

Smart Contract Auditor Tools and Techniques

How to become a Smart Contract Auditor

- [How to become Smart Contract Auditor and Bounty Hunter by Officer CIA](#)
- [Auditor's Roadmap by RazzorSec](#)

Transaction Visualization tools for hacks

- [MistTrack](#)
- [Phalcon BlockSec](#)
- [Bitquery Explorer](#)
- [Tx eth samczsun](#)
- [Tenderly](#)
- [Cruise Supremacy](#)
- [Cross-chain transaction tracker](#)
- [Front-running explorer](#)

Stanford Defi Security Summit 2022

- [Day-1 Full](#)
- [Day-2 Full](#)
- [Defi-Security-Summit Channel](#)

Stanford Defi Security Summit 2023

- [Day-0 Full \(DeFi Security 101\)](#)
- [Day-1 Full](#)
- [Day-2 Full](#)

Miscellaneous Tools

- [Cryptocurrency OSINT](#)
- [Tool for Storage visualization of Proxy contracts & to check storage collision](#)
- [Uniswap TWAP Oracle Price Manipulation Simulator](#)
- [Metamorphic contracts detector](#)
- [Vscode on Etherscan](#)
- [EVM traces with Python](#)
- [Tool to detect Out of Gas/Denial of Service](#)
- [List of Defi Hacks with Proof of Concept](#)
- [Tool to extract ABI from Unverified contracts](#)
- [Tool to get historical data from EVM chains](#)
- [Immunefi Web3 Security library](#)
- [Ethers.js playground](#)
- [ETH-Toolbox: Useful tools for Ethereum devs](#)
- [EVM codes Interactive Playground](#)
- [Echidna Fuzzer](#)
- [Trade volume metrics across all chains](#)
- [Tool to check audited code diff on-chain](#)
- [Oracle risk rating system](#)

- [Tool to diff contracts using simhashes](#)
- [Tool to match hashes of known contracts](#)
- [ABI decompiler](#)
- [Database](#) and [tool](#) to detect and report scams
- [Rug Checker tools](#)
- [User friendly Metadock extension by BlockSec](#)
- [Tool for checking cross-function and cross-contract reentrancy](#)
- [Tool to guess type of ABI encoded data](#)
- [Running slither and other tools on cloud](#)
- [samczsun's tool to get function signature from abi.encoded data](#)
- [Visualize EVM storage \(finally!\)](#)

On-Chain Monitoring tools for attacks (Refer [Pessimistic-blog](#))

- [Forta](#)
- [Defender](#)
- [Tenderly](#)
- [Lossless](#)
- [Hackless](#)
- [Blocknative](#)
- [Seraph](#)
- [Slowmist monitor](#)
- [Ironblocks](#)
- [Hypernative](#)
- [Hacken Extractor](#)
- [\[QuickNode's QuickAlerts\]](#)

- [Cyvers.ai](#)
- [Hexagate](#)
- [Peckshield's KillSwitch](#)

On-chain Simulators for user-Side Defense

- [Fire](#)
- [Pocket Universe](#)
- [Stelo](#)
- [Interlock](#)
- [Wallet guard](#)
- [Meshed Labs](#)
- [Blowfish](#)
- [Hexagate](#)
- [Rabby.io](#)- Alternative to metamask

OffcierCIA On-chain Investigation Tools

- [Ethtective](#)
- [Breadcrumbs](#)
- [Hal](#)
- [Dune Analytics](#)
- [Nansen.ai](#)
- [Bloxy.info](#)
- [Tx2uml](#)
- [EVM Trace](#)

- [3D VR blockchain visualization](#)
- [Unrekt.net](#)
- [Revoke.cash](#)
- [Tutela](#)

Echidna Fuzzing resources

- [Why Echidna is the best smart contract fuzzer](#)
- [Breaking solidity compiler with Fuzzing](#)
- [More on fuzzing using Echidna](#)
- [ToB setting up fuzzing for clients](#)
- [ToB livestream on fuzzing using Echidna](#)
- [Hybrid Fuzzing](#)
- [Intro to advanced, with tips & FAQs](#)

Symbolic Execution / Formal Verification Tools

- [Halmos](#)
- [Certora](#)
- [Mythril](#)
- [Kontrol](#)
- [hevm](#)

Static analysis Tools and More!

- [Oyente](#)

- [Osiris](#)
- [Maian](#)
- [TeEther](#)
- [Sereum](#)
- [ContractFuzzer](#)
- [ILF](#)
- [Slither](#)
- [Vandal](#)
- [Madmax](#)
- [Ethir](#)
- [Smartcheck](#)
- [SaferSC](#)
- [RecChecker](#)
- [KEVM](#)
- [Eth-Isabelle](#)
- [SmartPulse](#)
- [Semgrep](#)
- [C4udit](#)

Smart contract Security Techniques and Best practices (Refer [DefiVulnLabs](#))

- [Mastering Ethereum - Smart Contract Security](#)
- [Smart Contract Best Practices- The Smart Contract Security Field Guide](#)
- [Awesome-Smart-Contract-Security](#)
- [\(Not So\) Smart Contracts](#)
- [Smart contract best practices by ToB](#)

- [Smart Contract Attack Vectors](#)
- [Secureum Security Pitfalls 101](#)
- [Secureum Security Pitfalls 201](#)
- [How to Secure Your Smart Contracts: 6 Solidity Vulnerabilities and how to avoid them \(Part 1\)\(Part 2\)](#)
- [Top 10 DeFi Security Best Practices](#)
- [All Ethereum EIPs](#)
- [Missing support for EIP-2930 on BSC- Beware Multisigs!](#)
- [Handling "missing return" ERC20 tokens](#)
- [All types of Reentrant attacks](#)
- [Smart Contract Weakness Classification Registry \(SWC Registry\)](#)
- [Ethereum Post Merge Security and known attack vectors](#)
- [Best practice for Upgradeable smart contracts](#)
- [Guide to Governance attacks](#)
- [How to avoid Governance attacks](#)
- [DAO Governance Attacks and how to avoid them](#)
- [A white hat mindset- From the perspective of a smart contract auditor](#)
- [Commit and Reveal scheme to mitigate Front-run attacks](#)
- [Price Oracle Best practices](#)
- [Solving the issue with slippage in EIP-4626](#)
- [Defi Slippage attacks](#)
- [NFT Security collection](#)
- [Proxy contracts security guide](#)
- [Awesome Oracle manipulation](#)
- [100 point checklist before sending your smart contract for audits](#)
- [Solcurity security checklist for audits](#)

- [Smart contract Audit Checklist](#)
- [Solodit audit checklist](#)
- [Smart Contract Security Verification Standard \(SCSVS\)](#)
- [Top 10 Hacking Techniques of 2022- by Openzeppelin](#)
- [Question until it crashes- by Tincho](#)
- [Reproducing MEV attacks](#)
- [Chainlink oracle attacks](#)
- [Checklist for Signature verification](#)
- [Signature Replay attacks](#)
- [Improper verification of signatures](#) [SWC-121](#) and [SWC-117](#)

Audit reports and findings

- [Code4rena Audit reports](#)
- [Sherlock Audit reports](#)
- [The Auditor book- Sherlock and Code4rena findings](#)
- [Search Code4rena and Sherlock findings](#)
- [Immunefi Bug Bounty Writeups](#)
- [Solodit search with filters](#)
- [All Audit reports of Security companies](#)
- [List of Bridge hacks](#)

ZK security and Learning resources

- [Intro to Zk Security](#)
- [Zk bugs tracker](#)

- [Zk hash collision vulnerability](#)
- [Common Zero-Knowledge Proof Vulnerabilities](#)
- [Zk auditing cohort open sourced](#)
- [Zk Camp's Aztec/Noir Cohort](#)
- [Zk learning with 0xparc](#)
- [Zk learning resources by Shanzson :\)](#)

Free smart contract security-related resources

- [Ethereum Yellow paper course](#)
- [Awesome Openzeppelin](#)
- [Stanford Cryptography course](#)
- [Mastering Solidity Assembly \(YUL\)](#)
- [All about assembly](#)
- [Cyfrin's auditing course](#)

Privacy Tools

- [Tool for Private RPC](#)
- [Hop protocol](#)
- Using [Zmok](#) along with [Mullvad VPN](#)

Ethereum blogs to Deep Dive

- [Timeline of all Ethereum forks and upgrades](#)
- [How data is stored in Ethereum](#)

PoCs

- [Coinspect EVM attacks](#)
- [Defi Hack Labs](#)

Miscellaneous

- [List of all Blockchain security companies](#)
- [Upgrading Ethereum Eth2Book](#)
- [Deconstructing a Solidity contract series \(to understand and debug byte level code\)](#)
- [Solidity Notes by Chinmaya](#)
- [Formal verification Speedrun with Halmos, Kontrol and Certora](#)