and calldata to the Rico flash loan function, enabling the generation of calldata that directs Rico to transfer all funds to the attacker.

Loss	~36K	PoC	Link
Chain	Arbitrum	Transaction	Link

Attack Preparation

None

Exploit Procedure

Execute a malicious flash loan that forces Rico to transfer tokens out of the treasury.

Post Attack Handling

Swap token to USDC

Flash Loan Pattern

```
{ // scope for _token{0,1}, avoids stack too deep errors
address _token0 = token0;
address _token1 = token1;
require(to != _token0 && to != _token1, 'UniswapV2: INVALID_TO');
if (amount0Out > 0) _safeTransfer(_token0, to, amount0Out); // optimistically transfer tokens
if (amount1Out > 0) _safeTransfer(_token1, to, amount1Out); // optimistically transfer tokens
if (data.length > 0) IUniswapV2Callee(to).uniswapV2Call(msg.sender, amount0Out, amount1Out, data);
balance0 = IERC20(_token0).balanceOf(address(this));
balance1 = IERC20(_token1).balanceOf(address(this));
}
```

EIP-3156

Arbitrary Call

```
// flash borrow
// locked with itself to avoid flashing more than MINT
function flash(address code, bytes calldata data)
  external payable returns (bytes memory result) {
    // lock->mint->call->burn->unlock
    VatStorage storage vs = getVatStorage();
    if (vs.flock == LOCKED) revert ErrLock();
    vs.flock = LOCKED;

    getBankStorage().rico.mint(code, _MINT);
    bool ok;
    (ok, result) = code.call(data);
    if (!ok) bubble(result);
    getBankStorage().rico.burn(code, _MI

    vs.flock = UNLOCKED;
}
```

Not follow EIP-3156

The attacker provides a target address and call data to the victim contract to execute malicious actions.

Arbitrary Call

Rico

Attack Procedure

```
0  0 → CALL [Receiver] 0x68d843d31de072390d41bff30b0076bef0482d8f.0xa558c55d(raw data) ▸ ()
3    1 → CALL BankDiamond.flash Calldata(code=Circle: USDC Token, data=(long param)) ▸ (result=0x0000000000000000000000000000000000000000000000000000
14   1 → CALL BankDiamond.flash Calldata(code=TransparentUpgradeableProxy_912c_6548, data=(long param)) ▸ (result=0x0000000000000000000000000000000000
26   1 → CALL BankDiamond.flash Calldata(code=ChainLink Token (LINK), data=(long param)) ▸ (result=0x0000000000000000000000000000000000000000000000000000
38   1 → CALL BankDiamond.flash Calldata(code=Wrapped liquid staked Ether 2.0 (wstETH), data=(long param)) ▸ (result=0x0000000000000000000000000000000000
49   1 → CALL BankDiamond.flash Calldata(code=Wrapped Ether, data=(long param)) ▸ (result=0x0000000000000000000000000000000000000000000000000000
60   1 → CALL BankDiamond.flash Calldata(code=Arbitrum: USDC Token, data=(long param)) ▸ (result=0x0000000000000000000000000000000000000000000000000000
73   1 → CALL BankDiamond.flash Calldata(code=Circle: USDC Token, data=(long param)) ▸ (result=0x0000000000000000000000000000000000000000000000000000
86   1 → CALL BankDiamond.flash Calldata(code=Circle: USDC Token, data=(long param)) ▸ (result=0x0000000000000000000000000000000000000000000000000000
99   1 → CALL BankDiamond.flash Calldata(code=Wrapped liquid staked Ether 2.0 (wstETH), data=(long param)) ▸ (result=0x0000000000000000000000000000000000
110  1 → CALL TransparentUpgradeableProxy_912c_6548.approve Calldata(spender=Uniswap V3: Router, amount=2,478,235,540,754,361,715,555) ▸ (true)
113  1 → CALL Uniswap V3: Router.exactInputSingle Calldata(params=[tokenIn=TransparentUpgradeableProxy_912c_6548, tokenOut=Circle: USDC Token, fee=3,000, r
131  1 → CALL ChainLink Token (LINK).approve Calldata(spender=Uniswap V3: Router, amount=69,669,705,859,926,416,088) ▸ (true)
135  1 → CALL Uniswap V3: Router.exactInputSingle Calldata(params=[tokenIn=ChainLink Token (LINK), tokenOut=Circle: USDC Token, fee=3,000, recipient=[Recei
155  1 → CALL Wrapped liquid staked Ether 2.0 (wstETH).approve Calldata(spender_=Uniswap V3: Router, amount_=592,120,646,108,188,259) ▸ (true)
158  1 → CALL Uniswap V3: Router.exactInputSingle Calldata(params=[tokenIn=Wrapped liquid staked Ether 2.0 (wstETH), tokenOut=Arbitrum: USDC Token, fee=500
175  1 → CALL Wrapped Ether.approve Calldata(spender=Uniswap V3: Router, amount=287,173,939,050,505,854) ▸ (true)
178  1 → CALL Uniswap V3: Router.exactInputSingle Calldata(params=[tokenIn=Wrapped Ether, tokenOut=Circle: USDC Token, fee=3,000, recipient=[Receiver]0x68d
195  1 → CALL Arbitrum: USDC Token.approve Calldata(spender=Uniswap V3: Router, amount=2,392,168,258) ▸ (true)
198  1 → CALL Uniswap V3: Router.exactInputSingle Calldata(params=[tokenIn=Arbitrum: USDC Token, tokenOut=Circle: USDC Token, fee=100, recipient=[Receiver]
```

Post Attack Handling

Transaction

Demo: GameToken

Reentrancy

GameToken

Root Cause

The newBidEtherMin() function contains a logic error that lets a bidder submit just over 5% of the previous bid, resulting in the full amount being returned to any last bid address.

_sendEther function use "call" to send ETH exposes the contract to re-entrancy attacks.

Loss	~20 ETH	PoC	Link
Chain	Ethereum	Transaction	Link

Attack Preparation

None

Exploit Procedure

Execute a malicious flash loan that forces Rico to transfer tokens out of the treasury.

Post Attack Handling

Swap token to USDC

Reentrancy Issue

```
function withdrawAll() public {
    uint256 amount = _balances[msg.sender];
    (bool success,) = msg.sender.call{value: amount}("");
    require(success, "Ether Transfer Failed");

    _balances[msg.sender] = 0;

    emit unsafeBank__withdrawToken(msg.sender, amount);
}
```

Check-Effect-Interaction

1. Check: input validation
2. Effect: state variable update
3. Interaction: external contract call

Reserve Order

GameToken Attack

```
function newBidEtherMin() public view returns (uint256) {
    return (bidEther * auctionBidStepShare) / auctionBidStepPrecesion;
}
```

5

100

```
function makeBid() external payable {
    require(msg.value > newBidEtherMin(), "bid is too low");
    if (bidAddress != address(0)) {
        _sendEther(bidAddress, bidEther);
    }
    bidAddress = msg.sender;
    bidEther = msg.value;
    if (auctionEndTime == 0)
        auctionEndTime = block.timestamp + auctionStartTimer;
    else auctionEndTime += auctionBidAddsTimer;
}
```

```
function _sendEther(address to, uint256 count) internal {
    (bool sentFee, ) = payable(to).call{value: count}("");
    require(sentFee, "sent fee error: ether is not sent");
}
```

GameToken Attack

GameToken

Protection Method

1. Add reentrancy guard to the function to prevent recursive call
2. Follow the check-effect-interaction pattern

GameToken Attack

```
[Sender] 0x145766a51ae96e69810fe76f6f68fd0e95675a0b
0 → CALL value: 0.6 [Receiver] 0x8d4de2bc1a566b266bd4b387f62c21e15474d12a.0xe8b00990(raw data) ▸ ()
  1 → CALL value: 0.294 Game.makeBid Calldata () ▸ ()
  1 → STATICCALL Game.newBidEtherMin Calldata () ▸ (14,700,000,000,000,000)
  1 → CALL value: 0.014700000000000001 Game.makeBid Calldata () ▸ ()
    2 → CALL value: 0.294 [Receiver] 0x8d4de2bc1a566b266bd4b387f62c21e15474d12a.fallback(raw data) ▸ ()
      3 → STATICCALL Game.newBidEtherMin Calldata () ▸ (14,700,000,000,000,000)
      3 → CALL value: 0.014700000000000001 Game.makeBid Calldata () ▸ ()
        4 → CALL value: 0.294 [Receiver] 0x8d4de2bc1a566b266bd4b387f62c21e15474d12a.fallback(raw data) ▸ ()
          5 → STATICCALL Game.newBidEtherMin Calldata () ▸ (14,700,000,000,000,000)
          5 → CALL value: 0.014700000000000001 Game.makeBid Calldata () ▸ ()
            6 → CALL value: 0.294 [Receiver] 0x8d4de2bc1a566b266bd4b387f62c21e15474d12a.fallback(raw data) ▸ ()
              7 → STATICCALL Game.newBidEtherMin Calldata () ▸ (14,700,000,000,000,000)
              7 → CALL value: 0.014700000000000001 Game.makeBid Calldata () ▸ ()
                8 → CALL value: 0.294 [Receiver] 0x8d4de2bc1a566b266bd4b387f62c21e15474d12a.fallback(raw data) ▸ ()
                  9 → STATICCALL Game.newBidEtherMin Calldata () ▸ (14,700,000,000,000,000)
                  9 → CALL value: 0.014700000000000001 Game.makeBid Calldata () ▸ ()
                    10 → CALL value: 0.294 [Receiver] 0x8d4de2bc1a566b266bd4b387f62c21e15474d12a.fallback(raw data) ▸ ()
                      11 → STATICCALL Game.newBidEtherMin Calldata () ▸ (14,700,000,000,000,000)
                      11 → CALL value: 0.014700000000000001 Game.makeBid Calldata () ▸ ()
                        12 → CALL value: 0.294 [Receiver] 0x8d4de2bc1a566b266bd4b387f62c21e15474d12a.fallback(raw data) ▸ ()
```

Transaction

Demo: GalaxyFoxToken

Access Control

GalaxyFoxToken

Root Cause

The setMerkleRoot function currently has no access controls, allowing anyone to reset the merkle root and subsequently claim rewards from the treasury.

The contract is unverified and requires decompilation

Loss	~50K	PoC	Link
Chain	Ethereum	Transaction	Link

Attack Preparation

No preparation for the attack

Exploit Procedure

Configure the merkle root

Post Attack Handling

Swap token to stable coin

Merkle Tree

Merkle Root
hash (0, 7)
hash
hash (0, 3)
+
hash (4, 7)
hash
hash
hash (0, 1)
+
hash (2, 3)
hash (4, 5)
+
hash (6, 7)
hash
hash
hash
hash
Leaf 0
+
Leaf 1
Leaf 2
+
Leaf 3
Leaf 4
+
Leaf 5
Leaf 6
+
Leaf 7
hash
hash
hash
hash
Data 0
Data 1
Data 2
Data 3
Data 4
Data 5
Data 6
Data 7

Merkle Tree

Merkle Root
hash (0, 7)
hash
hash (0, 3)
+
hash (4, 7)
hash
hash
hash (0, 1)
+
hash (2, 3)
hash (4, 5)
+
hash (6, 7)
hash
hash
hash
hash
Leaf 0
+
Leaf 1
Leaf 2
+
Leaf 3
Leaf 4
+
Leaf 5
Leaf 6
+
Leaf 7
hash
hash
hash
hash
Data 0
Data 1
Data 2
Data 3
Data 4
Data 5
Data 6
Data 7

Decompilation Tools

The contract is unverified so you can not read the source code directly

Online Solidity Decompiler

Dedaub Decompiler

EVM Decompiler

GalaxyFoxToken

Access Control No protected modifier

call data length check

```
function setMerkleRoot(bytes32 _merkleRoot) public payable {
    require(msg.data.length - 4 >= 32);
    _merkleRoot = _merkleRoot;
}
```

```
function claim(address to, uint256 amount, bytes32[] proof) public payable {
    require(msg.data.length - 4 >= 96);
    require(proof <= uint64.max);
    require(4 + proof + 31 < msg.data.length);
    require(proof.length <= uint64.max);
    require(4 + proof + (proof.length << 5) + 32 <= msg.data.length);
    require(_claimStart > 0, Error('GfoxClaim: Not started'));
    require(block.timestamp >= _claimStart, Error('GfoxClaim: Not started'));
    require(amount > _claimedAmount[to], Error('GfoxClaim: Already claimed'));
```

Merkle Leaf Generation

GalaxyFoxToken

Attack Preparation

Attack Procedure

Post Attack Handling

```
[Sender] Attacker
0  0 → CALL value: 8.943354253693861759 [Receiver] Attacker Contract.0x2967b08a(raw data) ▸ ()
1      1 → STATICCALL Wrapped Ether (WETH).balanceOf Calldata([Sender]Attacker) ▸ (7,495,900,638,137,556)
2      1 → CREATE2 Attacker Helper Contract ▸ (raw data)
3      1 → CALL Attacker Helper Contract.t Calldata() ▸ ()
4          2 → STATICCALL Galaxy Fox: GFOX Token.balanceOf Calldata(account=Victim) ▸ (1,780,453,099,185,000,000,000,000,000)
5          2 → CALL Victim.setMerkleRoot Calldata(_merkleRoot=0xe8236ea3d247bd0c85596d7bb707f40ca374a6fa58d66ece1d80cdc2ac7ecbaf) ▸ ()
6          2 → CALL Victim.claim Calldata(to=Attacker Helper Contract, amount=1,780,453,099,185,000,000,000,000,000, proof=[]) ▸ ()
11         2 → STATICCALL Galaxy Fox: GFOX Token.balanceOf Calldata(account=Attacker Helper Contract) ▸ (1,335,339,824,388,750,000,000,000,000)
12         2 → CALL Galaxy Fox: GFOX Token.approve Calldata(spender=Uniswap V2: Router 2, value=(long param)) ▸ (true)
14         2 → CALL Uniswap V2: Router 2.swapExactTokensForTokensSupportingFeeOnTransferTokens Calldata(amountIn=1,335,339,824,388,750,000,000,000,000, amount
31         2 → STATICCALL Wrapped Ether (WETH).balanceOf Calldata(Attacker Helper Contract) ▸ (108,744,009,594,558,929,771)
32         2 → CALL Wrapped Ether (WETH).transfer Calldata(dst=[Sender]Attacker, wad=108,744,009,594,558,929,771) ▸ (true)
33             3 → EVENT Wrapped Ether (WETH).Transfer Calldata(src=Attacker Helper Contract, dst=[Sender]Attacker, wad=108,744,009,594,558,929,771)
34         2 → STATICCALL Wrapped Ether (WETH).balanceOf Calldata([Sender]Attacker) ▸ (108,751,505,495,197,067,327)
35     1 → STATICCALL Wrapped Ether (WETH).balanceOf Calldata([Sender]Attacker) ▸ (108,751,505,495,197,067,327)
36     1 → CALL value: 8.943354253693861759 0x0899529af5a64125d000bc36f503de012463f094.fallback(raw data) ▸ ()
```

More on Merkle Tree

More on Merkle Tree

Merkle Tree Visualization

EVM Tools

Tools for web3, evm and zk

Tools for web3, evm and zero knowledge proofs

Evm Tools

Merkle Tree Interaction

Merkle Trees Visualization

Web site created using create-react-app

netlify.app

More on Merkle Tree

Please Please Please read this, or you cannot solve the challenge in your homework

The second preimage attack for Merkle Trees in Solidity

The second preimage attack in Merkle trees can happen when an intermediate node in a merkle tree is presented as a leaf.

RareSkills / Sep 17

More on Merkle Tree

Intermediate Node Vulnerability / Second Preimage Attack

- Make sure you cannot pass leaf value as input.
- If the function can pass leaf value, its length should not be 64 bytes
- Double hash to generate the leaf node given input parameter.

The End