coggle
made for free at coggle.it

Ethereum Smart Contract Auditor Roadmap

- Smart Contract Auditor
  - Step 1 — Blockchain Fundamentals
    - Mastering Ethereum
    - Proof of Work vs Proof of Stake
    - The Eth2 Book
  - Step 2 — Solidity Fundamentals
    - Solidity Documentation
    - Smart Contract Programmer - Solidity 0.8
    - Secureum Solidity 101
    - Secureum Solidity 201
  - Step 3 — Gas Optimizations
    - Aggregated Tricks by pcaversaccio and Harikrishnan Mulackal
    - Kaden: Gas Optimization Tips
    - Juan: Advanced Gas Optimizations
  - Step 4 — Smart Contract Testing/Debugging
    - Hardhat Docs
    - Better Programming Hub
    - Code Eater - Hindi
    - Foundry
    - Tenderly
  - Step 5 — ERC Standards
    - Token Standards - ERC 20, 721, 777, 1155, 4626
    - Other Standards: ERC2981
  - Step 6
    - Openzeppelin Helper Libraries/Contracts
  - Step 7 — Upgradeable Contracts
    - Smart Contract Programmer - Upgradeable Contracts
    - Smart Contract Programmer - Risks of Upgradeable Contracts
    - Different Proxy Patterns - EIPs 897, 1822, 1967, 1538, 2535
  - Step 8 — Smart Contract Attack Vectors
    - Secureum Security Pitfalls 101
    - Secureum Security Pitfalls 201
    - SWC Registry
    - Smart Contract Programmer - Hack Solidity
    - Kaden: Smart Contract Attack Vectors
  - Step 9 — Yul
    - Inline Assembly
    - OPCODES
    - PRECOMPILES
    - Dynamic Gas Costs & Memory Expansion
  - Step 10 — CTFs
    - CTFs & WriteUps - A curated list (for reference)
    - Ethernaut
    - Capture The Ether
    - CipherShastra
    - Damn Vulnerable DeFi (After Completing Step 10)
  - Step 11 — DeFi Deep Dive
    - Finematics - DeFi
    - DeFi MOOC
    - Smart Contract Programmer - DeFi
    - Protocol Deep Dives: Uniswap v2/v3/v4, Compound, Curve, Aave, Balancer, Gearbox
    - Stablecoins => Algorithmic Stablecoins
    - Staking Rewards, Vaults
  - Step 12 — DeFi Attack Vectors
    - Flash Loan => Price Oracle Manipulation
    - Front-Running => Sandwich attacks
    - Rug Pulls => Unlimited Token Allowance
  - Step 13 — Postmortems & BugFixes
    - Immunefi
    - BlockSec
    - SlowMist
    - Rekt News
    - PeckShield
  - Step 14 — Report Reading
    - Secureum Audit Findings 101
    - Secureum Audit Findings 201
    - Consensys, Trail of Bits, Openzeppelin, Code4rena, Sherlock
    - Database: Solodit
  - Step 15 — Security Standards & Checklists
    - SCSVS
    - Rari-Capital Solcurity
  - Step 16 — Important Ethereum Improvement Proposals (EIPs)
    - Core: 150, 1559, 2929, 2930, 3198, 3529, 3675, 4399, 1153, 4758
    - Interface: 712
    - ERC: 165, 1167, 1271, 2535, 2612, 2771, 2981, 4337, 4626
    - Meta: All
  - Step 17 — Arsenal
    - Remix
    - VS Code IDE
    - Slither
    - Mythril
    - Manticore
    - Echidna
    - Surya
    - Scribble
    - BlockSec ETH/BSC Tx Analysis
    - ethtx ETH Tx Analysis
  - Step 18 — Continuous Learning and Research
    - Ethereum Yellow Paper
    - Ethereum Execution Specs
    - Ethereum Consensus Specs
    - Ethereum Magicians
    - Eth Research
    - Newsletters: Blockthreat
    - Join Security Communities on Discord: Immunefi, Secureum, Blockchain Pentesting, Eth Security, Eth R&D
    - Deep Dive Research Papers: Arxiv
    - Be Active on Twitter & follow up with latest research, and attack vectors

© Razzor