

Sensitive On-Chain Data Exercise 3

Intro

Cryptic Raffle is a new on-chain lottery game.

The raffle contract is deployed on Goerli testnet, and its address is:

`0xca0B461f6F8Af197069a68f5f8A263b497569140`

Anyone can participate and earn ETH.

The game is initially deployed with 0.1 ETH.

Rules

- The manager of the game (contract owner), creates new raffles every once in a while
- A raffle consists of 3 numbers between 0-255
- In order to win the raffle, the player needs to guess all 3 numbers in the right order.
- Participation cost 0.01 ETH (which accumulates in the smart contract)
- The winner takes all the pot of the current raffle

There are some addicted gamblers who are trying different strategies to win the raffle.

Lucky you, you can beat them all thanks to your smart contract hacking skills.

You're (your Attacker account) broke and you only own 0.1 ETH.

Your goal is to win the current raffle round and claim all the pot.

Note: This exercise is executed on an Goerli testnet local fork block number `8660077`. Everything is already configured in the `hardhat.config.js` file.

Note: In this exercise you don't have access to the source code of the `CrypticRaffle.sol` smart contract.

Setup

Update your `.env` file and add the GOERLI Infura RPC url:

```
GOERLI = 'https://goerli.infura.io/v3/9aa3d95b3bc440fa88ea12eaa4456161'
```

Accounts

- 0 - AddictedGambler1
- 1 - AddictedGambler2
- 2 - Attacker (You)

Tasks

Task 1

Win the raffle and claim all the ETH that is currently in the contract's pot.

Bonus

Find another way to find the winning numbers 😊

Useful Links

- [Goerli EtherScan](#)
- [Cast Commands](#)

Goerli Public RPC Nodes

```
https://goerli.infura.io/v3/9aa3d95b3bc440fa88ea12eaa4456161  
https://ethereum-goerli-rpc.allthatnode.com
```