bit.ly/howiaudit

EthPrague 2023

Dominik Teiml

Contents

my story

Dominik Teiml studied Maths & Computer Science at the University of Oxford. He got into blockchain with Gnosis, where he focused on decentralized exchanges and formal verification. Later he transitioned to security assessments, first at Certik and later at Trail of Bits. He was part of the founding of Ackee Blockchain, where he focused on employee training and auditing. Dom is the author of the Yellow Paper Course and the creator of Woke, a development and testing framework for Solidity.

Currently, he is teaching at RareSkills.io, working on Woke, running a podcast Crypto Cafe, and doing freelance security work and fuzzing.

Why are there so many hacks?

- Permissionlessness
- Open-source
- Anonymious
- Irreversibility
- Value

How to start an auditing company

- Tools
  - Reasons:
    - Become more efficient
    - Gain reputation → clients
    - Help the community
    - Code delivarables
  - Security engineering:
    - Art of finding bugs
    - Static analysis
    - Fuzzing

        - Symbolic execution
- Communication
    - Slack
        - `#x-tool-roswell`
        - `#audit-uniswap`
        - `#x-client-uniswap`
- Reports
    - Asciidoc!

Tips for preparing for an audit contracts

- Write good documentation!
  - Variable naming: `balances` → `address_2_balance`
  - Storage variables begin with `$`

How to do an audit

80% of an audit is onboarding

- Do preparatory learning
  - option theory
- Read docs - whitepaper, podcast
- Explain the project to the client

Actual audit

- Woke Dash
- Understand the code
  - top-down or bottom-up?
- (Optional) fuzz tests

Demo

Next steps