DoraHacks Challenges

POLYSWARM

Presenter: Ben Schmidt, CSO @ PolySwarm

2018 @ Swarm Technologies, Inc.

polyswarm.io

info@polyswarm.io

Introduction

- Two problems: one exploitation, one reversing
- Both problems are on the Ropsten testnet
- The goal: get on the winners[] list!

Challenge 1: GuessMe

- Guess the number, win a prize!
- Recommended tools:
  - https://etherscan.io
  - https://remix.ethereum.org
  - https://solidity.readthedocs.io
- Challenge: https://bit.ly/2CFCVhT

GuessMe Tips

- If you're stuck, read up on reference types:
    - https://solidity.readthedocs.io/en/v0.4.21/types.html#reference-types

- Step through the transaction in Remix

- An address is just a random number, more or less

GuessMe Solution

- The Guess structure points to storage slot 0
- Writing to this overwrites the random number
- Solution:
    - Generate an address with last 16bits < 10
    - Send transaction guessing this number

Challenge 2: RESolidify

- Figure out the secret, and pass the check!
- Recommended tools:
  - https://binary.ninja
  - https://github.com/trailofbits/ethersplay
  - https://github.com/ConsenSys/mythril
- Challenge: https://bit.ly/2yAc0o7

RESolidify Tips

- a ^ b ^ msg.sender

- Might be a 0x42 in there somewhere…

- Look at the creation transaction if you’re having trouble finding a secret

- Goal phrase: “that was very cash money of you”

RESolidify Solution

- secret_xor = dogecointothemoonlambosoondudes!
- key = secret_xor ^ guess ^ msg.sender ^ 0x4242...
- Use this xor key to encode your payload so it matches “that was very cash money of you”

Thanks!

Got questions? Let us know!

@PolySwarm / info@polyswarm.io

POLYSWARM