# ROADMAP TO SC AUDITOR

## Table of Contents

1. Smart Contract Audit- Youtube: @PatricAlphaC & @CyfrinUpdraft
2. Mastering Ethereum Book: @gavofyork and @anntonop (github)
3. Ethereum Yellow paper course from @AckeeBlockchain - Youtube
4. More videos/articles about EVM
   - EVM Storage - A Low-Level Guide To Solidity's Storage Management: Link: https://t.co/HLTAP39uRK
   - Full in-depth explanation of the Ethereum Virtual Machine: Link: https://t.co/mu0fJPeLec
   - **A free advanced course on the technicalities of the EVM**: Link: https://t.co/cijzrWPnot
   - The EVM Handbook: Link https://t.co/J8fbTJchfl
   - EVM puzzles: Link: https://t.co/2OEKQX7RAi
   - EVM Opcodes: Link: https://t.co/VGSDeyEFGP
   - Reversing The EVM: Raw Calldata: Link: https://t.co/ysRFZ5EJYi
   - EVM: From Solidity to byte code, memory and storage Link: https://t.co/SNiHHqS2xp
5. Go through the @TheSecureum Bootcamp for Smart Contract auditing. Blog Article, Videos and Quiz: https://t.co/3FTAi0rAfx
6. Start reading audit reports -
   - @SoloditOfficial : https://t.co/7REBeNznXA
   - @code4rena: https://t.co/zUXFhgbVPs
   - @sherlockdefi : https://t.co/uYOTjIxrjY
   - @ShieldifySec : https://t.co/uYBET0psMr
7. You need to learn the most Common Attack Vectors

- List of Some Attack Vectors/Smart Contract Vulnerabilities! – https://twitter.com/ShieldifyAnon/status/1730617426096640284?s=20
- Learn EVM Attacks - https://t.co/b8NHeqOdcG
- SCV-List - https://t.co/upyLGKRnLg
- Smart contract attack vectors: https://t.co/4IitsfF5wV
- A Historical Collection of Reentrancy Attacks - https://t.co/ZsSBSy7ESq
- List of 100+ DEFI Attacks + Hacks Analysis: https://t.co/dmziUJ8u5S
- List Of 18 Defi Vulnerabilities + Code Examples : https://t.co/SF2eJiBaEd

- Smart Contract Security Verification Standard - https://t.co/3nHnkaoWa3
- Ethereum Smart Contract Security Best Practices: https://t.co/RRoMzwpPKc
- The Solcurity Standard: https://t.co/vOWRmlXu5X
- Web3 Security Library - https://t.co/Nn1EttPqYX
- List of Bridge Hacks - https://t.co/ETSN1ZCmKT
- DeFi Attack Vectors - https://t.co/RNuoYR9FdL
- Smart Contract Vulnerabilities - https://t.co/jU1GHBJGpL
- Solidity security blog - https://t.co/4YxGXggqKD
- Top 10 DeFi Security Best Practices - https://t.co/DmEKxvTbQO
- DeFi Slippage Attacks - https://t.co/EJwqGZXWgX
- Lending/Borrowing DeFi Attacks - https://t.co/cjFr91Lgeu
- DAO Governance DeFi Attacks - https://t.co/GDadbarki0
- Precision Loss Errors - https://t.co/pkt3Y1La5C
- NFT attacks - https://t.co/7PbdZAKe2r
- MEV - https://t.co/a7kAOzHvnO-
- 6 Critical Vulnerabilities - https://t.co/R6FpEqArDC
- 22 Vulnerabilities - https://t.co/zVZm3Th2Qm
- You Have To Know These 13 Critical Liquidation Vulnerabilities - https://t.co/umw63tZFt2
- List of Top 28 DeFi Attack Vectors - https://t.co/2NdVJOAt6W

## EXTRAS

### List of Some Attack Vectors/Smart Contract Vulnerabilities

- Reentrancy
- Reentrancy via Modifier
- Read-Only Reentrancy
- Cross-Function Reentrancy
- Cross-Contract Reentrancy
- Front-Running
- Front-Running - Unprotected withdraw
- Front-Running - Sandwich attack
- Front-Running - ERC20 approval
- Front-Running - Signatures
- Back-Running
- Flash-Loan Governance Attack
- Flash-Loan Price Attack
- Denial Of Service (DOS) by complex fallback function
- Denial Of Service (DOS) by gas limit
- Denial Of Service (DOS) by non-existent address or malicious contract
- Floating Point Arithmetic
- ECDSA Signature malleability
- ECDSA Signature replay
- Replay Attack
- Price Oracle Manipulation
- Cross-Chain Bridge Manipulation
- Initial Supply Mint Issue
- Divide before multiply

- Integer Underflow
- DeFi Slippage attack
- Amplification Attack Double Spending
- Malicious Honeypot
- Unsafe Delegatecalls
- Loops Gas Limit
- Phishing With Improper Authorization
- Unexpected Ether With Forcibly Sending Ether
- Block timestamp Manipulation
- Unchecked return values
- Insecure Randomness
- Proxy Storage Collision
- Strict equalities
- Timestamp Dependence
- Use of Deprecated Functions
- Requirement Validation
- Absent modifiers
- Force Feeding
- Rounding Down To Zero

## 8. Start doing some CTFs (Optional)

- Ethernaut by @OpenZeppelin
-> https://ethernaut.openzeppelin.com
- Damn Vulnerable Defi by @tinchoabbate
-> https://damnvulnerabledefi.xyz
- Capture the Ether by @smarx
-> https://capturetheether.com
- Paradigm CTF by @paradigm_ctf
-> https://ctf.paradigm.xyz

## 9. Smart Contract Auditing Methodology & Process

- Process – https://twitter.com/ShieldifyAnon/status/1653126078578171922?s=20
- Methodology mindmap - https://t.co/SQF4Jxnxn8

## 10. Smart Contract Audit Checklist - (This is only if you like using checklists) - @SoloditOfficial

checklist - https://solodit.xyz/checklist
- SmartContracts-audit-checklist - https://t.co/cdfocNvcsS
- t11s checklist - https://t.co/vOWRmlXu5X
- The Ultimate 100+ Point Checklist Before Sending Your Smart Contract for Audit - https://betterprogramming.pub/the-ultimate-100-point-checklist-before-sending-your-smart-contract-for-audit-af9a5b5d95d0

## 11. You must read these papers **if you're auditing _____**

## **1.** Lending Protocol

- Lending and Borrowing: Link: https://t.co/adUsGzQvK4
- Liquidations: Link: https://t.co/ASzppXFkyi
- Rewards: Link: https://t.co/exPB5taUhe
- Typical vulnerabilities: Link: https://t.co/W7Ih0v8WQ3
- Attacks Checklist: Link: https://t.co/GDadbarki0
- Vectors of Attack and Preventing Potential Issues: Link: https://t.co/W71euMcbtR

## 2. AMM Protocol

- Decentralised Finance **and Automated Market Making: Link:** https://t.co/axHffm5TmV
- AMM Integration Tips: Link: https://t.co/DjQrXCYCvX
- Understanding the Vulnerabilities: Link: https://t.co/KARypoKnSW
- **Typical vulnerabilitie**s: Link: https://t.co/q7kf0ULahU
- DeFi Slippage Attacks: Link: https://t.co/EJwqGZXWgX
- Generalizing knowledge on DEXs with AMMs -Part I: Link: https://t.co/CYJSUreJoI
- Generalizing Knowledge on DEXs with AMMs -Part II: Link: https://t.co/oT3D2cOHGe

## 3. Liquid Staking protocol

- Staking withdrawals: Link: https://t.co/wfoeJQhl47
- How Do Ethereum Withdrawals Work: Link: https://t.co/X3tlMakFfq
- EIP-4895: Beacon chain push withdrawals as operations: Link: https://t.co/fwCKRRkURg
- Ethereum Distributed Validator Specification: Link: https://t.co/QNgKqockaD
- Maximal extractable value (MEV): Link: https://t.co/jCUvnmCUw2

## 4. Cross Chain Protocol(LayerZero) protocol

- Best Practice: Link: https://t.co/jwu2XrwvP4
- A Deeper Look Into DeFi's Cross-Chain Tech: Link: https://t.co/oetqTFQDON
- LayerZero Omnichain Contract Examples: Link: https://t.co/8iY1X0WHKN
- LayerZero Integration Checklist: Link: https://t.co/JZhPW8CPZC
- LayerZero's Cross-Chain Messaging Vulnerability Link: https://t.co/iZovtVC7gt
- Cross-Chain Security with LayerZero Labs: Link: https://t.co/wlO0Ic9xby
- UA Configuration Lock: Link: https://t.co/sGobPlPiEm

## 5. Cross-chain/Bridge

- Open problems in cross-chain protocols Link: https://t.co/nGIqpU1WG2

## 6. Protocol integrates with external Oracle smart contracts

- All about Oracles: Link: https://t.co/aVusAT9DVI
- The Dangers of Price Oracles in Smart Contracts: Link: https://t.co/1SIuqHMR1a
- TWAP Oracle Manipulation Risks, Mudit Gupta: Link: https://t.co/gCXMJHdMuA
- TWAP Oracles After the Merge, Mark Toda: Link: https://t.co/VjON9qs0NG
- So you want to use a price oracle: Link: https://t.co/M3QRszIA7U
- Pricing LP tokens | Warp Finance hack: Link: https://t.co/js90u5J2O9
- Uniswap V3 tick price manipulation: Link: https://t.co/R0BADP3aBR

- Chainlink Oracle Security Considerations: Link: https://t.co/u7T6VoijGc

### 7. ERC-4337(Account Abstraction)

- All About ERC-4337 (Account Abstraction): Link: https://t.co/FRSOMjHc4K
- Account Abstraction Security Guide: Link: https://t.co/CaU0faKjfu
- ERC4337 Audit Checklist: Link: https://t.co/g5ymwpyzHG

### 8. ZK (Zero Knowledge) Protocol

- A curated list of awesome ZK resources, libraries, tools and more: Link: https://t.co/cr8hPQ123V
- Security Reviews: Link: https://t.co/BZ5WhCZhqY
- ZK Bug Tracker - Common Vulnerabilities: Link: https://t.co/GYhHcq7Vky

### 9. NFT protocol

- NFT Attack Vectors: Link: https://t.co/hMAKb2gInK
- NFT attacks: Link: https://t.co/7PbdZAKe2r

### **10.** Vault Protocol

- Check if the user's balance is updated based on funds received and not the funds declared to be sent
- If there is a Vault in the system, then users' funds are stored on it - Check if the depositing rounds down the assets and withdrawing rounds up
- Check if shares are distributed in proportion to the user's deposited funds - Check that the vault is allowed to transfer tokens only from msg.sender to prohibit stealing from users who approved the vault contract

## 12. It's time for some practice **and earning money** 1.

@code4rena
- audits/contests 2.
@sherlockdefi
- audits/contests 3.
@HatsFinance
- competition + bug bounty platform 4.
@CodeHawks
- audits/contests 5.
@cantinaxyz
- audits/contests 6.
@immunefi
- bug bounty platform 7.
@HackenProof
- bug bounty platform

## 13. Bonus some books + Foundry Resources

- DeFi and the Future of Finance - https://t.co/1smIRe4IND

- How to DeFi: Advanced - https://t.co/p1Hx7NGmkM
- The Auditor book- Sherlock and Code4rena findings - https://theauditorbook.com
- Amazing List of Foundry Resources - https://t.co/uwnt4wEMLr