Decentralized Finance HW3 Write-Up

Allen Chen B10209040

November 6, 2023

Metamask Wallet Address

0x31D256A107A253bc17dC9c2dE874d4984d1f00c1

0 Greeter

Address: 0x700426e6810Eb2AfeB3EA16f650e1007D61B1D5e

Is locked: False

Approach: Use Metamask wallet transfer 0.0001 ethers on sepolia testnet first. Put contract address in At Address field on remix, and then Call the Unlock function to complete the task.

1 Gate

Address: 0x7bAF9BaDDa18F19F175F22bC40e3DeF9461492D7

Is locked: False

Approach: First we need to find where the secret is. Booleans use 1 byte, an address uses 20 bytes, and we know each slot can hold 32 bytes. As a result, we can simply calculate that the secret is stored in slot 3. Then we can utilize the web3 devolopment platform Alchemy to find what this secret actually is. Using eth getStorageAt method, putting in the contract address and slot 3, we can obtain a data "0x0000000000000000000000000000000000000000007465737490aa7465737490aa" . Once we get this secret data, we can try to interact with the gate contract by using interface and abi.encoding. In this way we can fulfill the requirement of the unlock function in the gate contract.

2 Delegation

Address: 0xc808E98002eE25c415328AB17EB4AF1c34f76569

Is locked: True

Approach: Use similar methods as challenge 1 to get the secret and interact with the contract. We can successfully execute change owner via interface, and then the owner will be changed because of delegatecall. However I had a hard time finding why it was't unlocked.

3 Reentrance

Address: 0xC2d52Da94aA5fDFA93c73264e0b49E925650d3B0

Is locked: True

Approach:

Addresses in array form

[0x31D256A107A253bc17dC9c2dE874d4984d1f00c1,0x700426e6810Eb2AfeB3EA16f650e1007D61B1D5e,
0x7bAF9BaDDa18F19F175F22bC40e3DeF9461492D7,0xc808E98002eE25c415328AB17EB4AF1c34f76569,
0xC2d52Da94aA5fDFA93c73264e0b49E925650d3B0]