SECUREUM

A-MAZE X

Smart Contract Security CTF

DeFi Security Summit

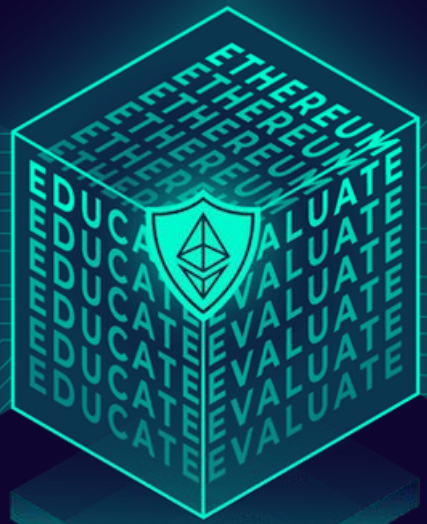
Fondation de la Maison de la Chimie

JULY 14, 2023 | PARIS

SECUREUM

A-MAZE X

SECUREUM



SECUREUM

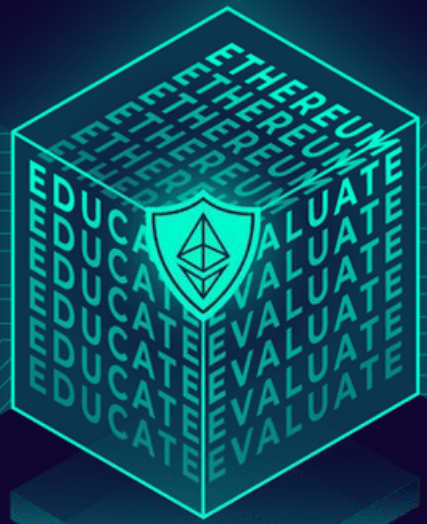
A-MAZE X

$ 1,000,000,000’s Value

1,000’s Protocols

100’s Experts

Ethereum



SECUREUM

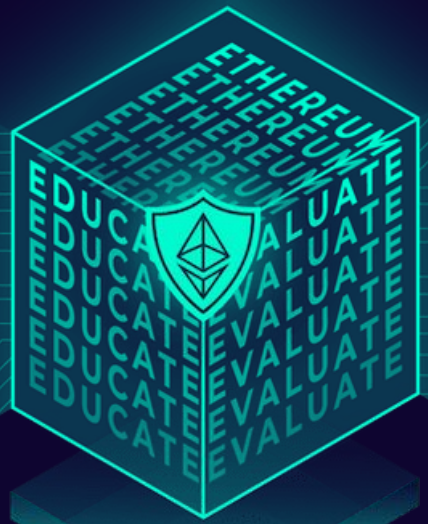
A-MAZE X

$ 1,000,000,000’s Value

1,000’s Protocols

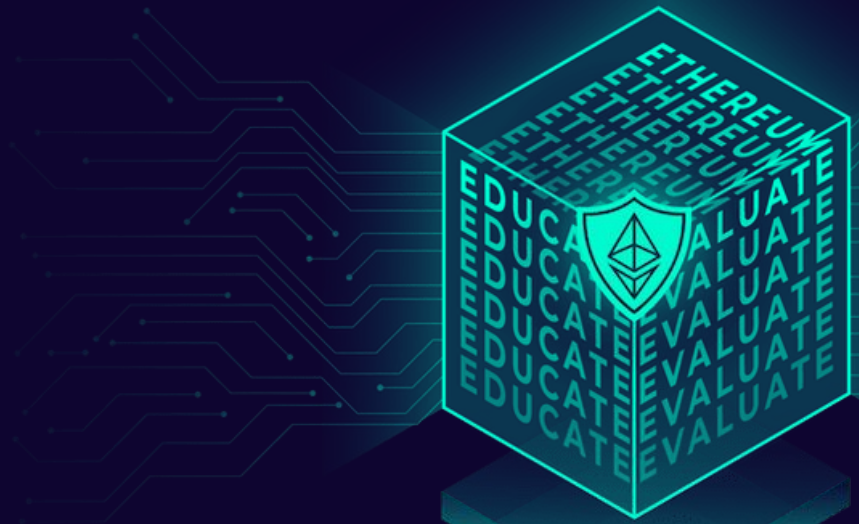
100’s Experts

Ethereum



SECUREUM
A-MAZE X

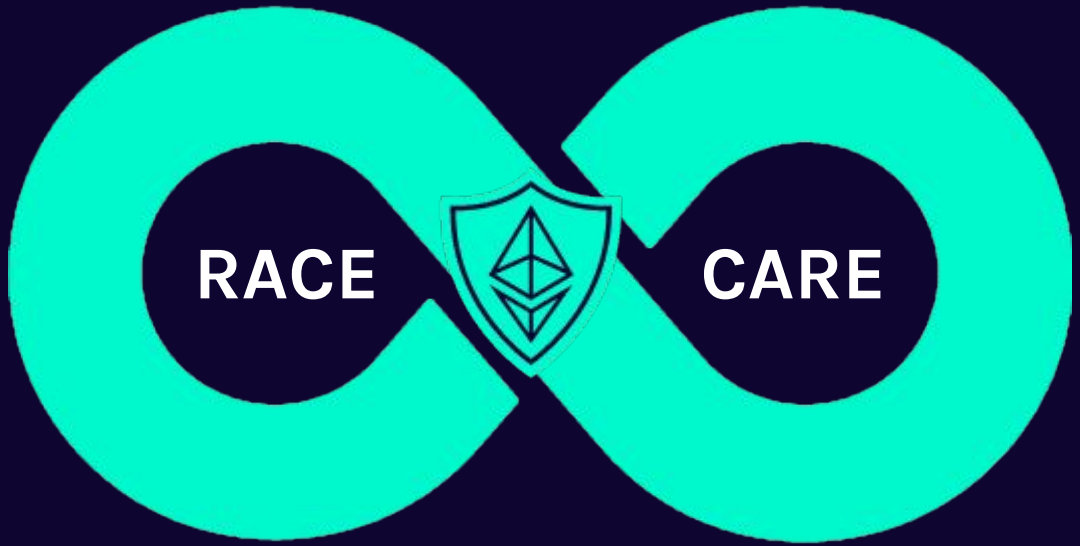
Scaling Security



SECUREUM

A-MAZE X

JOIN OUR SERVER ON DISCORD



Collaborators

SPEARBIT

SHERLOCK

CERTORA

TRAIL OF BITS

Veridise.

SECUREUM

A-MAZE-X

14 JULY, 2023

SECUREUM

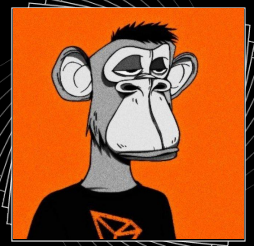
A-MAZE-X CTF

DEFI SECURITY 101
PARIS, FRANCE

SECUREUM
A-MAZE X

The Secureum Initiative

- 0x4non
  - Full time Blockchain Hacker
  - twitter: @eugenioclrc

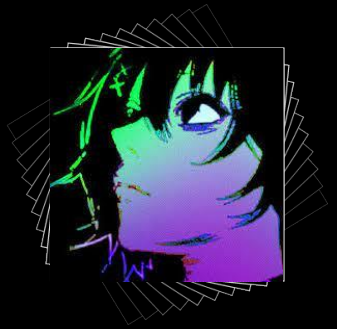


- luksgrin
  - PhD student in Applied Mathematics
  - Junior Security Researcher at Spearbit
  - twitter: @Cryptonicle1

SECUREUM
A-MAZE X

The Secureum Initiative

- Pablo Misirov
  - InfoSec and UX researcher, Spearbit
  - twitter: @p_misirov



- Pēteris Priedītis
  - EVM Security Researcher
  - twitter:@PPrieditis

SECUREUM
A-MAZE X

The Secureum Initiative

- RamiRond
  - Masters student in computer science
  - twitter: @RomiRand

- nftmerchant
  - CPA & Security Researcher
  - twitter: @nftmerchant

SECUREUM
A-MAZE X

CTF Instructions

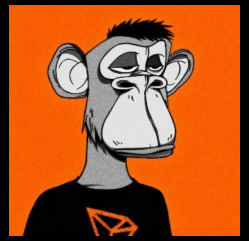
- **8 Challenges Related to Common Vulnerabilities**
  - 3 easy; 2 medium; 3 advanced
- **3 days** for **Hacking**
- 30 minutes for **explanation & solution**

SECUREUM
A-MAZE X

Important DeFi Concepts

- The ERC20 token standard
- Flash Loans
- CREATE, CREATE2 opcodes
- Automatic Market Makers (AMMs)
- Reentrancy Attacks
- Lending in DeFi
- Oracle manipulation and Collateral liquidation

SECUREUM
A-MAZE X



Challenge 1: Operation magic redemption 🪄🔮

- ERC20 token that is burneable, based on a real case

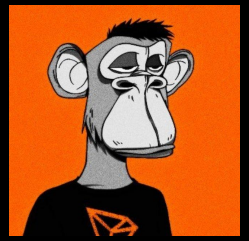
Goal

- Recover 1000 mETH from exploiter and redeem mETH to ETH to avoid further losses

Contracts

- MagicETH.sol

SECUREUM
A-MAZE X

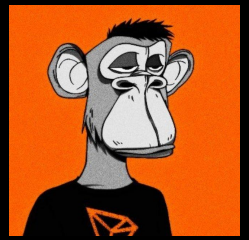


Challenge 1: Operation magic redemption 🪄🔮

Concepts

- Consider this as challenge as a warm up
- ERC20 pretty similar to WETH
- Review the ERC20 logic and how is implemented

SECUREUM
A-MAZE X



Challenge 2: Mission Modern WETH; Rescue the Ether 🧗🧭

- At first sight is similar to challenge #1

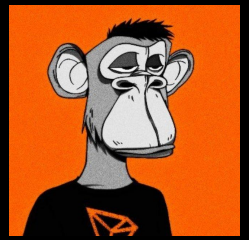
Goal

- The contract has locked 1000 ETH, you have to perform a white hat rescue.

Contracts

- ModernETH.sol

SECUREUM
A-MAZE X



Challenge 2: Mission WETH10; Rescue the Ether 🧗🧭

Concepts

- Simple token, similar to WETH but with an extra function that let you redeem all your tokens.
- (Check for extra hints in readme, beware there were be spoilers)

SECUREUM
A-MAZE X

Challenge 3: The LendEx Destruction 🤺🃏

- Contract code is not immutable

Goal

- Change contract code for a deployed contract and steal tokens

Contracts

- LendingHack.sol, LendExGovernor.sol
- Create2Deployer.sol, CreateDeployer.sol

SECUREUM
A-MAZE X

Challenge 4: Operation Rescue POSI Token! 💼🔓

- Tokens stuck at an unclaimed address
- Factory contract that deploys “smart wallets”

Goal

- Access the unclaimed address and recover the tokens

Contracts

- mySafeFactory.sol

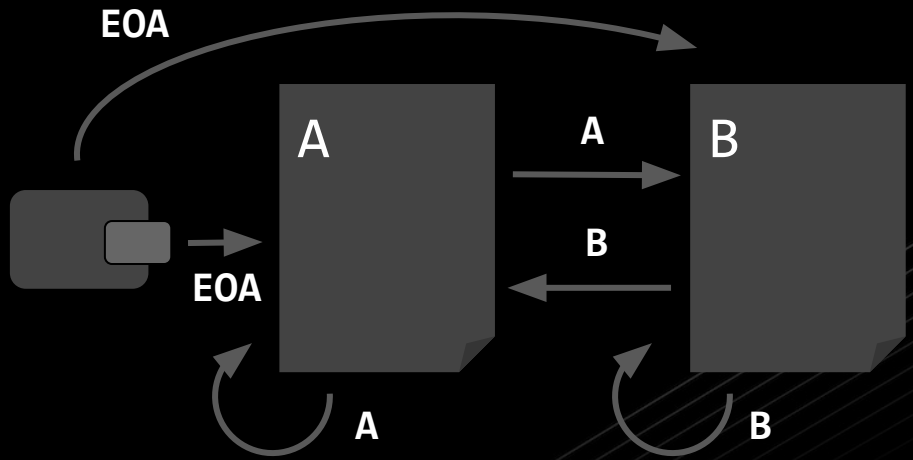
SECUREUM
A-MAZE X

Challenge 4: Operation Rescue POSI Token! 💼🔓

Concepts

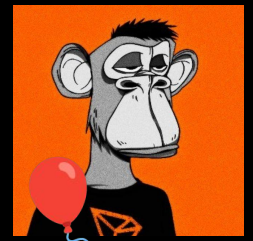
- CREATE2 deterministic addresses
- msg.sender under different contexts

```
hash(0xff, msg.sender, salt, bytecode)
```



SECUREUM
A-MAZE X

Challenge 5: Balloon Vault



- Alice and Bob funds are in danger, rescue their funds before an evil actor steal from them.

Goal

- You have to drain Alice and Bob wallets

Contracts

- Vault.sol
- WETH.sol (WETH9 similar implementation)

SECUREUM
A-MAZE X

Challenge 6: Safe Yield? 🏦📈

- DeFi protocol
- Users can get flash loans and swap on the dex
- Depositors earn fees

Goal

- Drain at least 100 ETH from the pool

Contracts

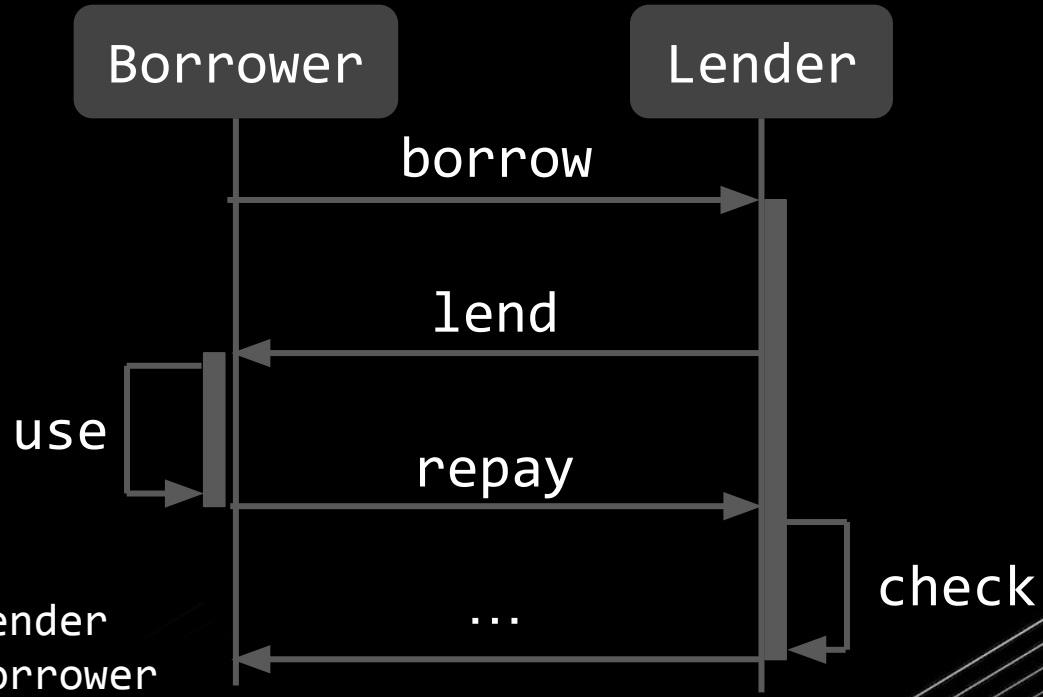
- YieldPool.sol

SECUREUM A-MAZE X

Challenge 6: Safe Yield?

Concepts

- Flash Loans



- ERC-3156
  - IERC3156FlashLender
  - IERC3156FlashBorrower

SECUREUM
A-MAZE X

Challenge 7: Crystal DAO 💎💎

- A factory deploys ERC1167 clones of a DAO treasury
- Admin can execute arbitrary logic with a signature
- Admin is set on deploy

Goal

- Recover the tokens stuck at the treasury

Contracts

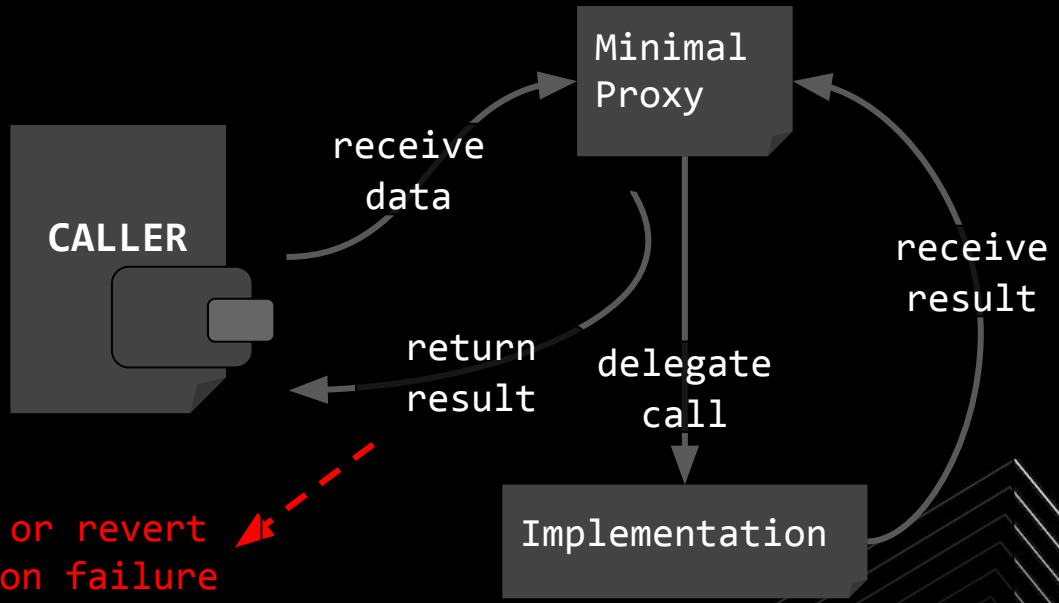
- crystalDAO.sol

SECUREUM
A-MAZE X

Challenge 7: Crystal DAO 💎💎

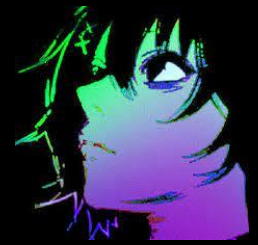
Concepts

- ERC1176 Minimal Proxy
- EIP712 Signatures
- ecrecover()



SECUREUM A-MAZE X

Challenge 8: Liquidatooor🔱🔱



- Lending/Borrowing protocol (Deposit collateral,borrow debt)
- Health Factor and Liquidations
- Over / Under collateralized positions

Goal

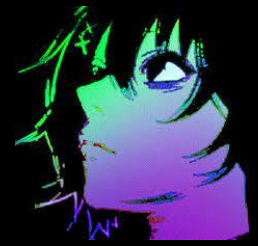
- Liquidate the user and end with at least 200 TOKENs!

Contracts

- AMM.sol
- Oiler.sol

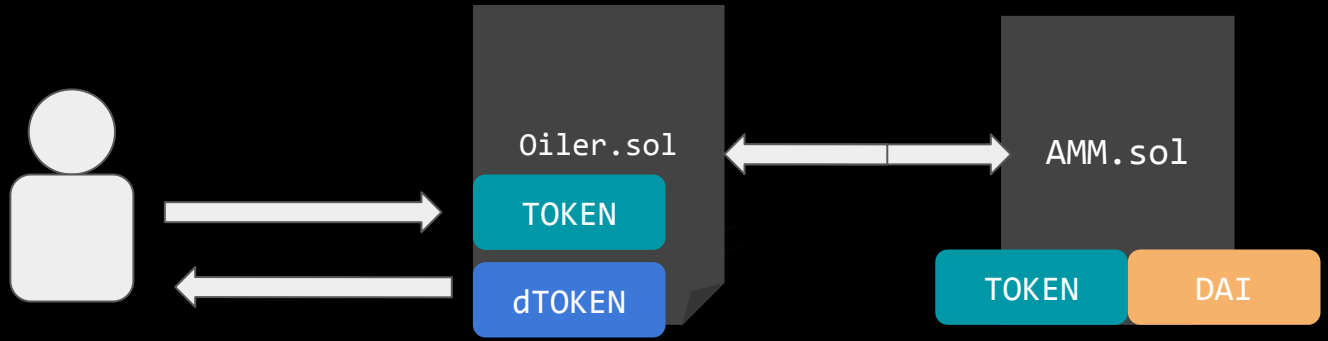
SECUREUM
A-MAZE X

Challenge 8: Liquidatooor🔱🔱



Concepts

- Oracles
- General `k = x * y` understanding
- Lending/Borrowing risk parameters



SECUREUM A-MAZE X

Acknowledgements

Our heartfelt thanks to our mentors for their invaluable reviews of these challenges

Patrickd
@patrickd_de

Tincho Abbate
@tinchoabbate

StErMi
@StErMi

SECUREUM

A-MAZE X

Time to hack!!

JOIN OUR SERVER ON DISCORD

Access the repository

GitHub

TELEGRAM CHANNEL