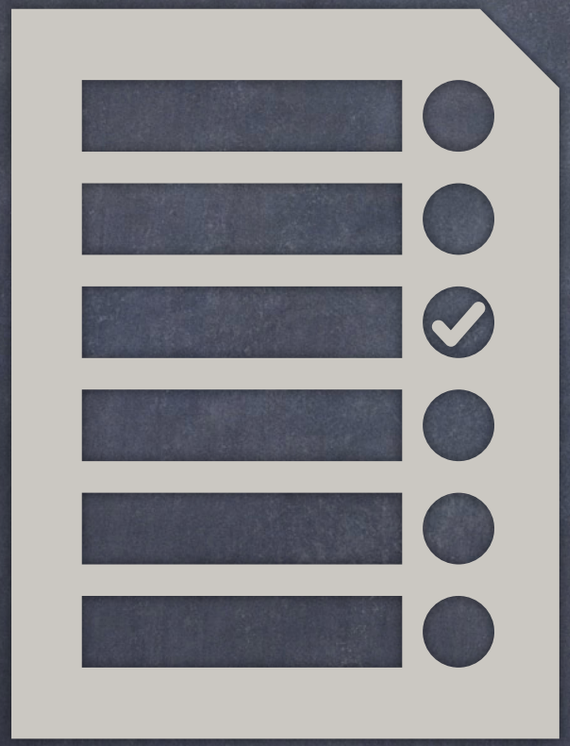
Audit Techniques & Tools 101

Secureum Bootcamp

#1

Audit



External Security Assessment

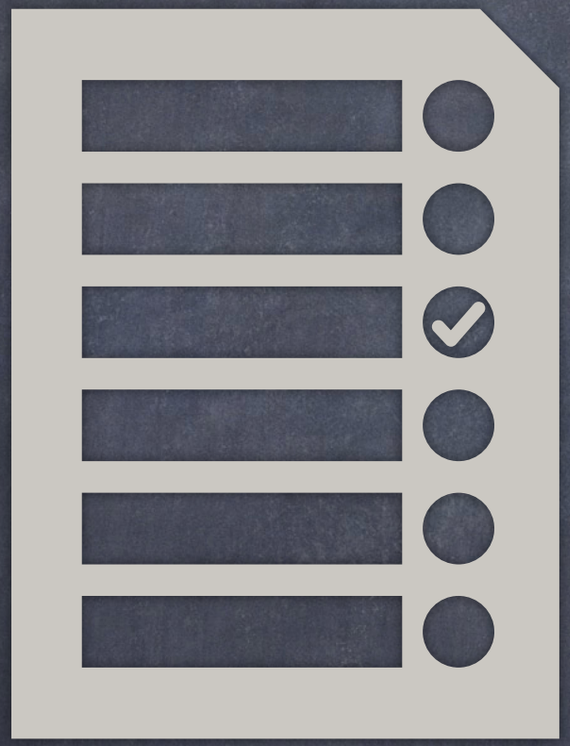
Security Vulnerabilities

Pitfalls & Best Practices

Software Quality

#2

Scope

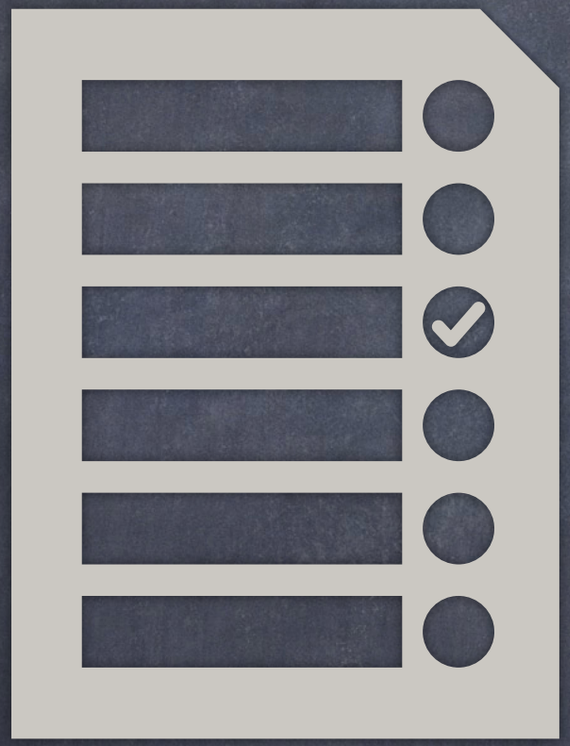


Smart Contracts

Offchain Code

#3

Goal



Assess & Alert

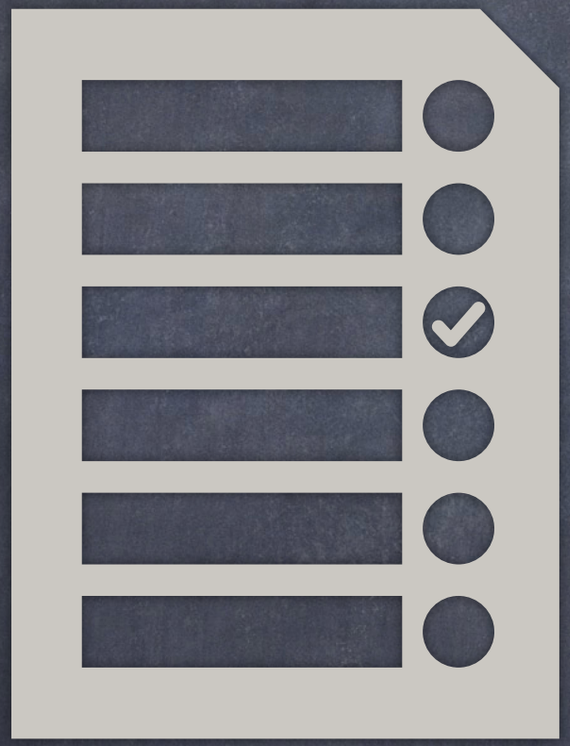
Security Posture

Attack Surface

Mitigate Risk

#4

Non-Goal



Security Warranty

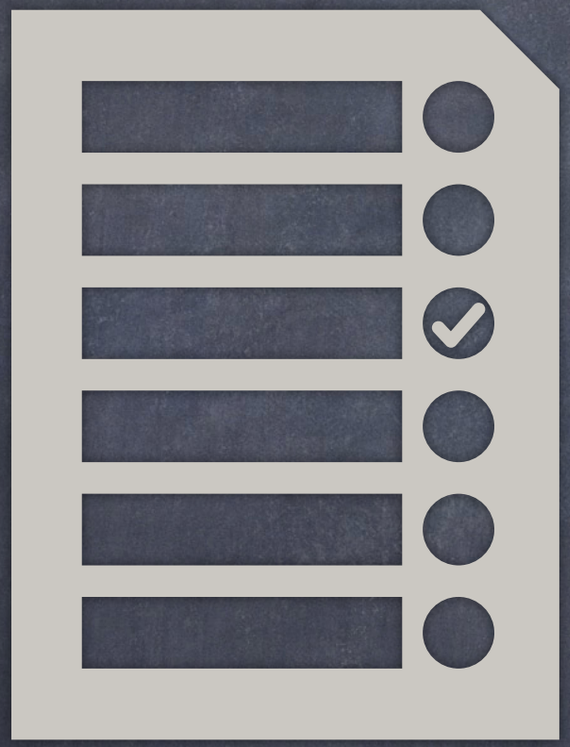
Bug Free

Best Effort

Constraints

#5

Target



Project Teams

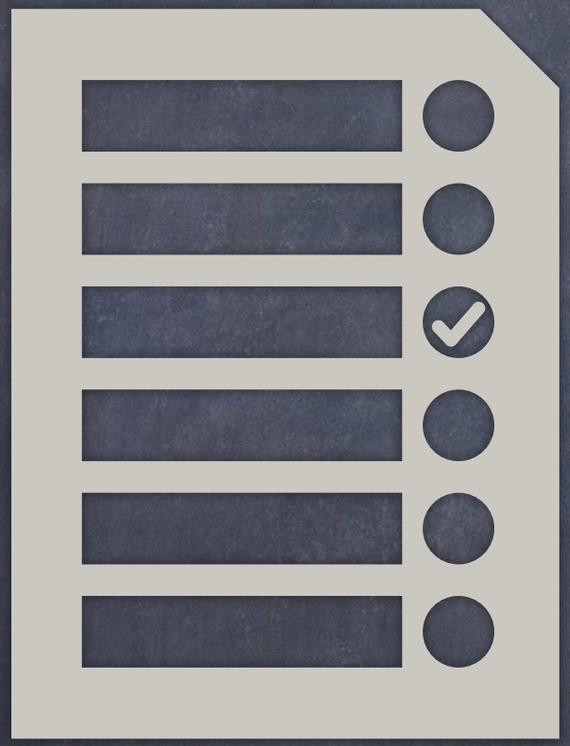
Paying Clients

Not Project Users

Technical/Business Goals

#6

Need



In-house Expertise

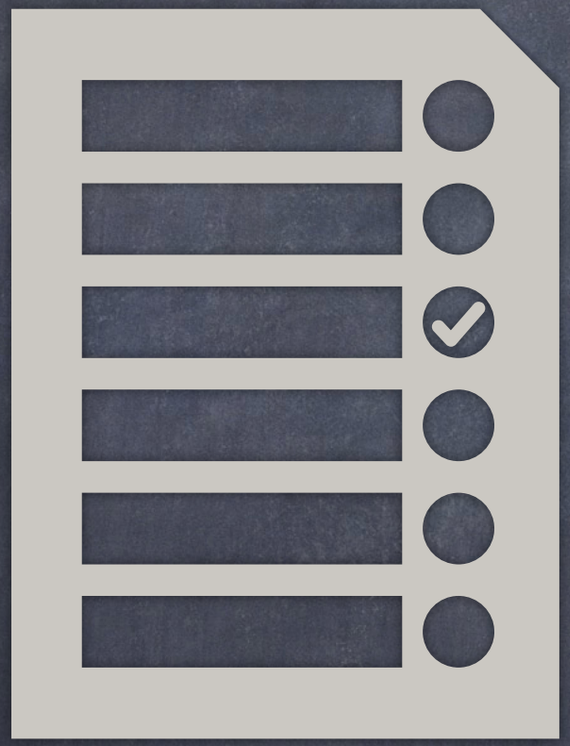
Time/Effort

External Review

Domain Experts

#7

Types



New/Repeat

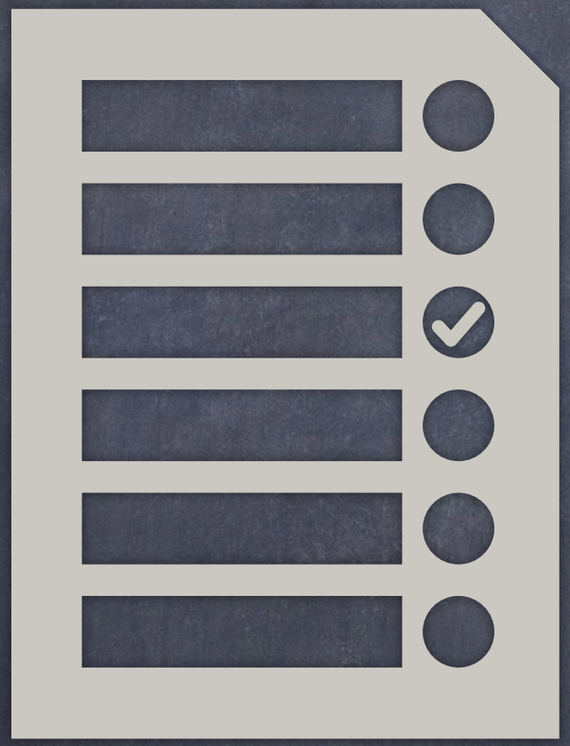
Fix

Retainer

Incident

#8

Timeline



Type/Scope/Nature

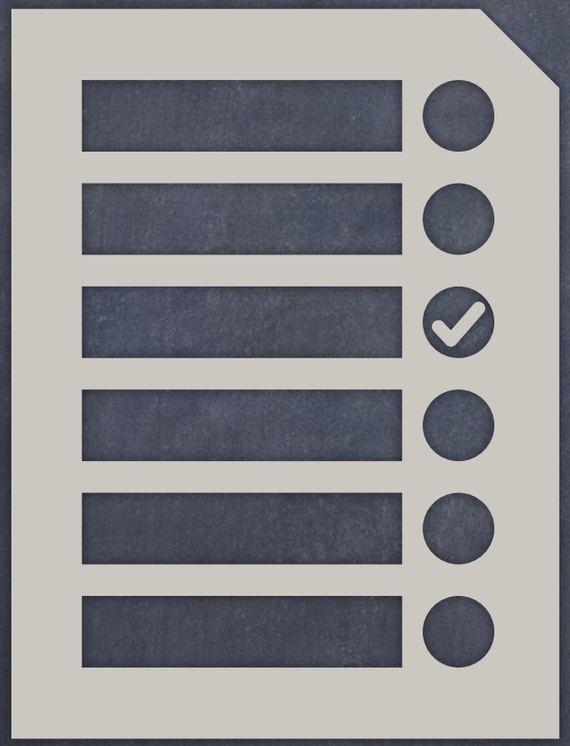
Days

Weeks

Months

#9

Effort



Number of Auditors

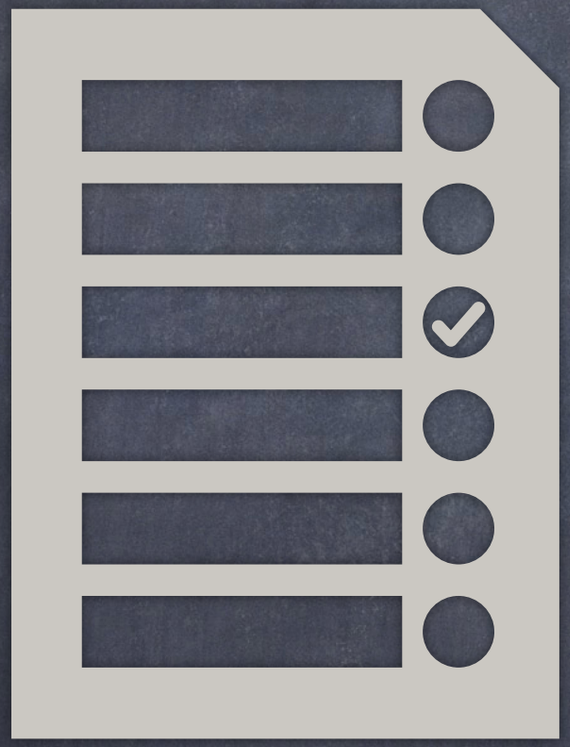
More than One

Supplementary/
Complementary

Expertise/Experience

#10

Cost



Type/Scope/Nature

Audit Firm

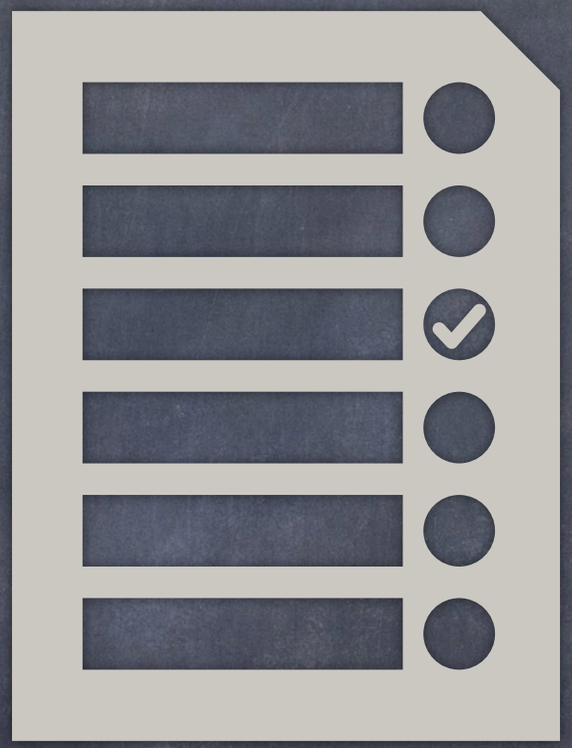
Demand/Supply

Thousands of $s

#11

Pre-Reqs

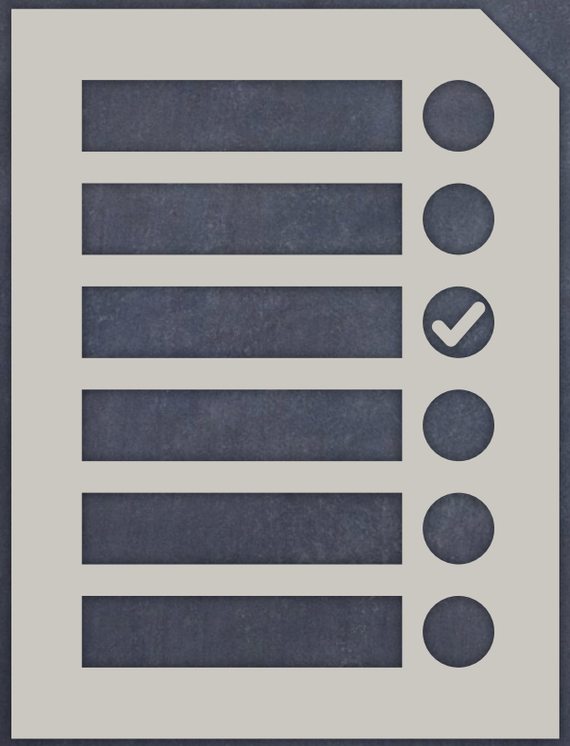
- Clear Scope
- Repository
- Team
- Specification
- Documentation



- Threat Model
- Prior Reviews
- Timeline/Effort
- Engagement Mode
- Point of Contact

#12

Limitations



Residual Risk

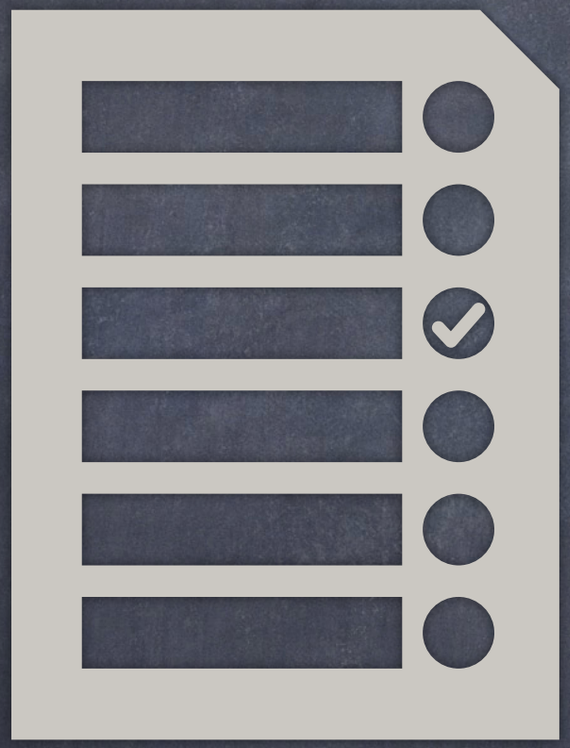
All Audits -> Not Equal

Snapshot

Necessary/Sufficient

#13

Reports



Scope/Goals/Effort/
Timeline/Approach/Tools

Findings/Classification/
Severity/Exploits/Fixes

Recommendations/Best-
practices

Comprehensive Document

#14

Classification

Access Control

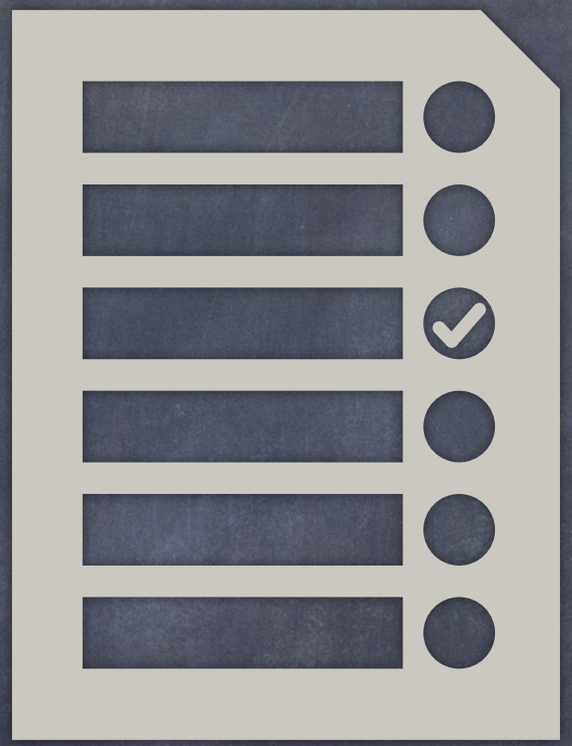
Auditing/Logging

Authentication

Configuration

Cryptography

Data Exposure



Data Validation

Denial-of-Service

Error Reporting

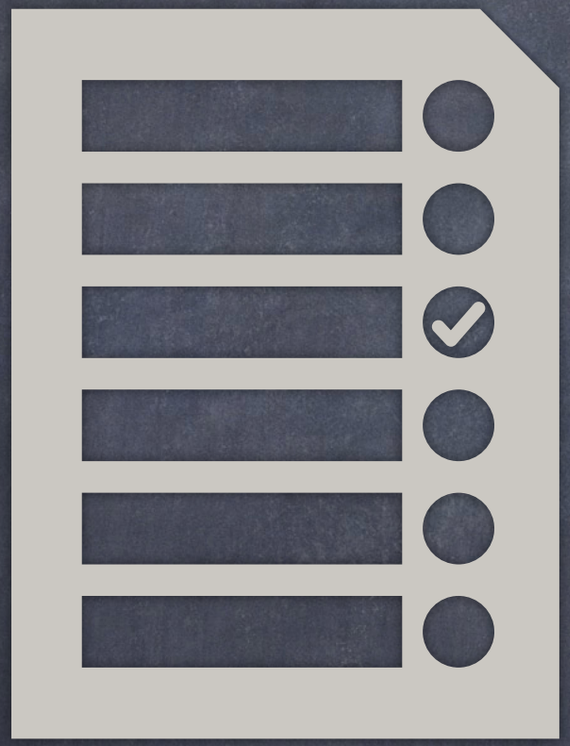
Patching

Session Management

Timing

#15

Difficulty



OWASP

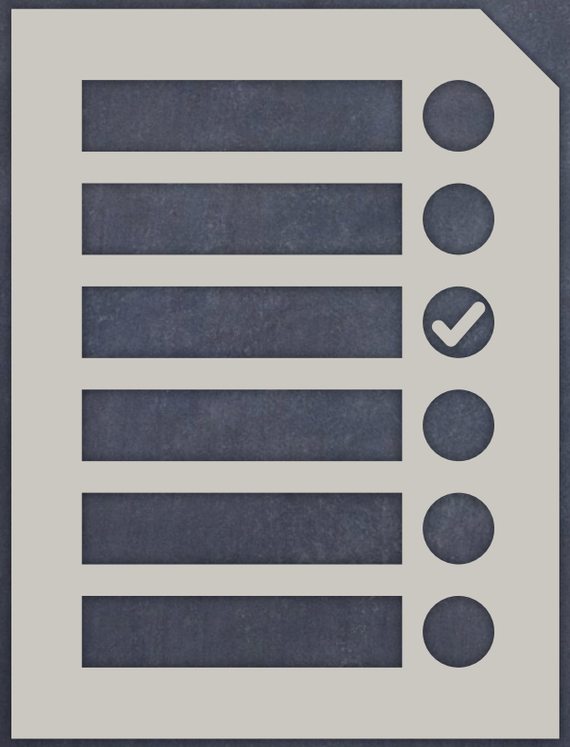
Low

Medium

High

#16

Impact



OWASP

High

Medium

Low

#17

Severity

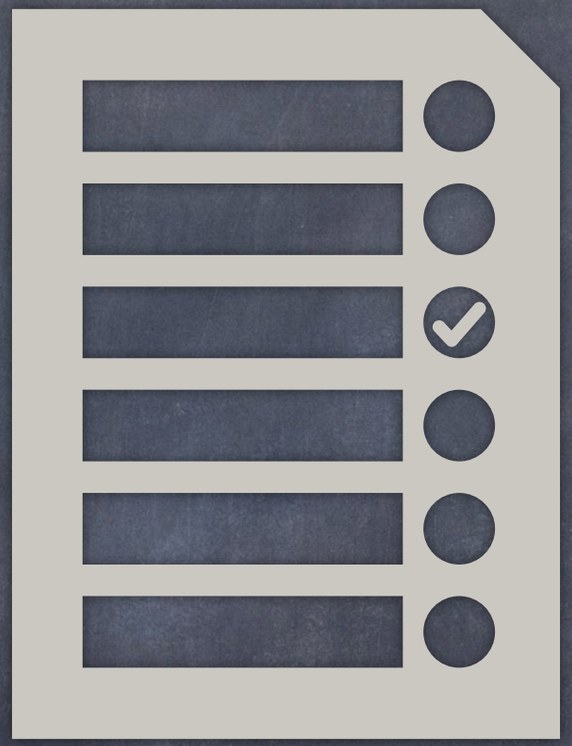
OWASP: Likelihood x Impact

Low-Low=Note

Low-Med=Med

Low-High=High

Med-Low=Low



Med-Med=Med

Med-High=High

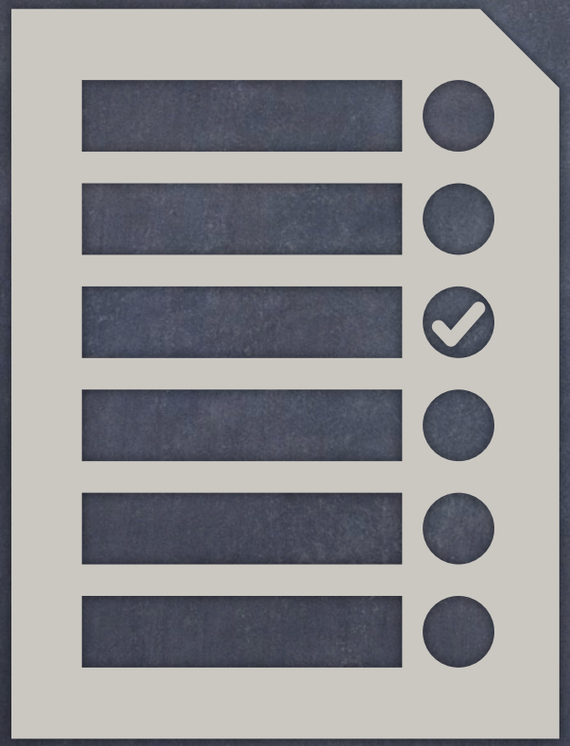
High-Low=Med

High-Med=High

High-High=Critical

#18

Checklist



Test

Internal Review

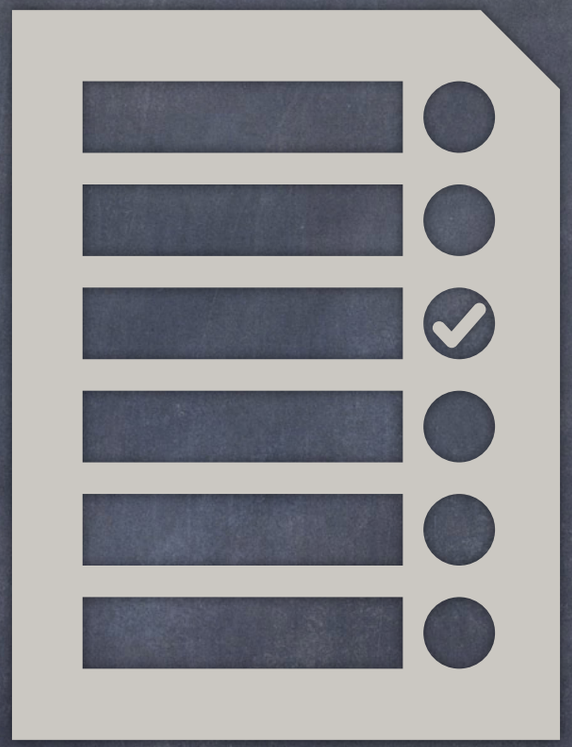
Document

Communicate

#19

Analysis Techniques

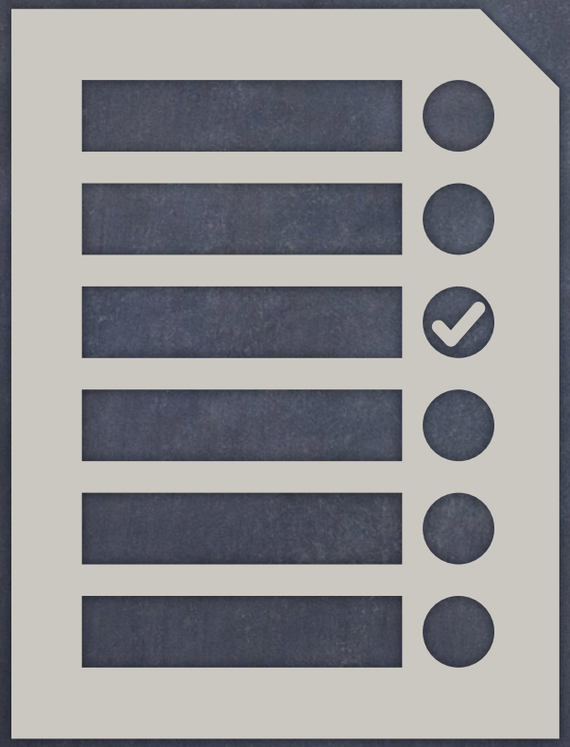
- Manual/Automated
- Specification
- Documentation
- Testing
- Static Analysis



- Combination
- Fuzzing
- Symbolic Checking
- Formal Verification
- Manual Analysis

#20

Specification



What/Why
Requirements/Design

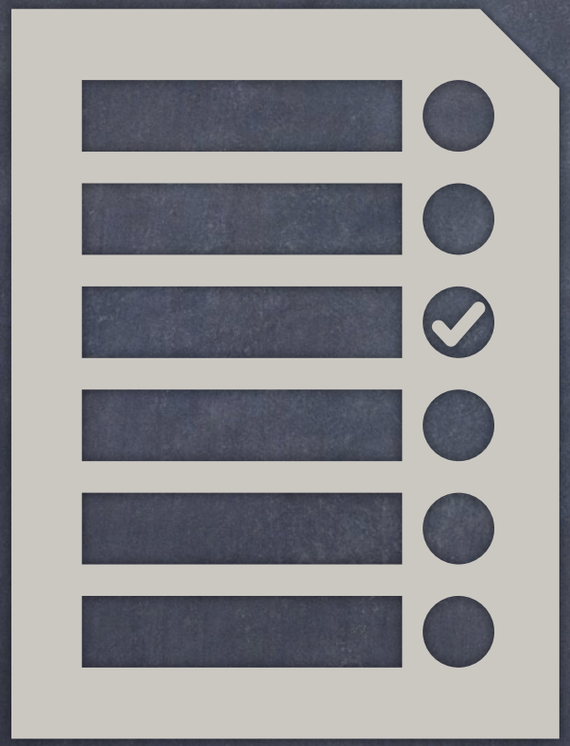
Assets/Actors
Trust/Threat

Assumptions/Shortcomings

Infer: Lost Time

#21

Documentation



What/How
Architect/Implement

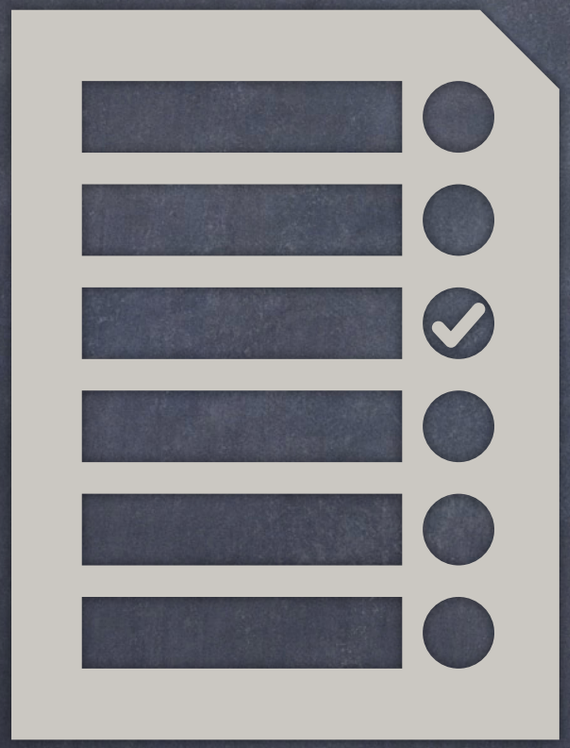
README/Comments

Assumptions/Shortcomings

Infer: Lost Time

#22

Testing



Software Engineering

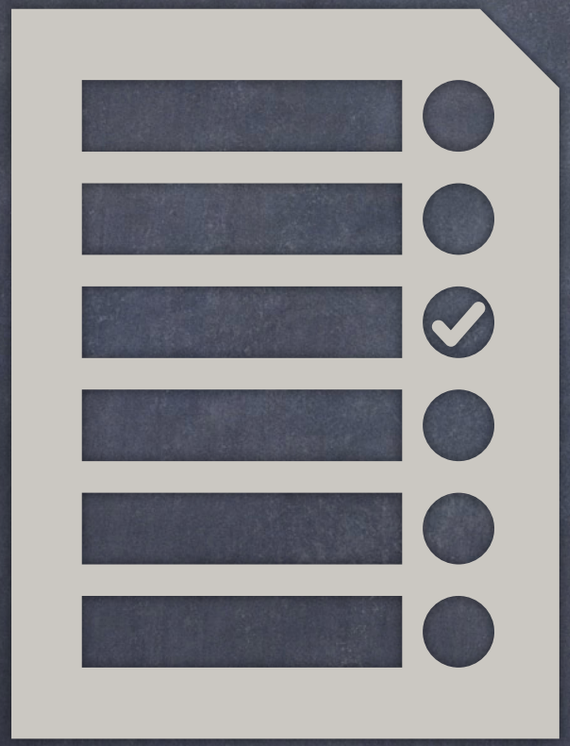
Expected Outputs
Chosen Inputs

Unit/Functional/
Integration/E2E/Smoke

Test Cases/Coverage

#23

Static Analysis



W/o Program Execution

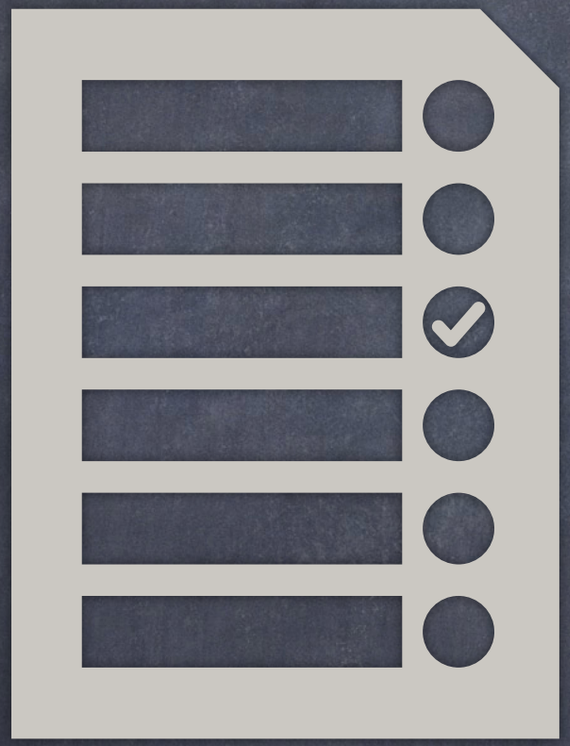
Solidity/EVM

Control+Data Flow

E.g.: Slither, Maru

#24

Fuzzing



Software Testing

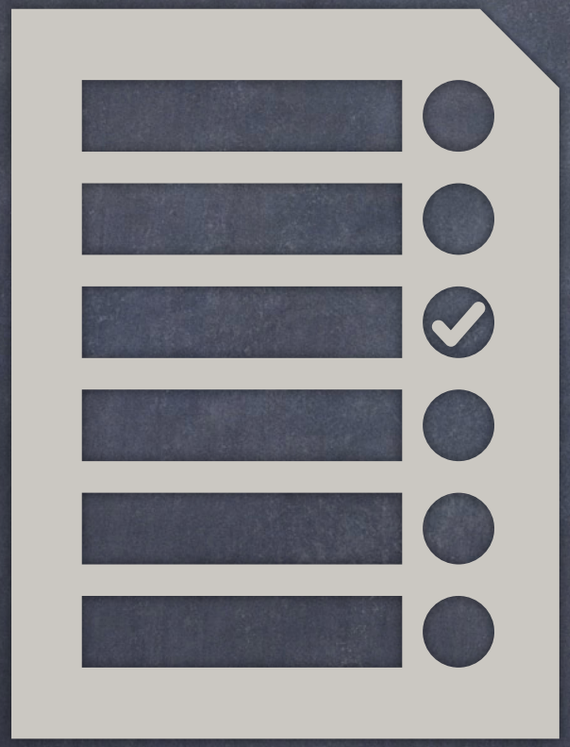
Random/Invalid Inputs

Monitor
Crashes/Failures/Leaks

E.g.: Echidna, Harvey

#25

Symbolic Checking



Symbolic Inputs
Set of States/Transitions

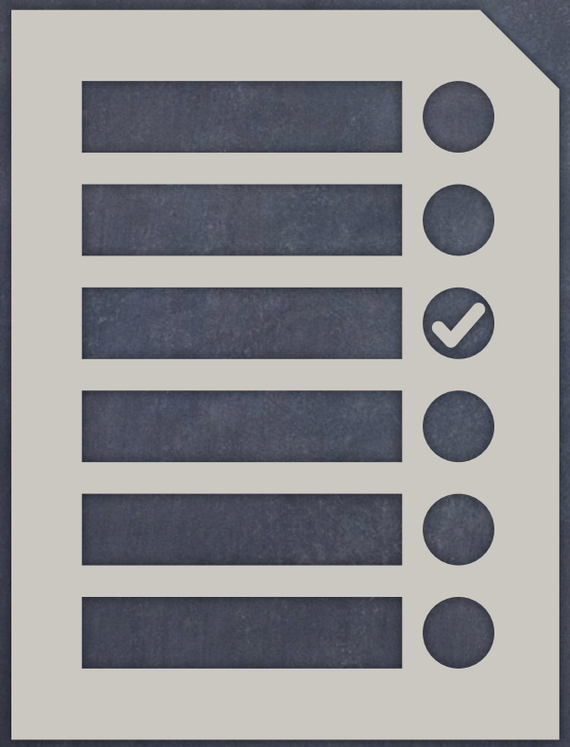
Models & Properties

Language & Logic

E.g.: Manticore, Mythril

#26

Formal Verification



Proving Correctness

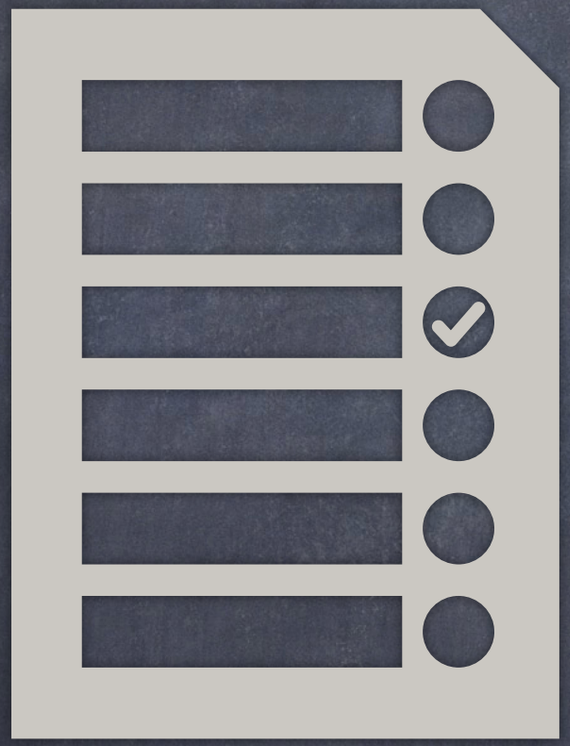
Formal Specification & Methods

Specific/Deep Properties

E.g.: Certora Prover, VerX, KEVM

#27

Manual Analysis



Complementary to Automated Analysis

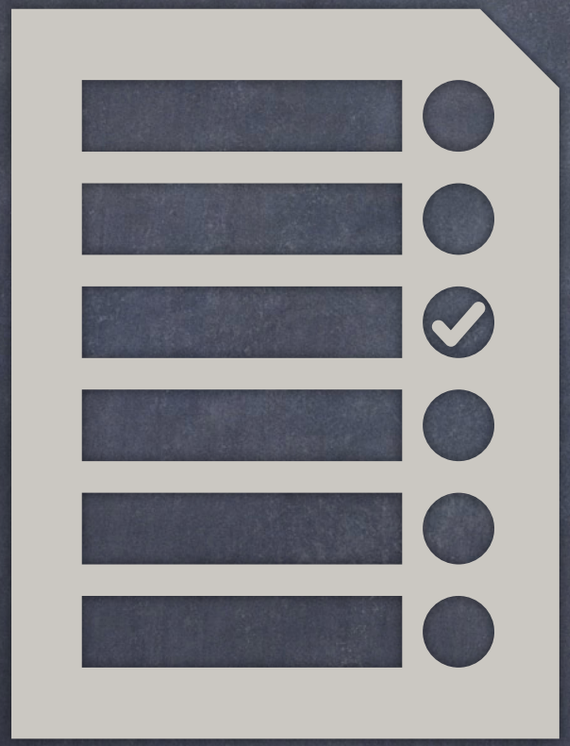
Business Logic & Application Constraints

Slow & Expensive
Not Deterministic/Scalable

Critical Human Aspect

#28

False Positives



Incorrectly Flagged Vulnerabilities

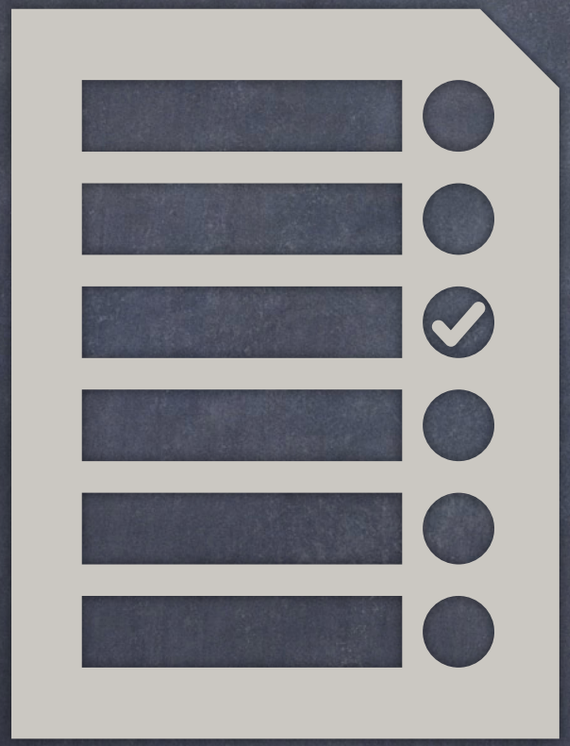
Incorrect Assumptions or Analysis Simplifications

Increases Effort
Decreases Confidence

True vs False Positives

#29

False Negatives



Missed Flagging Vulnerabilities

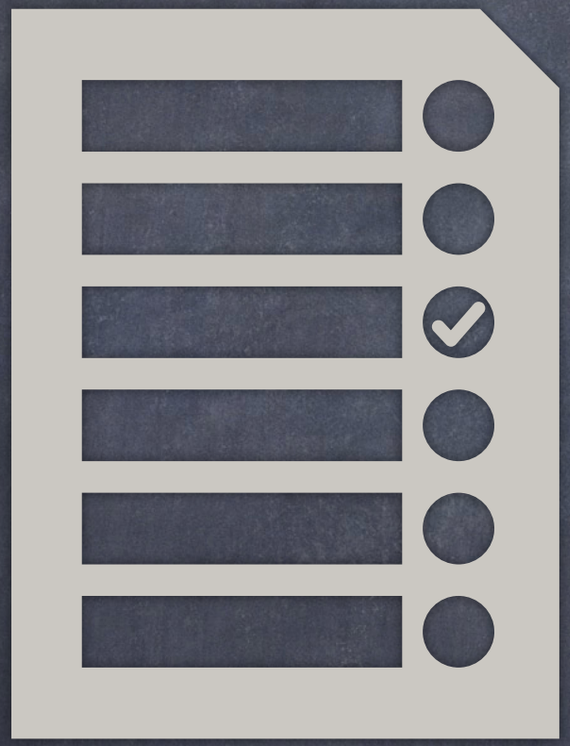
Incorrect Assumptions or Analysis Inaccuracies

Increases Risk
Decreases Confidence

True vs False Negatives

#30

Audit Firms



Security Expertise

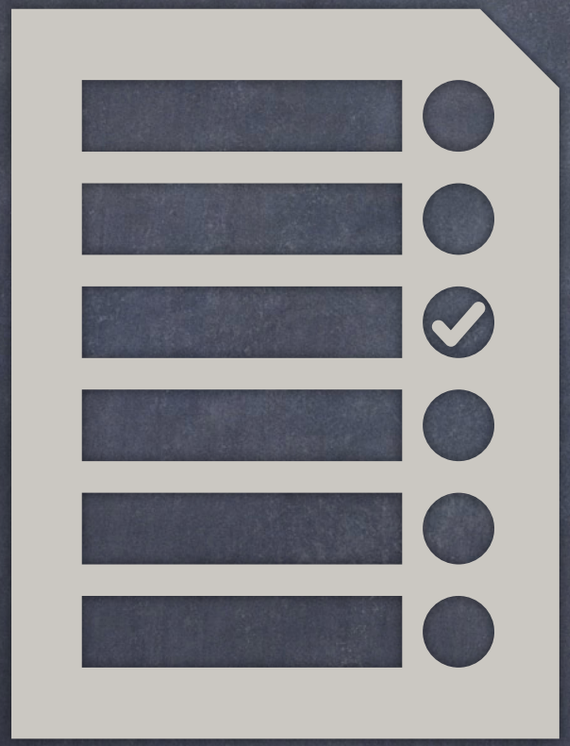
Smart Contracts, Ethereum

Traditional vs Specialized

E.g.: ConsenSys Diligence,
Sigma Prime, Trail of Bits

#31

Security Tools



Assist Developers & Auditors

Potential Vulnerabilities

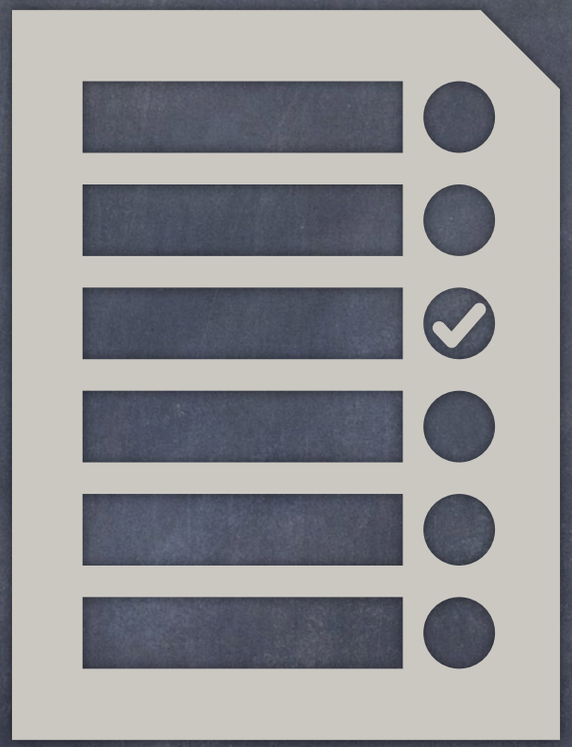
Common Pitfalls
Best Practices

Complement Manual Analysis

#32

Security Tools

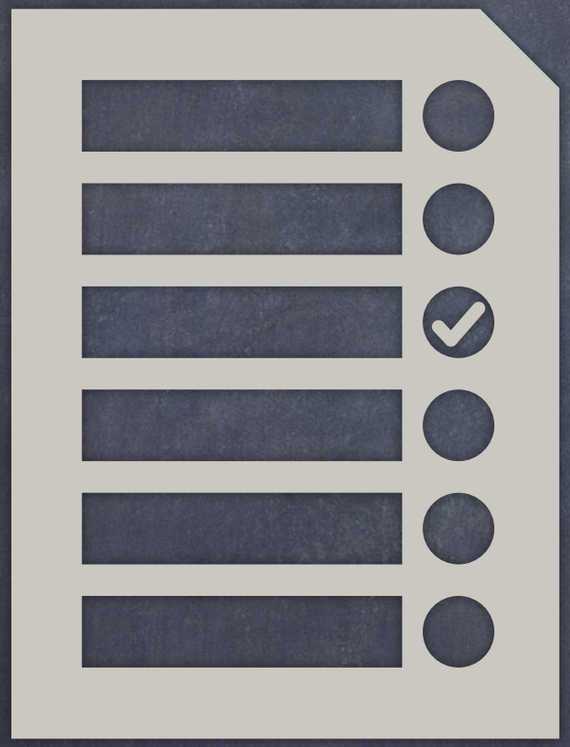
- Testing
- Test Coverage
- Linters
- Static Analysis
- Symbolic Checkers



- Fuzzing
- Formal Verification
- Visualization
- Disassemblers
- Monitoring

#33

Slither
Overview



Static Analysis Tool
Trail of Bits

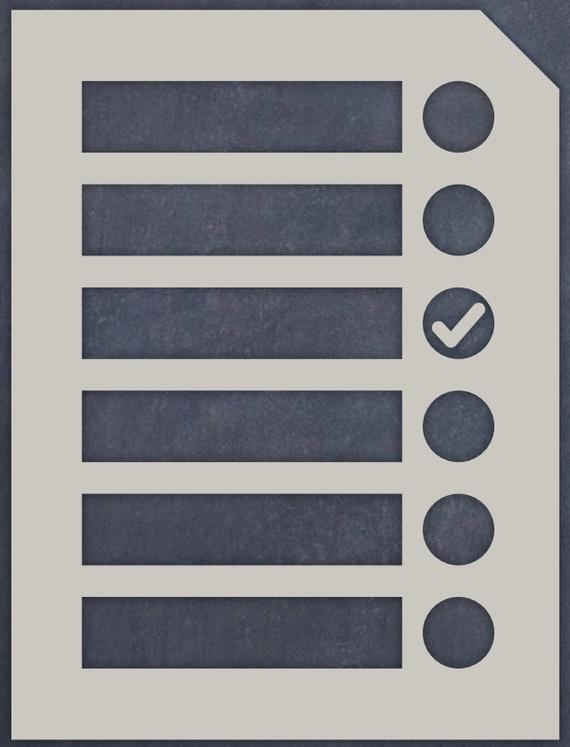
Solidity, Python 3
Easy-to-use, Free

Solidity/EVM Pitfalls
Best Practices

75+ Detectors, Custom
Analyses, Printers & More

#34

Slither
Features



Vulnerability Detectors,
Contract Info Printers

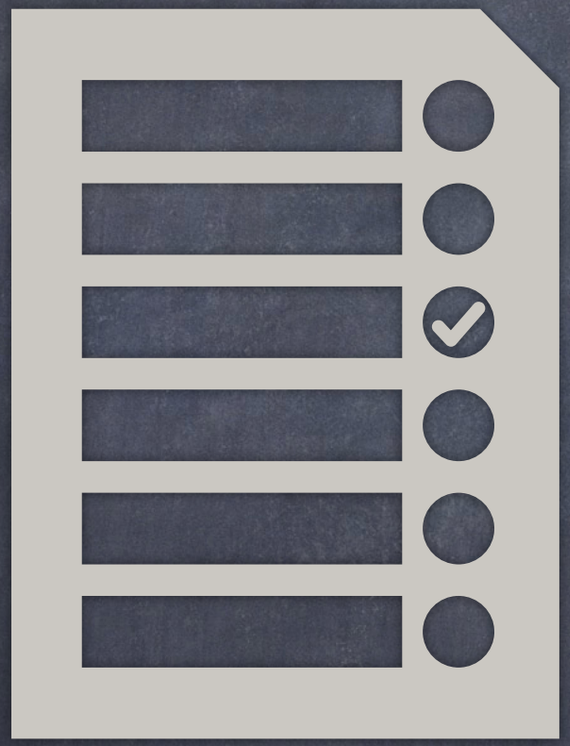
Low False Positives
Runtime < 1 sec/contract

Continuos Integration
Supports Most Frameworks

SLithIR
High-precision Analyses

#35

Slither Detectors



75+ Detectors

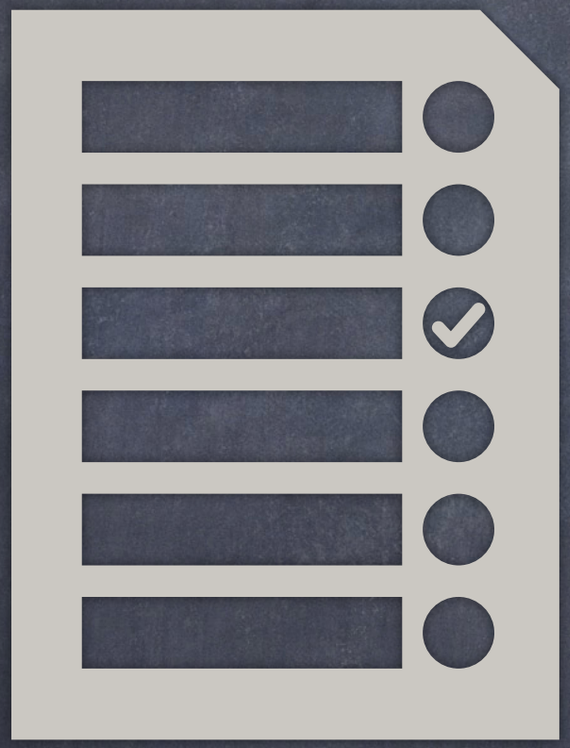
Truffle/Embark/Dapp/ Etherlime/Hardhat

Run/Exclude Specific Detectors

E.g.: reentrancy-eth, unprotected-upgrade

#36

Slither Printers



Print Different Contract Information

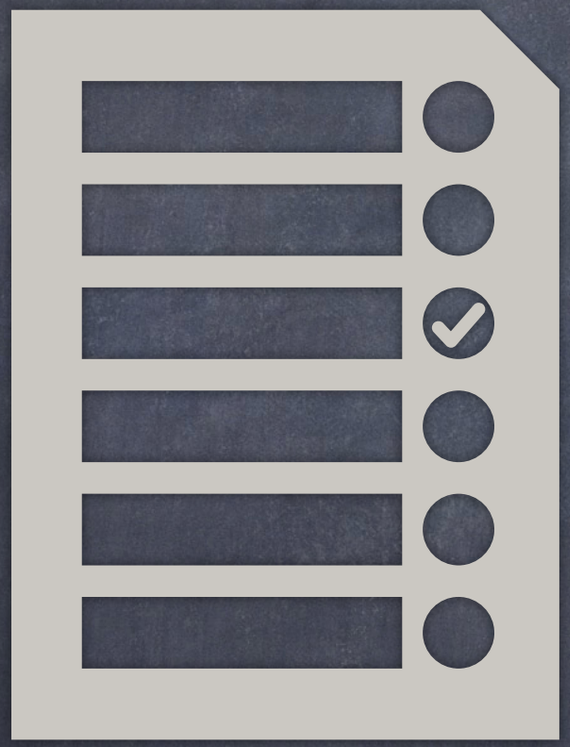
CFG, Call graph, Summaries, Inheritance

Functions, Modifiers, Variables, Dependencies

SlithIR, EVM

#37

Slither Upgradeability



Delegatecall Proxy/ Implementation/V2

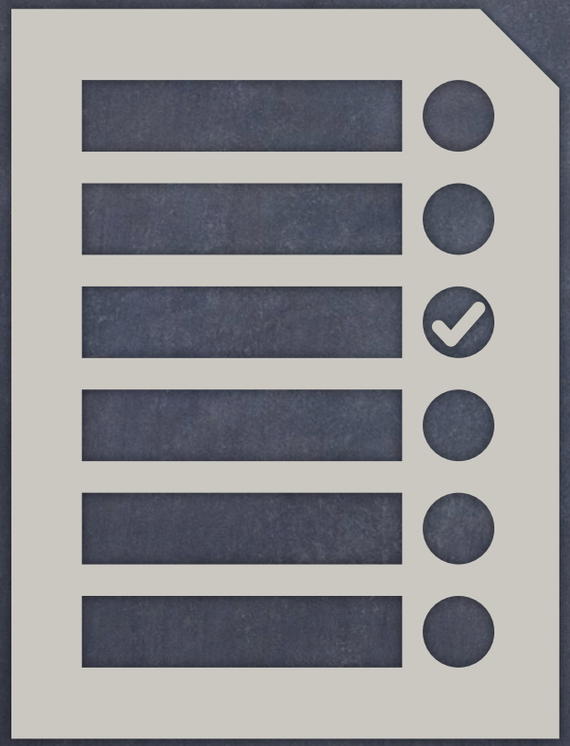
Variables: Missing/Extra/ Order/Initialized

Init: Missing/Multiple/ Initializer

Functions: Collision/ Shadowing

#38

Slither Code Similarity



Detect Similar Solidity Functions

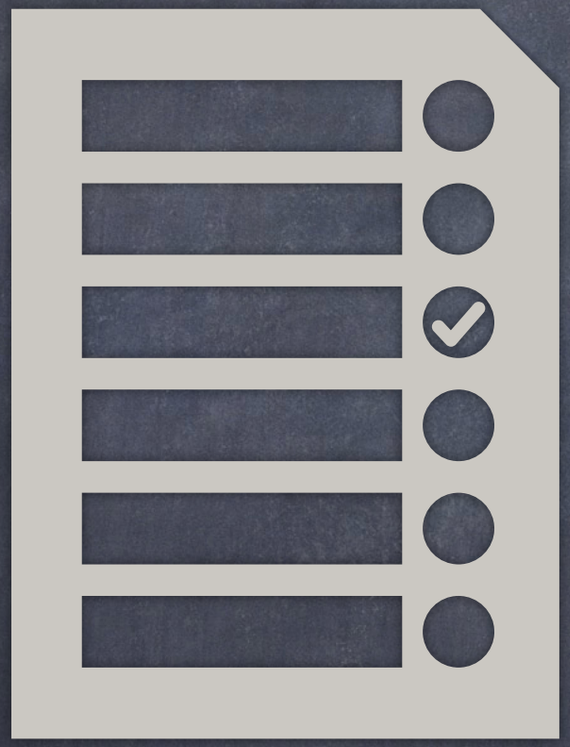
ML: Trained Models, Etherscan Verified

60K Contracts, 850K Functions

Copy/Fork Vulnerabilities

#39

Slither Flat



Contract Flattening Tool

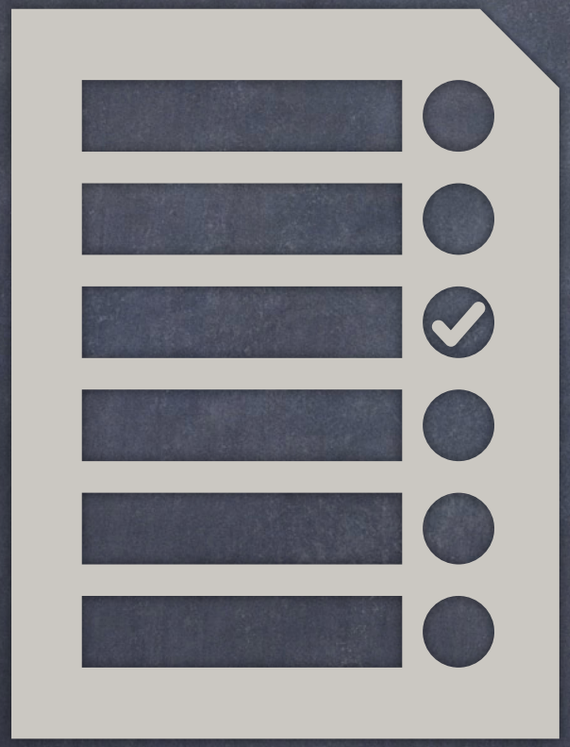
Strategies: Most Derived, One File, Local Import

Circular Dependencies

Platforms: Truffle, Hardhat, Etherlime etc.

#40

Slither-Format



Automatic Patch Generation

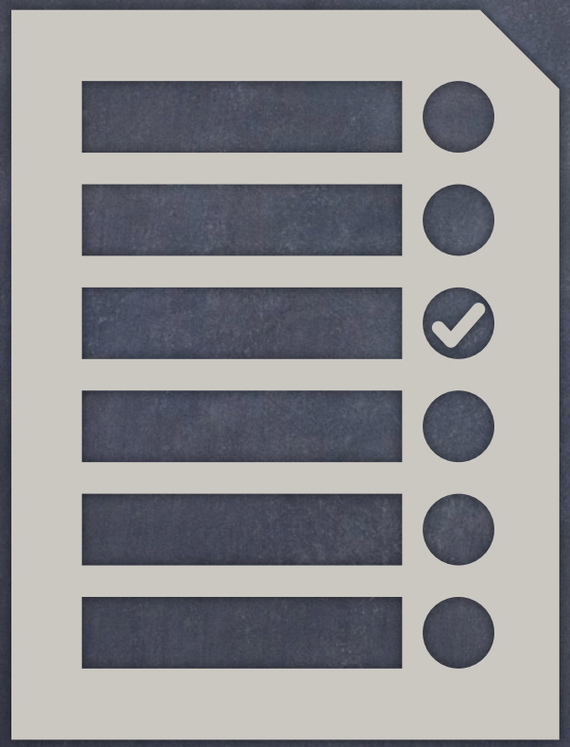
Git Compatible

Detectors: Unused State, Naming Convention etc.

Review & Apply

#41

Slither ERC Conformance



ERC Conformance Tool

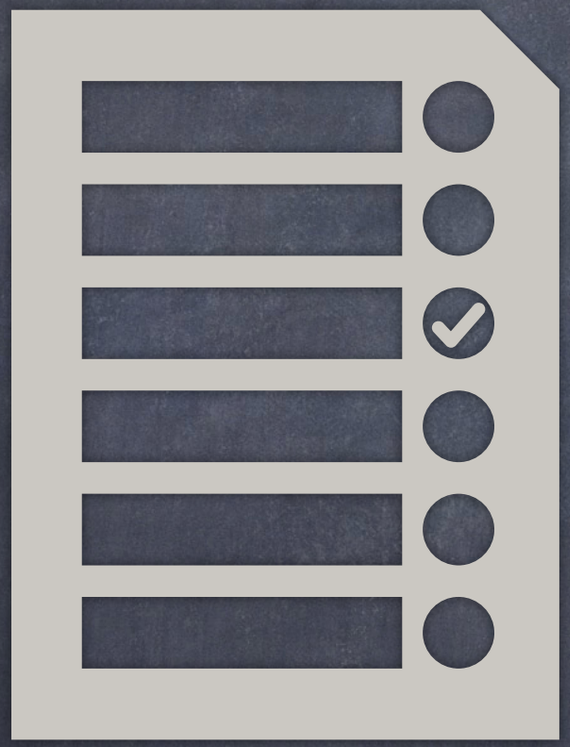
ERC20, ERC721, ERC777, ERC165, ERC223, ERC1820

Functions: Present/ Return/View etc.

Events: Present/Emit/ Indexed etc.

#42

Slither-Prop



Property Generation Tool

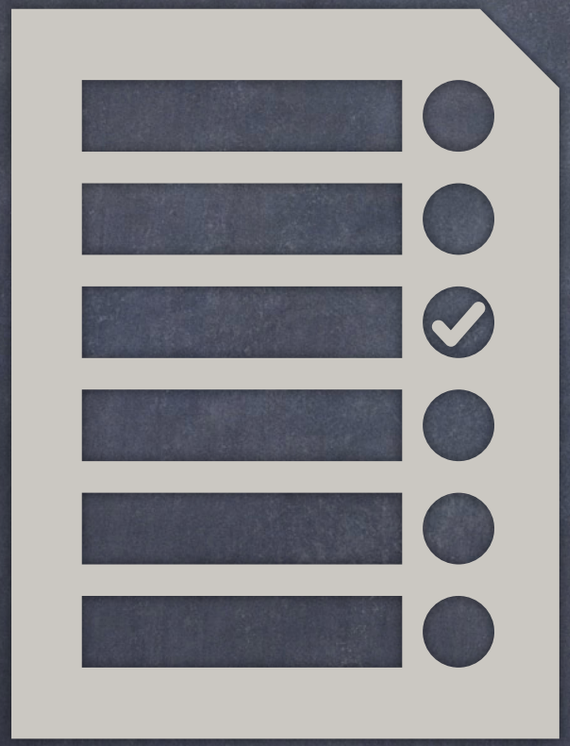
Code Properties/
Invariants

Test w/ Unit Tests or
Echidna

ERC20 Scenarios

#43

Slither New Detectors



Extensible Architecture
New Detectors

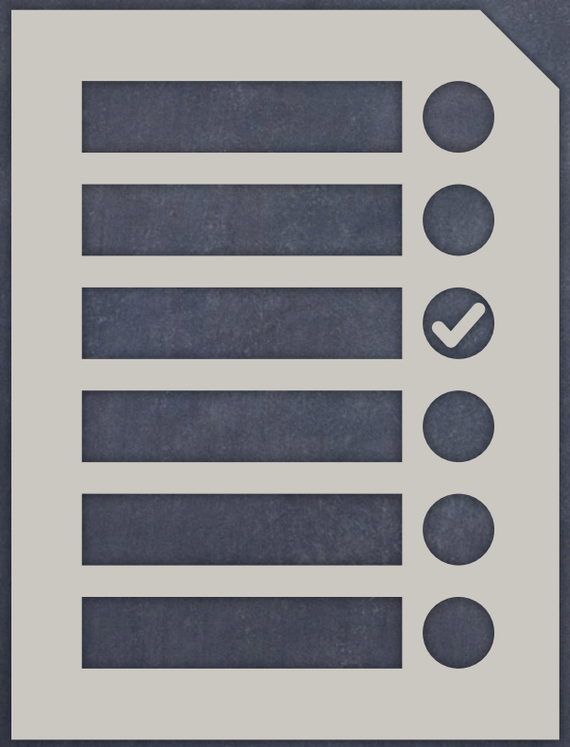
Argument, Help, Impact, Confidence, Wiki

_detect(): Detector Logic

Project Specific/
Community Contributions

#44

Manticore



Symbolic Execution Tool
Trail of Bits

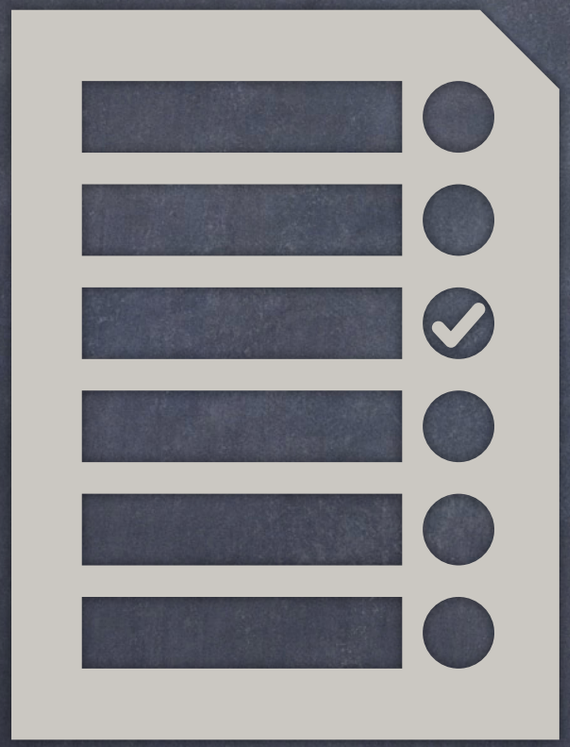
Symbolic Inputs -> State Exploration

Input Generation, Error Discovery

Instrumentation, Programmatic Interface

#45

Echidna



Fuzzing Tool
Trail of Bits

Haskell-based

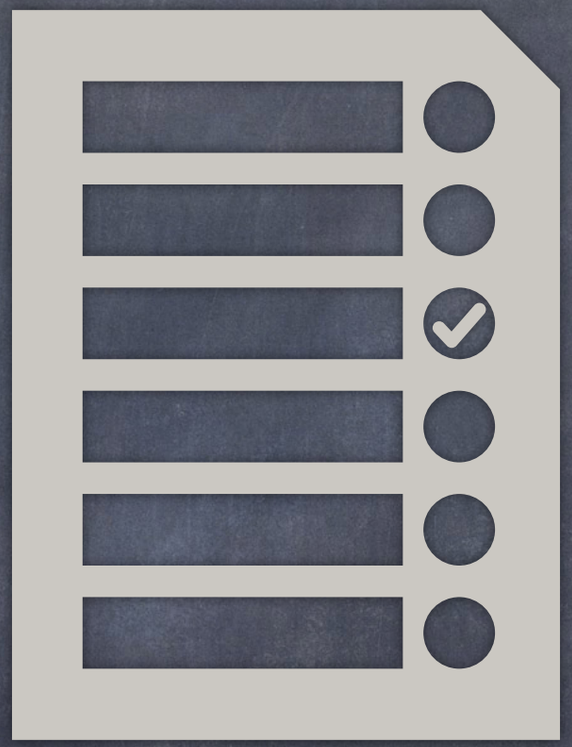
Grammar-based Fuzzing Campaigns

Falsify Predicates/ Assertions

#46

Echidna Features

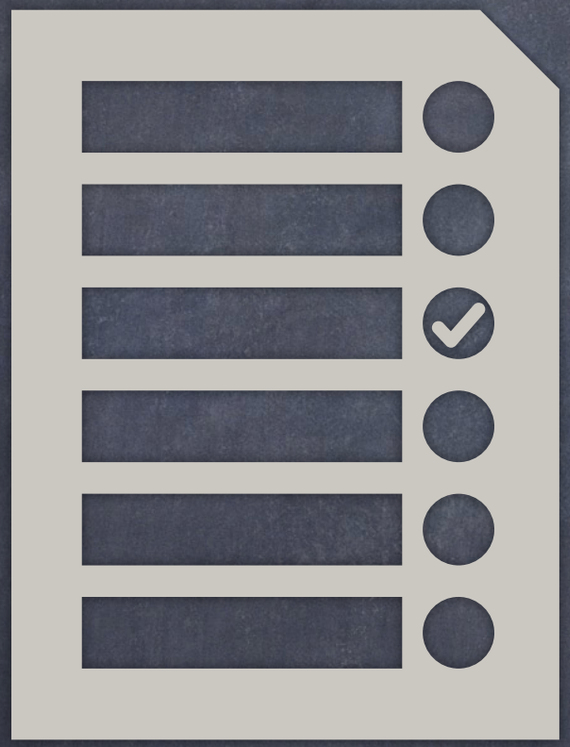
- Code Tailored Inputs
- Corpus Collection
- Coverage/Mutation
- Guided Exploration
- Deeper Bugs



- Slither-Prop Powered
- Source Code Integration
- Multiple UI
- Testcase Minimization
- Workflow Integration

#47

Echidna Usage



Executing Test Runner
Contract + Invariants

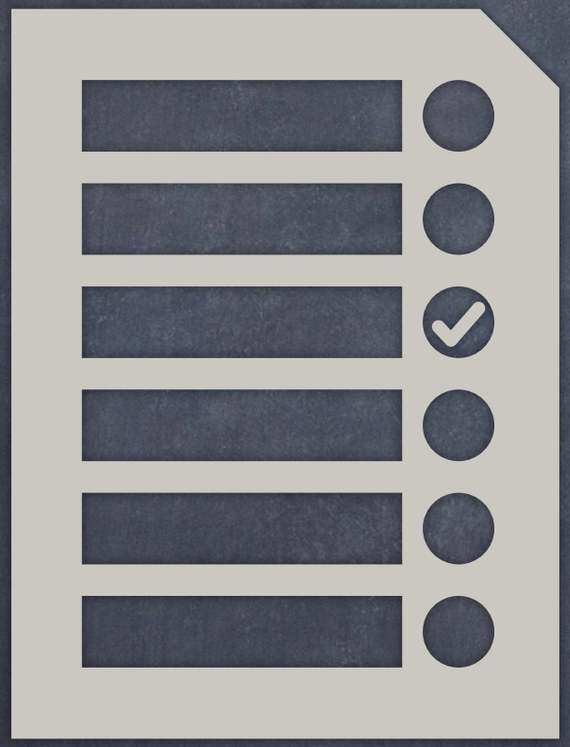
Invariant + Random Calls
-> Counterexamples

Invariant Writing

Collecting/Visualizing
Coverage

#48

Eth Security Toolbox



Tools Package
Trail of Bits

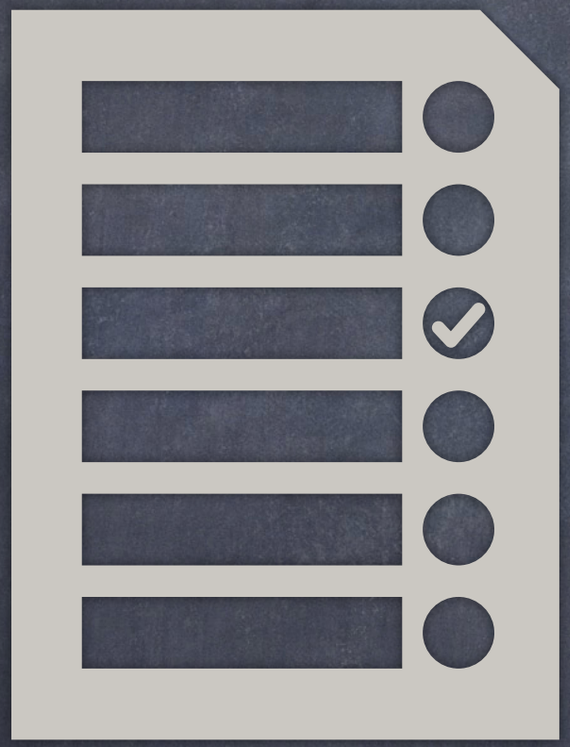
Docker Container

Preinstalled +
Preconfigured

Slither, Echidna,
Manticore, Rattle, Ethno

#49

Ethersplay



Binary Ninja plugin
Trail of Bits

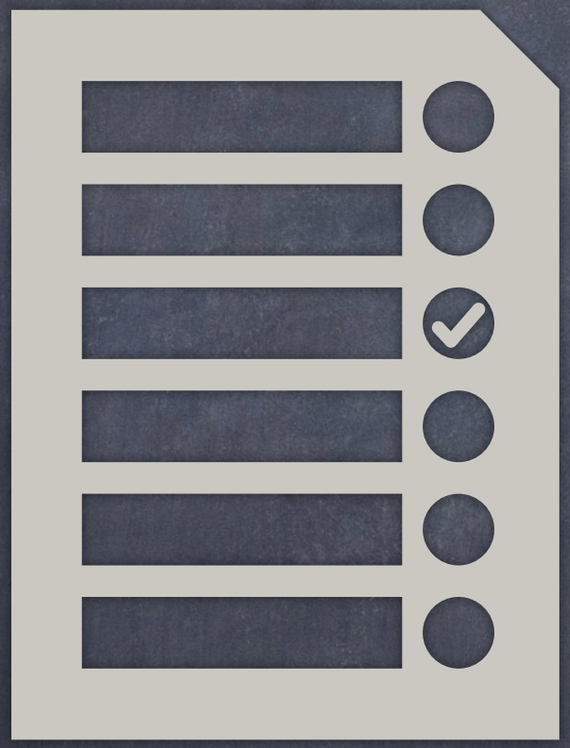
Input: EVM Bytecode

Displays Control Flow Graphs

Displays Manticore Coverage

#50

Pyevmasm



Security Tool
Trail of Bits

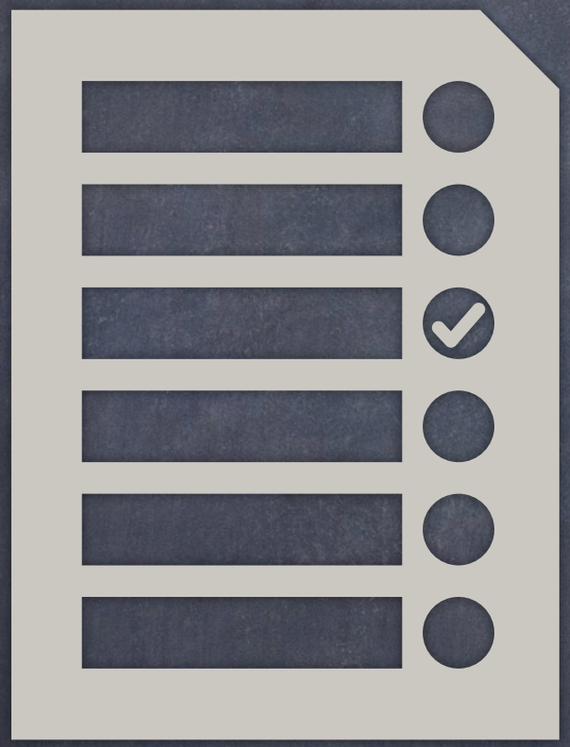
EVM Assembler &
Disassembler

Command-line Utility

Python API

#51

Rattle



Security Tool
Trail of Bits

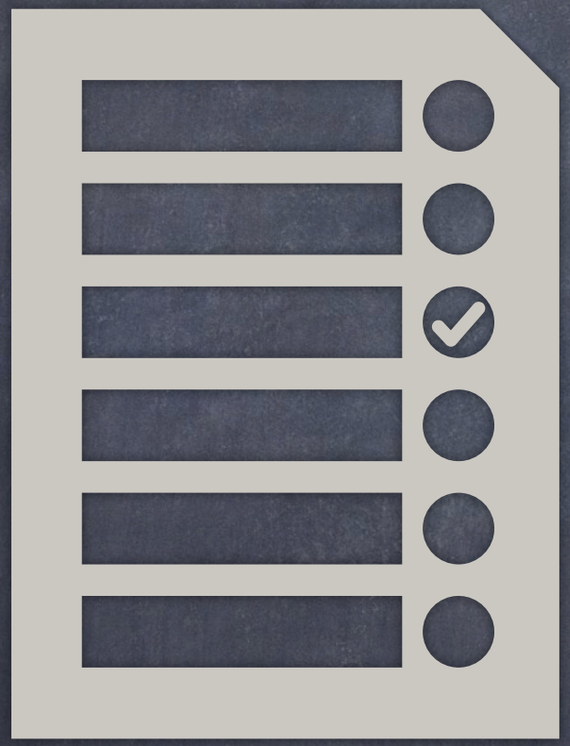
EVM Binary Static Analysis Framework

EVM Byte Strings, Flow-sensitive Analysis

Stack -> SSA Register
More Readable Code

#52

EVM CFG Builder



Security Tool
Trail of Bits

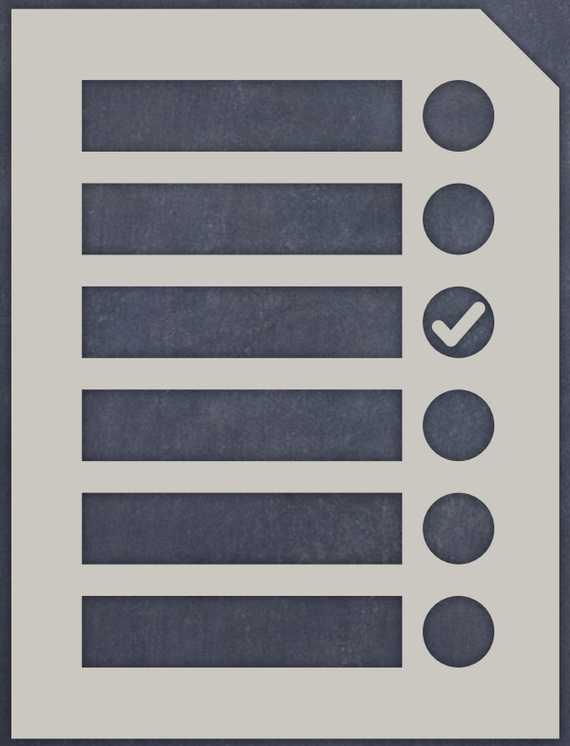
EVM Bytecode -> Extract CFG

CFG, Function Names, Attributes -> DOT File

Used by Ethersplay, Manticore & Other Tools

#53

Crytic
Compile



Security Tool
Trail of Bits

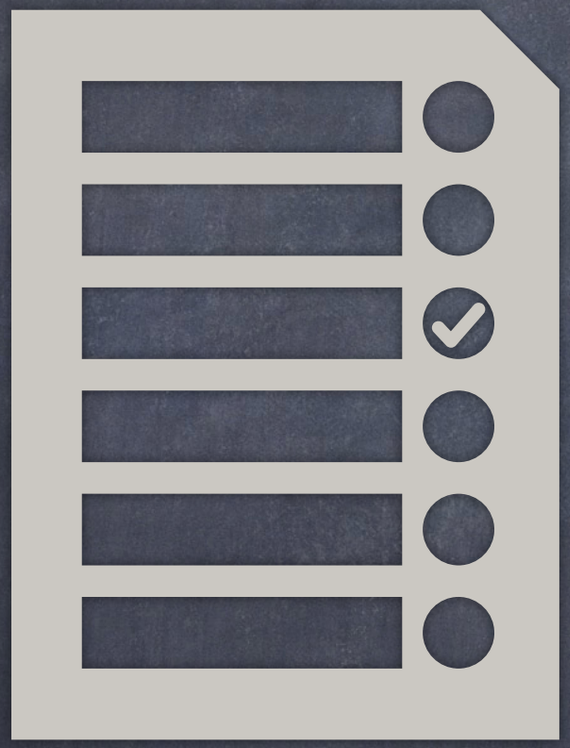
Smart Contract
Compilation Library

Solc, Truffle, Embark,
Etherscan, Brownie etc.

Slither, Echidna, Manticore
etc.

#54

Solc-Select



Security Helper Tool
Trail of Bits

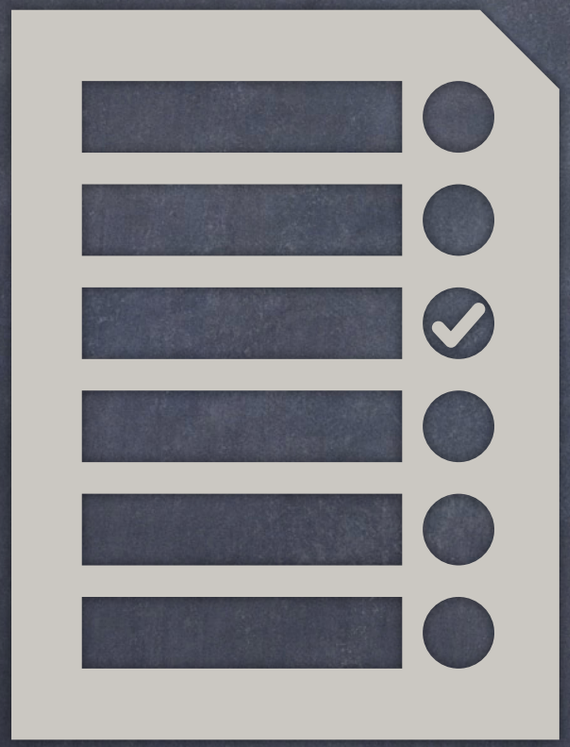
Switch -> Solidity
Compiler Versions

Install/Switch + Wrapper

Official solc Binaries

#55

Etheno



Testing Tool
Trail of Bits

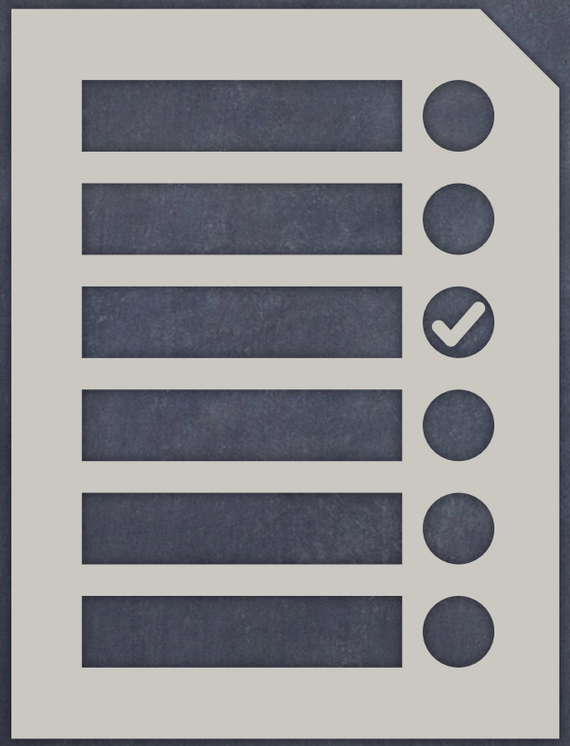
JSON RPC multiplexer: Diff Tests, Multiple Clients

Analysis Tool Wrapper: Manticore, Echidna

Test Frameworks: Ganache, Truffle

#56

MythX



Security Service
ConsenSys Diligence

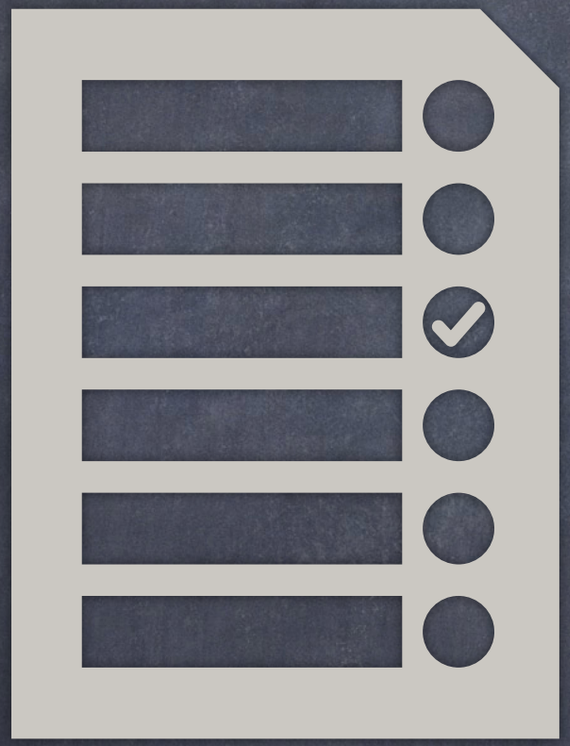
Paid API-based Service

Maru + Mythril + Harvey

46+ Detectors

#57

MythX Process



API-Based

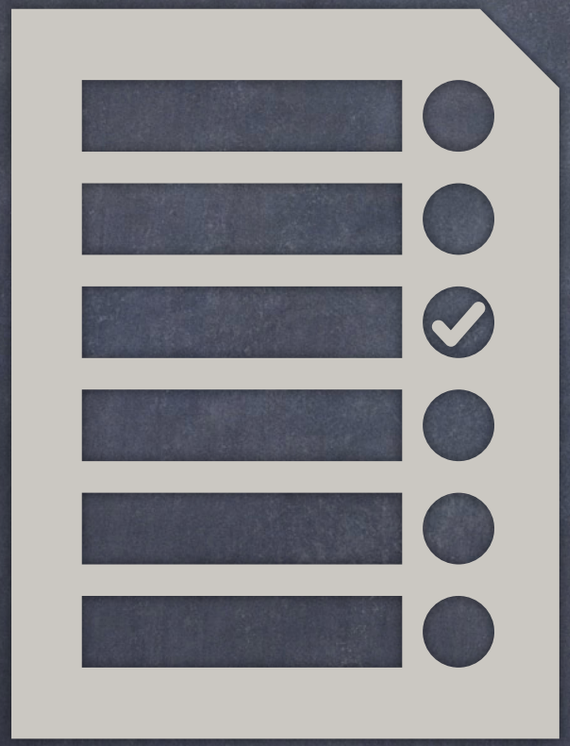
Submit Code

Run Analyses

Receive Report

#58

MythX Tools



Static Analysis -> Maru

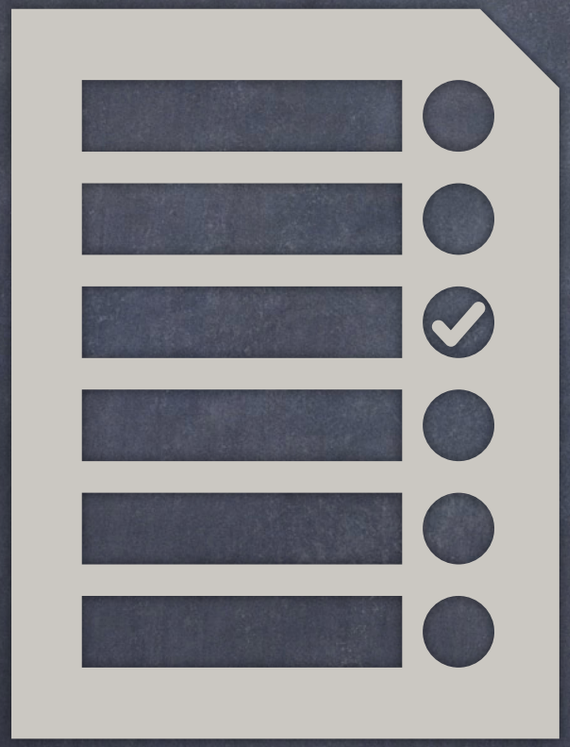
Symbolic Analysis -> Mythril

Greybox Fuzzing -> Harvey

Combination -> Comprehensive Analysis

#59

MythX Coverage



SWC Registry

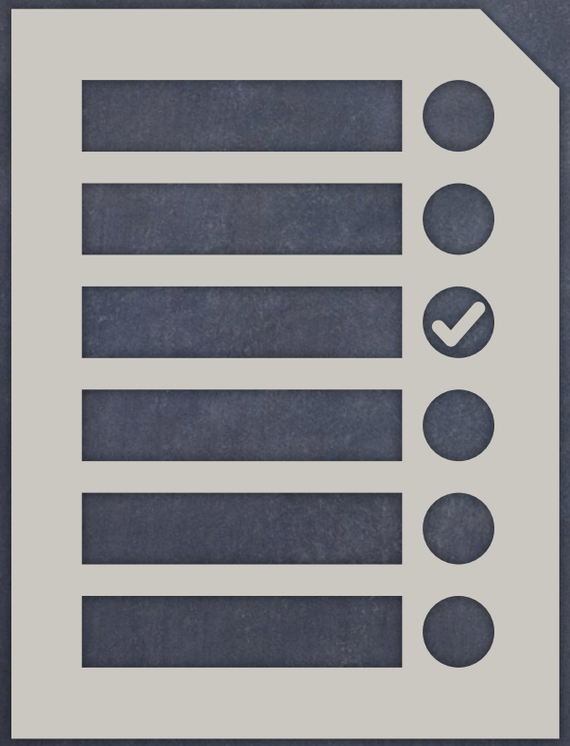
Smart Contract Weakness Classification

46+ Detectors

Comprehensive Coverage

#60

MythX SaaS



SaaS -> Security-as-a-Service

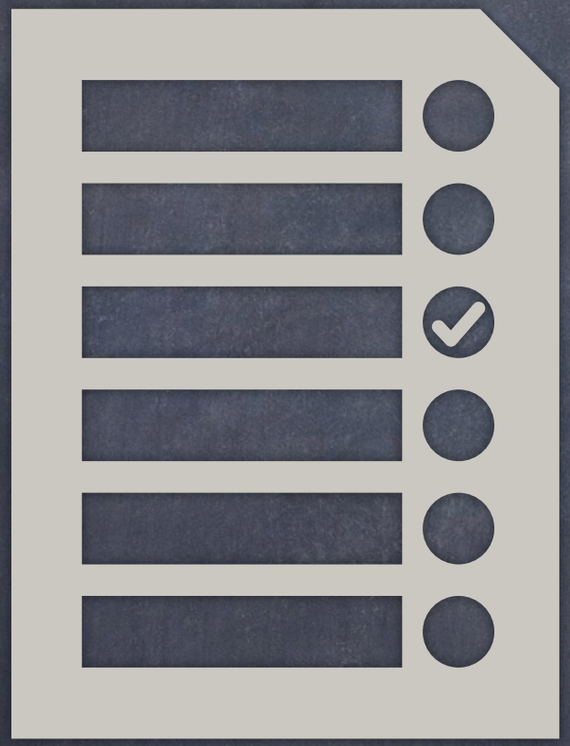
Cloud vs Local -> Better Performance

Three Tools -> Better Coverage

Continuos Upgrades

#61

MythX Privacy



Contract Code -> SaaS APIs

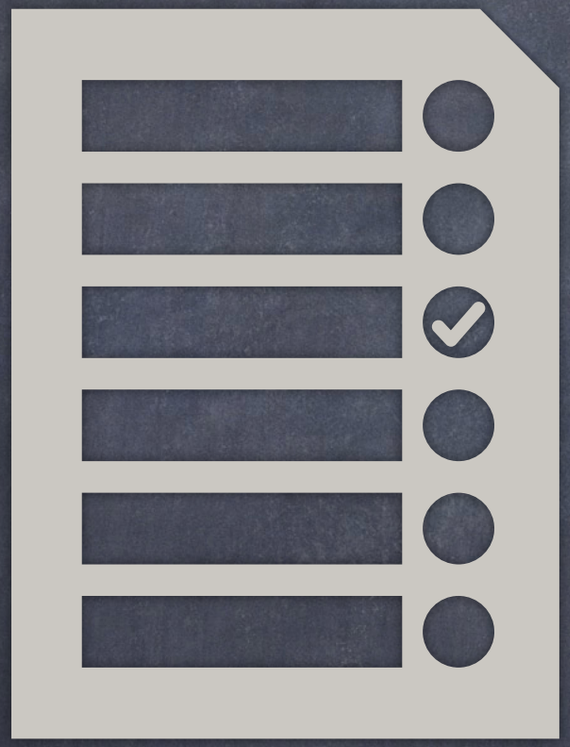
TLS Encryption

Code -> Secure Server Not Shared w/ Others

Results -> Authorized Access

#62

MythX Performance



Configurable Scans

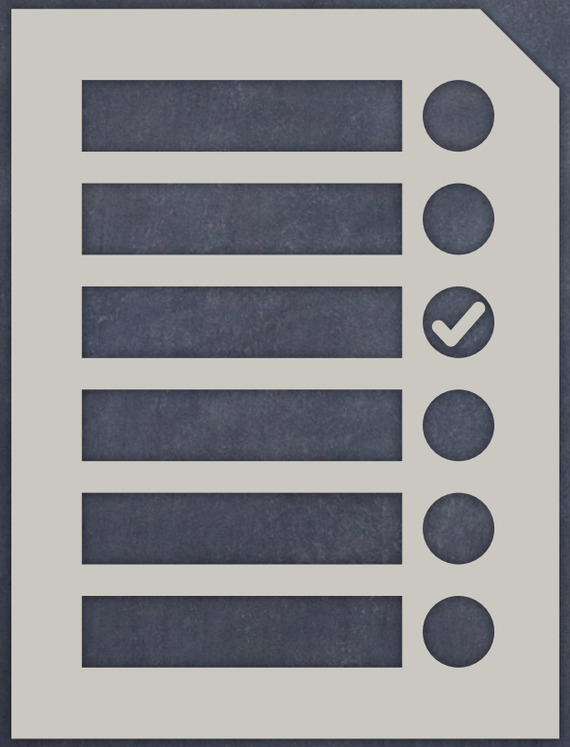
Quick: 5 mins

Standard: 30 mins

Deep: 90 mins

#63

MythX Versions



CLI: Unified Tool

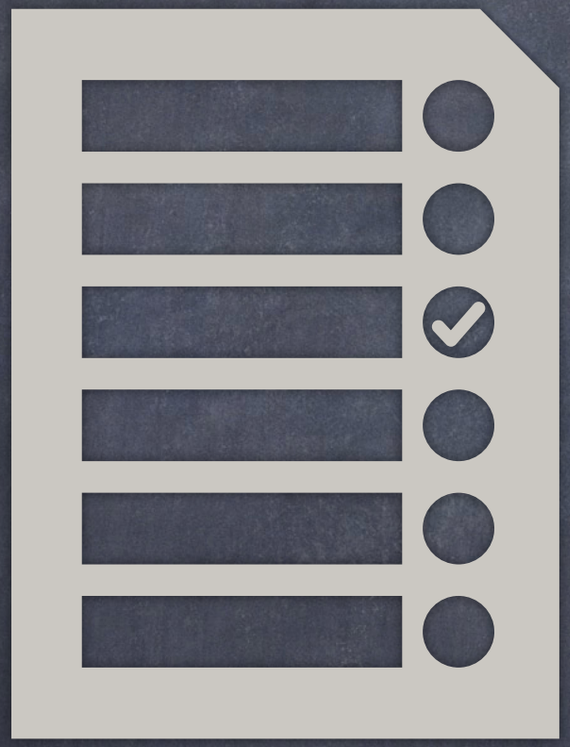
Library: JS/TS Integrations

PythX: Python Library

VSCode: Extension to scan/view

#64

MythX Pricing



On-Demand: USD 9.99 for 3 scans

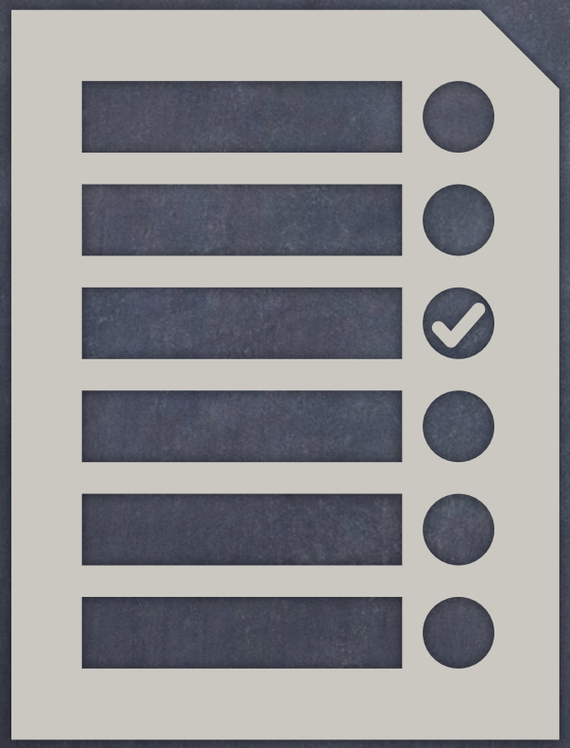
Developer: USD 49/month for 500 scans

Professional: USD 249/ month for 10,000 scans

Enterprise: Custom pricing

#65

Scribble



Verification Tool
ConsenSys Diligence

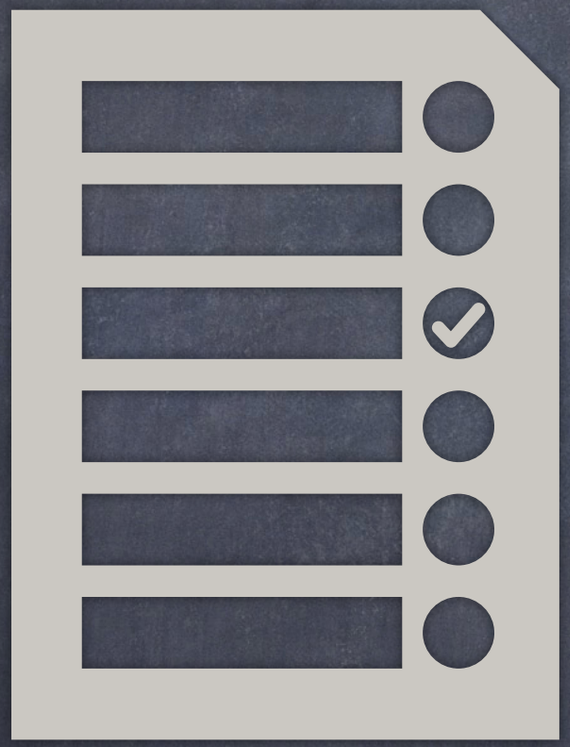
Scribble Language
Annotations -> Assertions

Instrumented+Equivalent
Contracts

Run Harvey/Mythril/MythX

#66

Fuzzing-as-a-Service



Fuzzing Service
ConsenSys Diligence

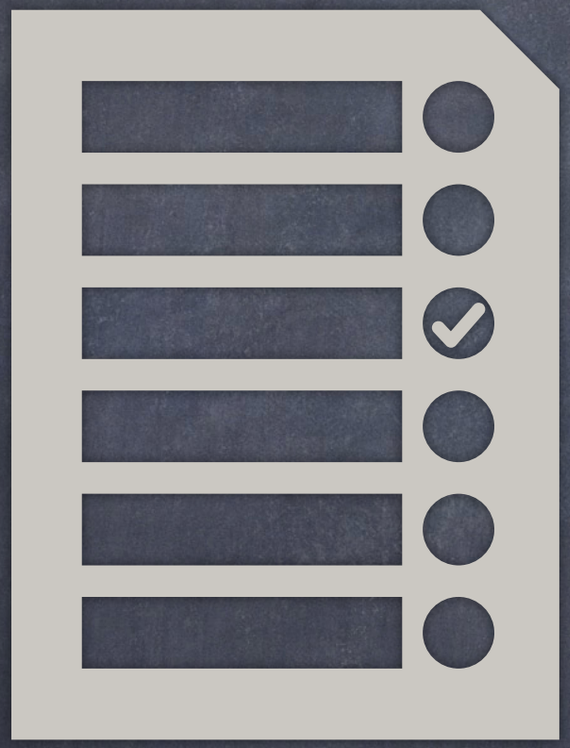
Specifications -> Scribble

Submit -> Fuzzing Campaigns -> Harvey

Receive/Fix -> Violations

#67

Karl



Security Tool
ConsenSys Diligence

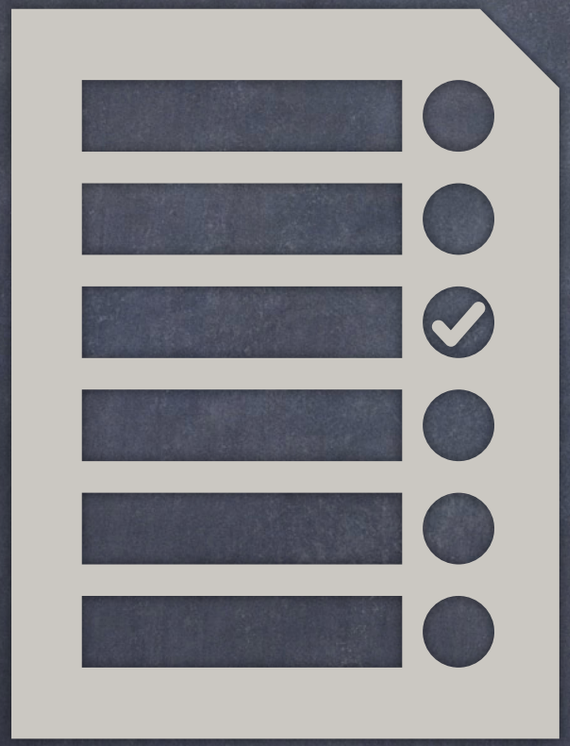
Monitor Ethereum
New Deployed Contracts

Run Mythril

Report Vulnerabilities in
Real-time

#68

Theo



Security Tool
ConsenSys Diligence

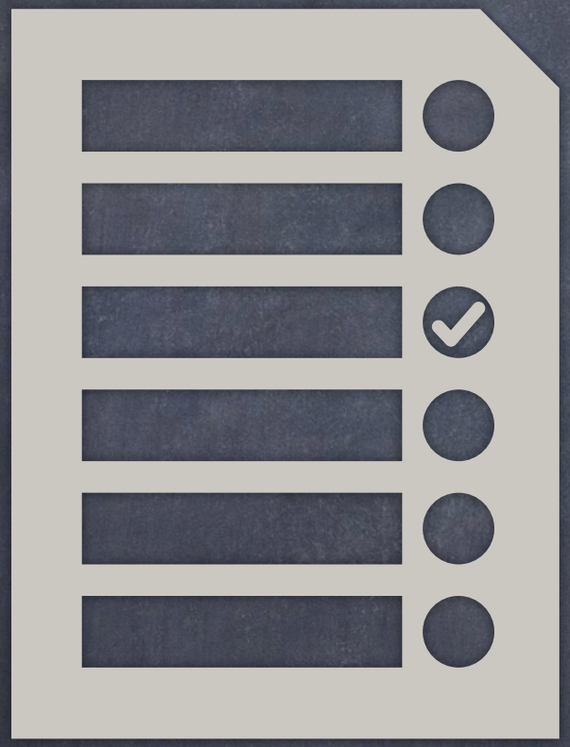
Exploitation Tool

Metasploit-like Interface
-> Python REPL

Reconnaissance -> Exploit
-> Front/Back run

#69

Visual Auditor



Visual Studio Extension
ConsenSys Diligence

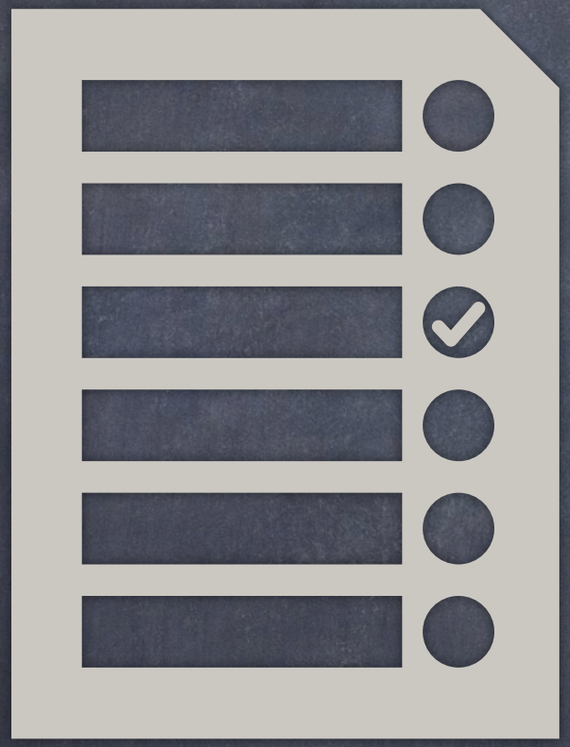
Security-aware Syntax/
Semantics Highlighting

Code Review/Reporting/
Augmentation

Solidity & Vyper

#70

Surya



Visualization Tool
ConsenSys Diligence

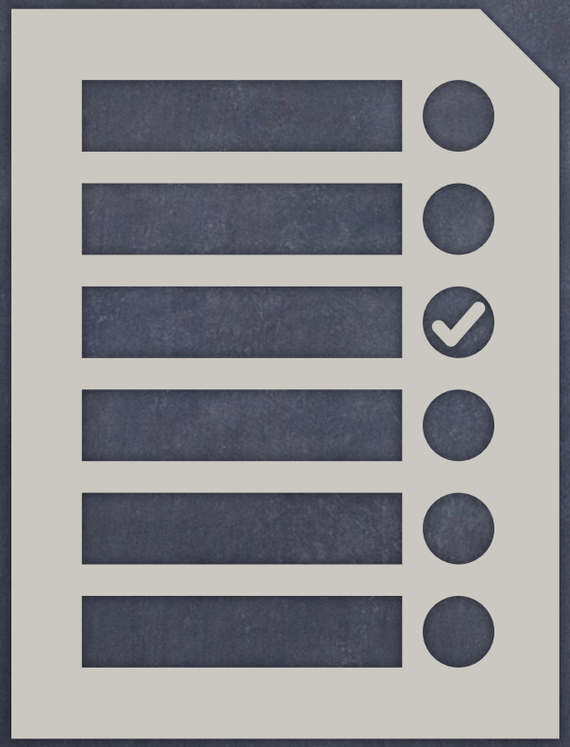
Call Graph
Inheritance Graph

Integrated w/ Visual Auditor

Commands: graph/ftrace/ flatten/describe etc.

#71

SWC Registry



Smart Contract Weakness Classification

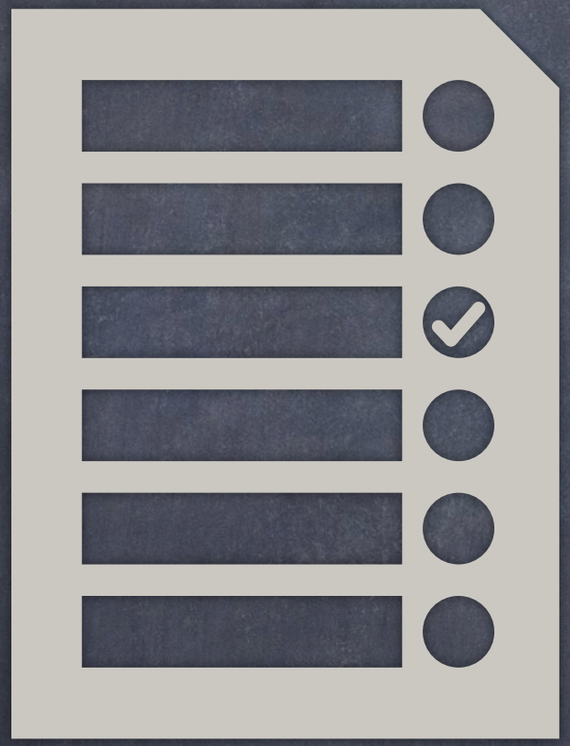
Aligned to Web2 CWE Structure & Terminology

Goal: Common Language, Classification

Goal: Compare & Improve Tools

#72

Securify



Security Scanner
ChainSecurity

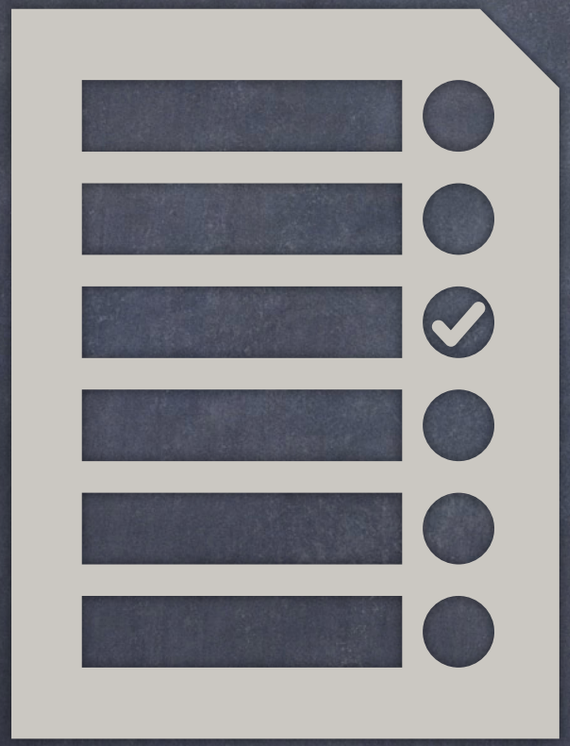
Static Analysis

Written in Datalog

38+ Detectors

#73

VerX



Verification Tool
Temporal Safety Properties

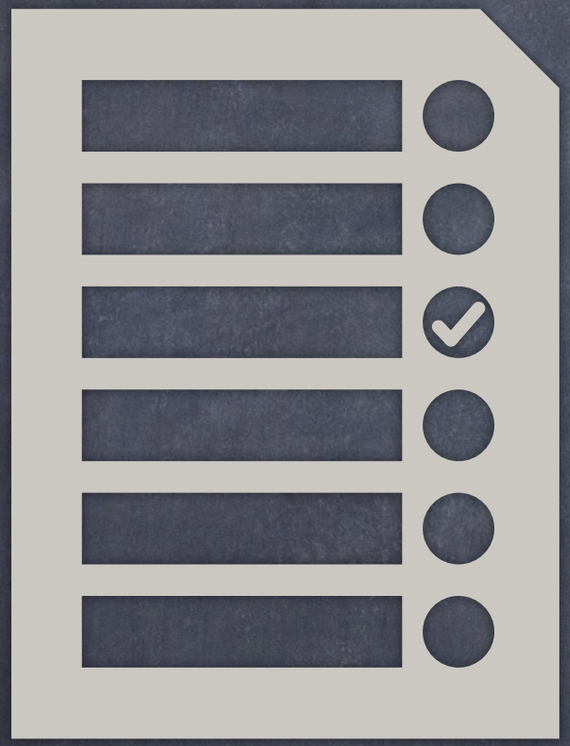
Reduction: Temporal
Safety -> Reachability

Efficient Symbolic
Checking Engine

Delayed Abstraction

#74

SmartCheck



Security Tool
SmartDec

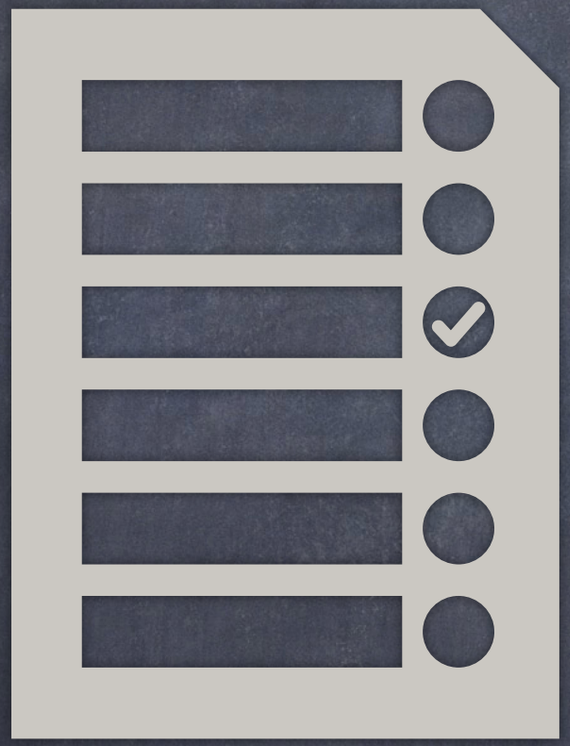
Extensible Static Analyzer

XML-based IR

XPath Pattern Checking

#75

K-Framework



Verification Framework
Runtime Verification

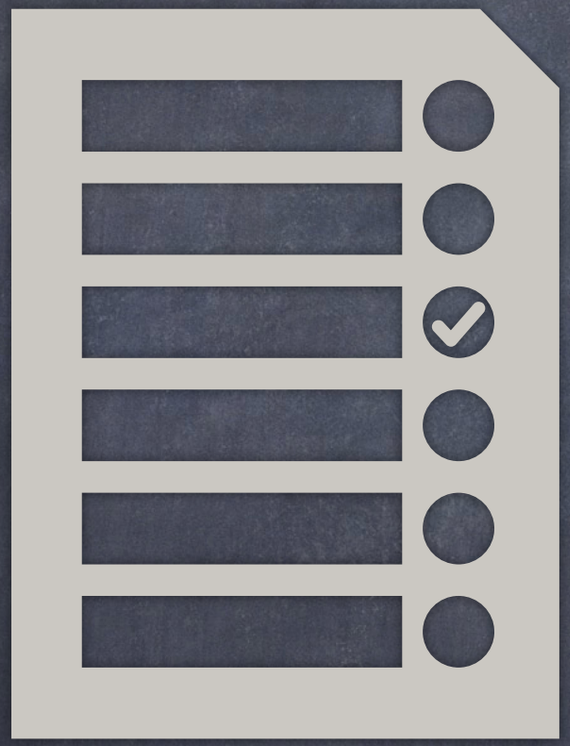
KEVM: Model of EVM in K-Framework

First Executable EVM Specification

Framework for Building Tools

#76

Certora Prover



Formal Verification
Certora

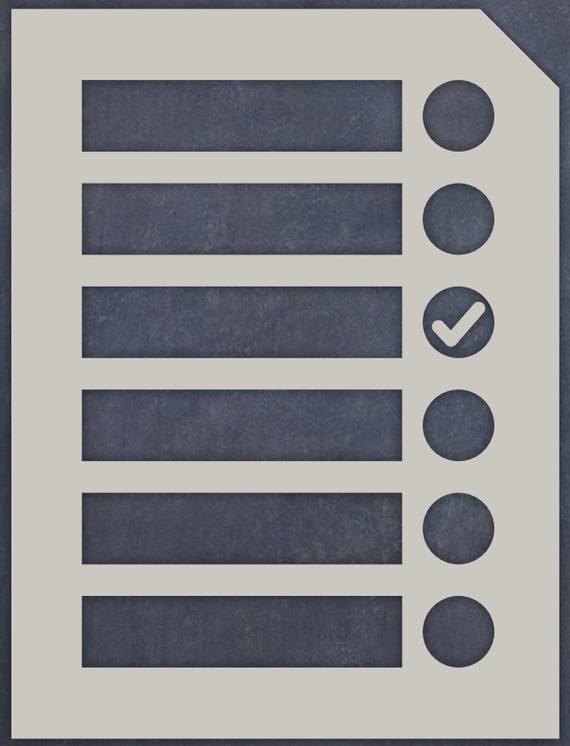
Rules: Specify Language
& Symbolic Checking

Prover: All Paths/Inputs
Counterexample

Abstract Interpretation
Constraint Solving

#77

HEVM



EVM Implementation
DappHub

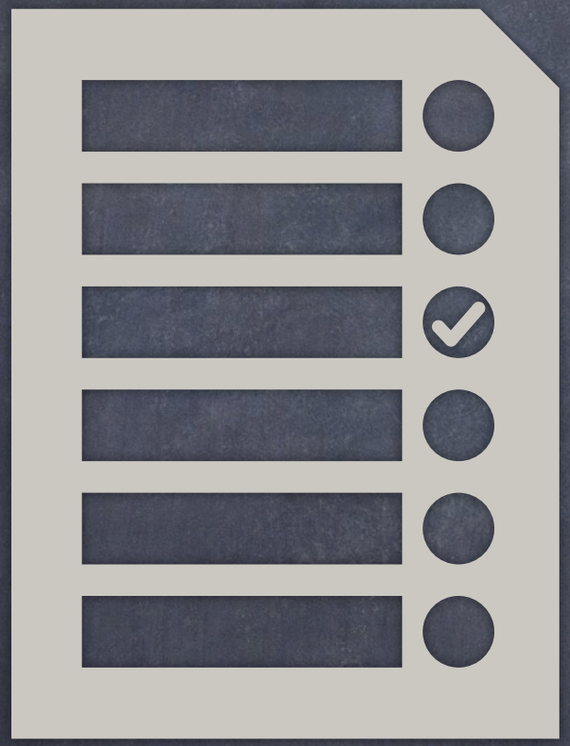
EVM -> Testing &
Debugging

Tests: Unit/Property

Interactive Debugging

#78

CTFs



Capture The Flags
Fun/Edu Challenges

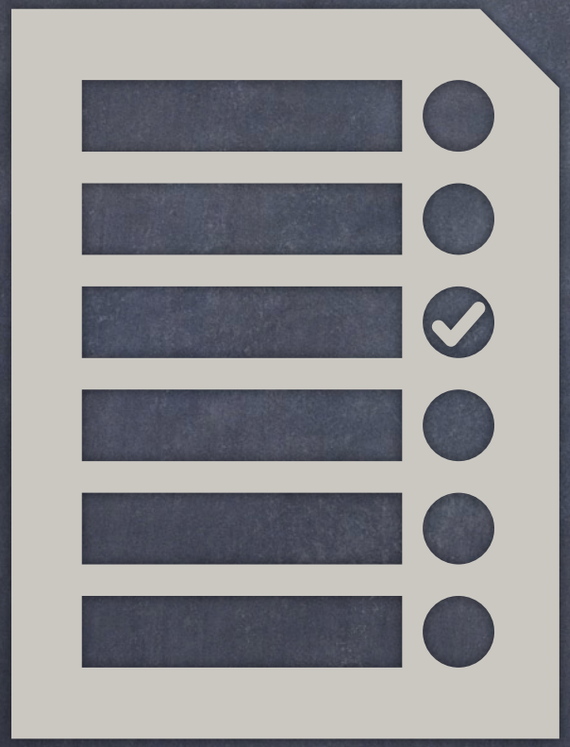
Hack Dummy Contracts
w/ Vulnerabilities

Capture The Ether
Ethernaut

Damn Vulnerable DeFi
Paradigm CTF

#79

Security Tools



Assist Humans
Automate Tasks

Fast, Cheap, Scalable, Deterministic

Common Pitfalls & Best Practices

E.g.: Slither, MythX

#80

Process

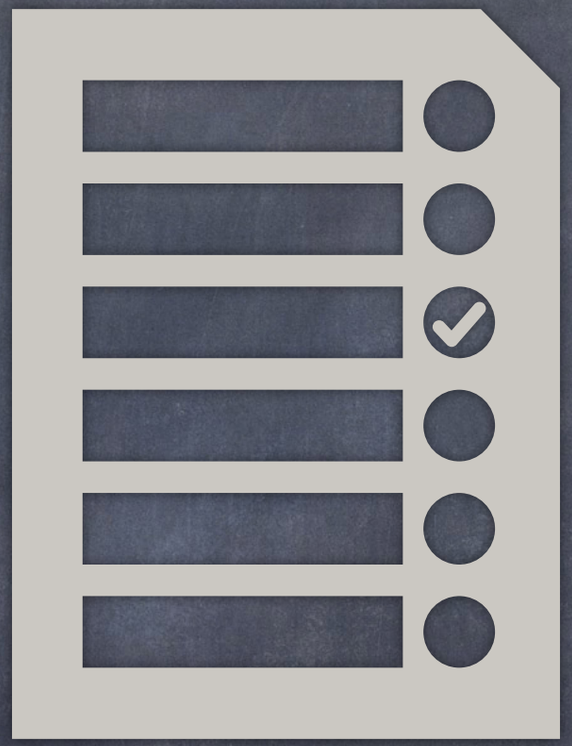
Read Spec/Docs

Fast Tools

Manual Analysis

Slow/Deep Tools

Discuss Findings



Convey Status

Iterate

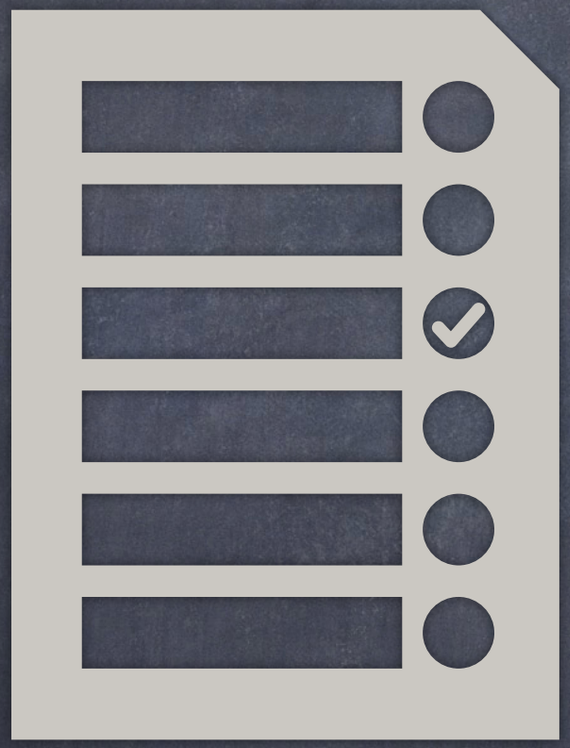
Write Report

Deliver Report

Evaluate Fixes

#81

Read
Spec/Docs



Requirements/Design/
Architecture

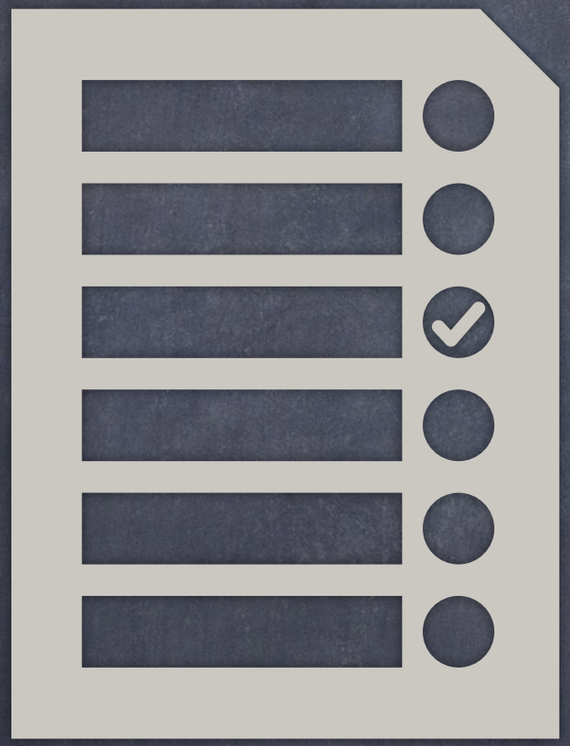
Specification vs
Documentation

Absence -> Inference
Wasted Time/Effort

Assets & Actors & Actions

#82

Fast Tools



Linters, Static Analyzers
Run in Seconds

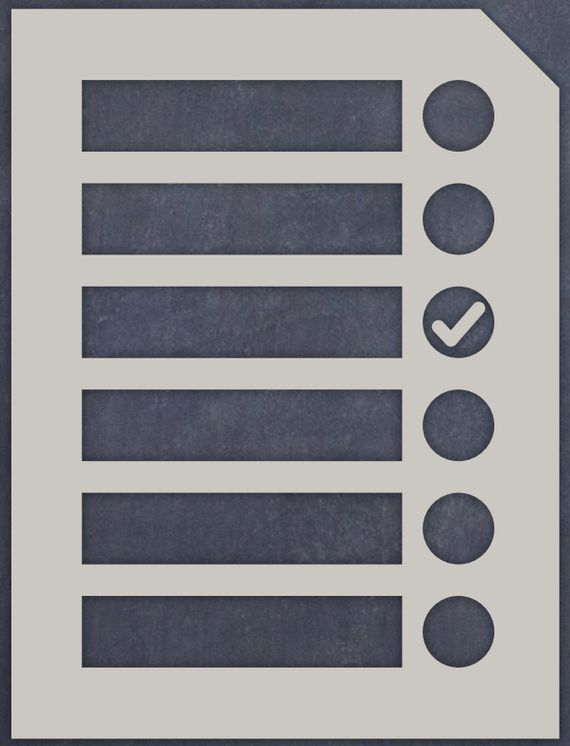
Common Pitfalls
Best Practices

Control/Data Flow
False Positives/Negatives

E.g.: Slither, Maru

#83

Manual Analysis



Missed Flagging Vulnerabilities

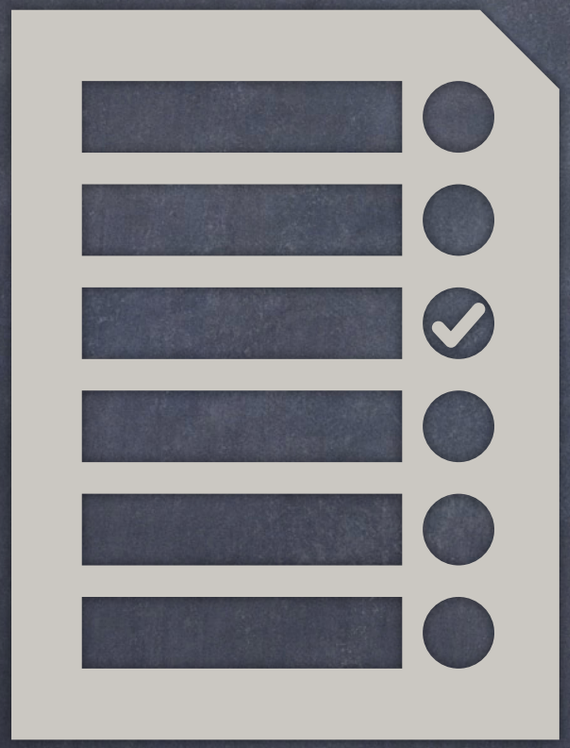
Business Logic & Application Constraints

Implementation vs Spec/Documentation

Infer Constraints

#84

Slow/Deep Tools



Fuzzing/Symbolic Checking/Verification

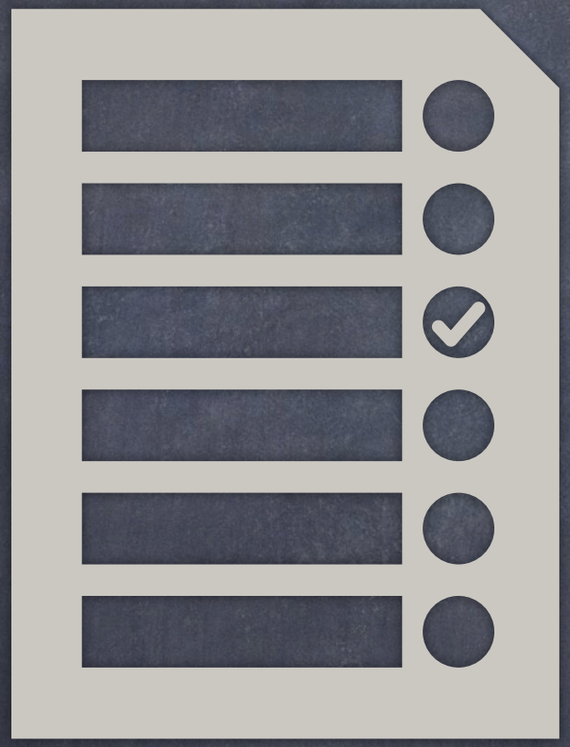
Custom Properties Run in Minutes

More Prep/Expertise Deeper Analyses

E.g.: Manticore, MythX, Echidna, Harvey, Scribble

#85

Discuss w/ Auditors



"Given enough eyeballs, all bugs are shallow"

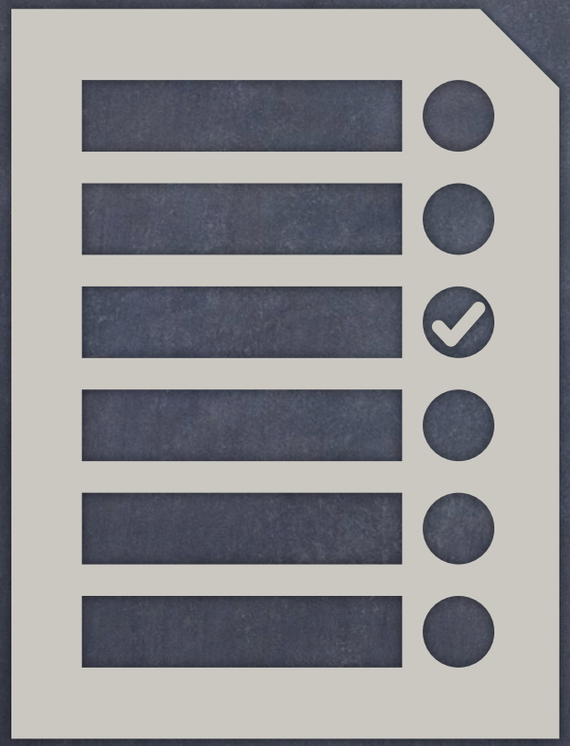
Independent vs Group

Bias & Effectiveness

Overhead vs Overlap

#86

Discuss w/ Project Team



Open Communication Channel

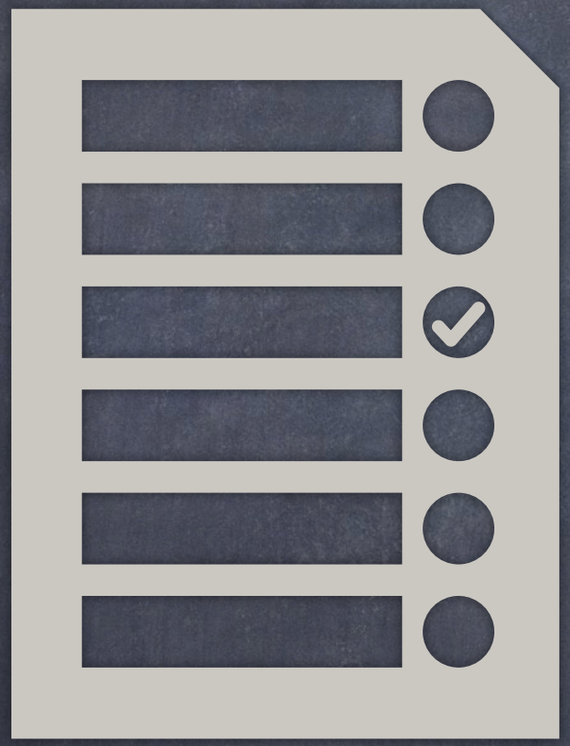
Clarify Assumptions

Discuss Findings/Impact/ Fixes

Update Status

#87

Write Report



Summary & Details

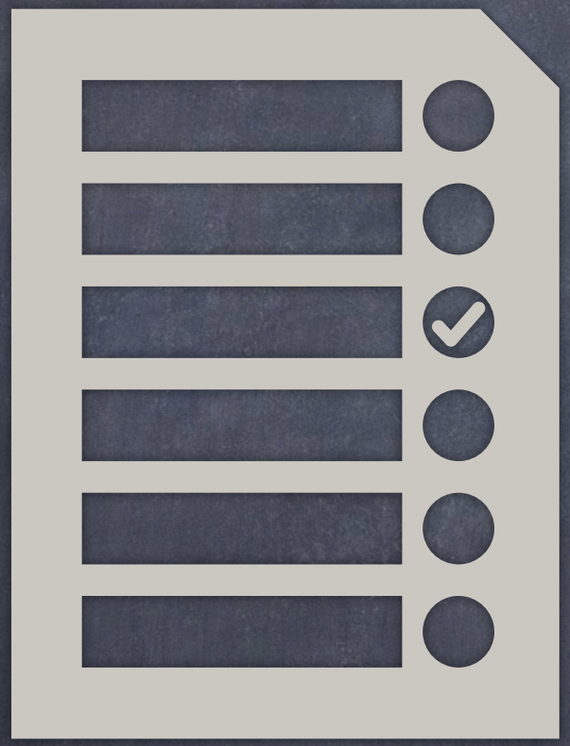
Findings: Severity, Scenarios, Suggestions

Quality: Coding, Conventions, Coverage

Articulate & Actionable

#88

Deliver Report



Publish & Present

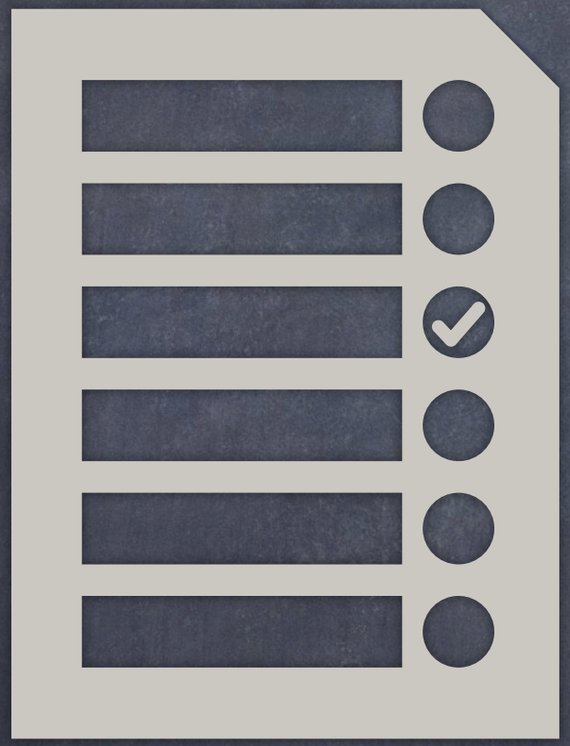
Agree on Findings/ Severity

Review & Respond

Private/Public

#89

Evaluate Fixes



Findings: Accept/ Acknowledge/Deny

Fixes: Recommend/Review

Evaluation: Time & Timeline

Ensure Security

#90

Manual Review

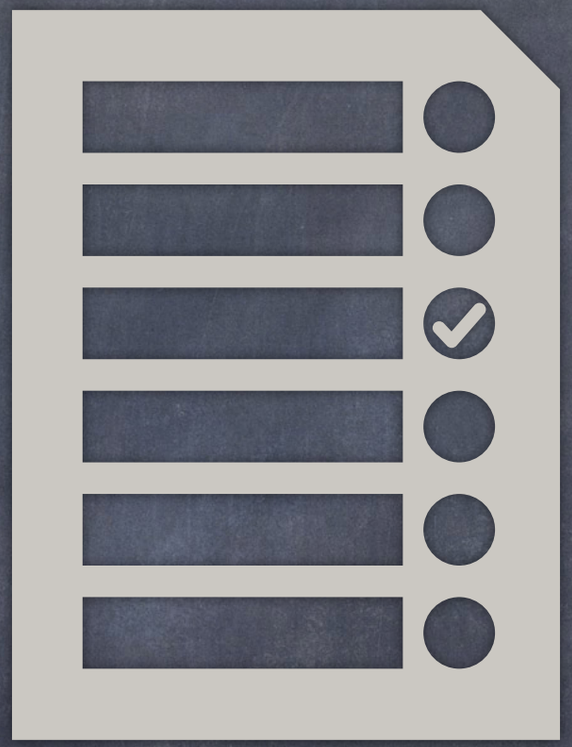
Different Approaches

Access Control

Asset Flow

Control Flow

Data Flow



Different Focus

Inferring Constraints

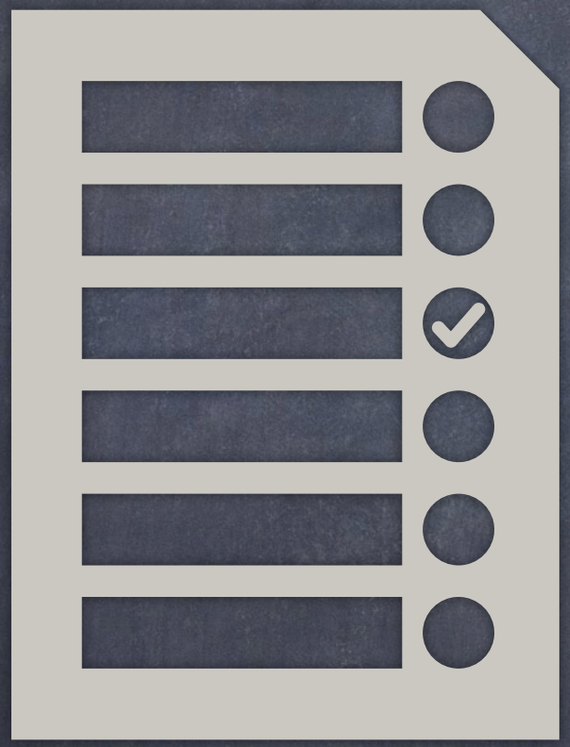
Dependencies

Assumptions

Checklists

#91

Access Control



Fundamental Security Primitive

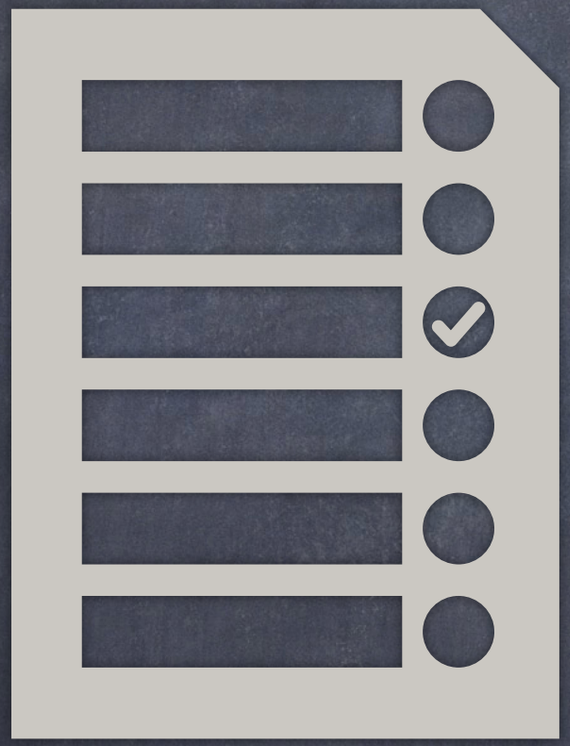
Who has access to What?
Actors -> Assets

Roles: Admins/Users
Visibility/Modifiers

Correct & Complete & Consistent

#92

Asset Flow



Assets: ETH or ERC20/ ERC721 tokens

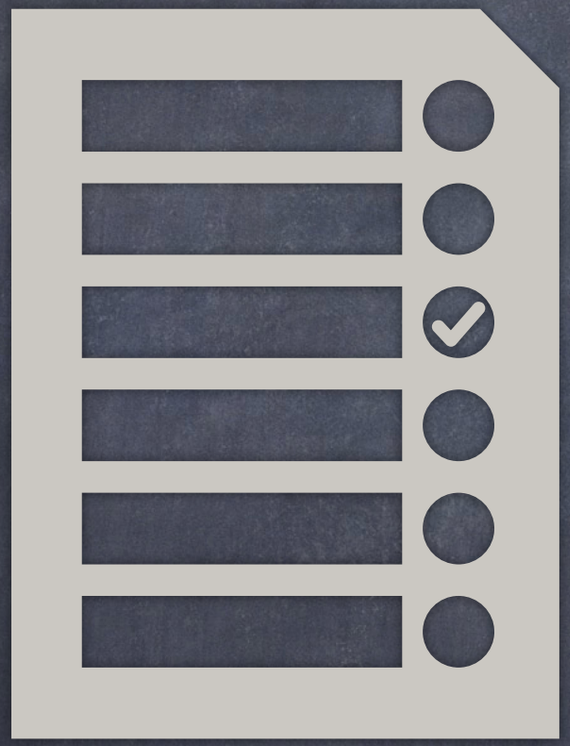
Who/When/Which

Why/Where

What Type/How Much

#93

Control Flow



Transfer of Control:
Execution Order

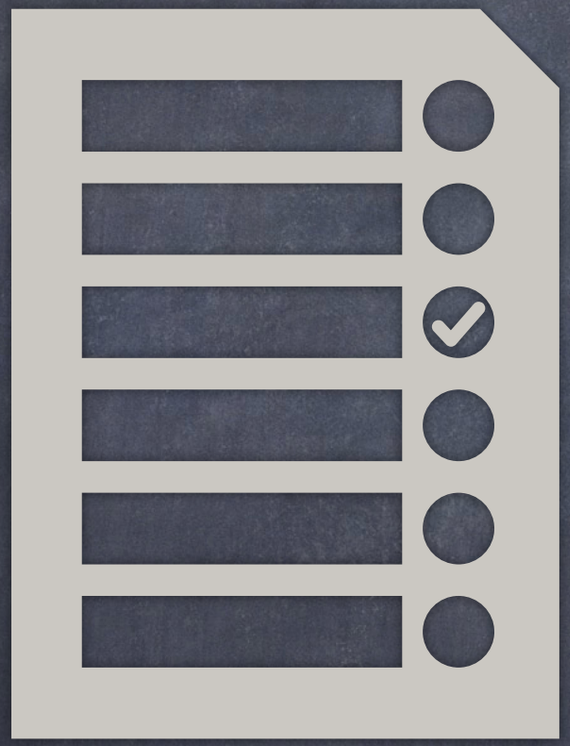
Intra/Inter Procedural

Conditionals & Loops

Control Flow Graph

#94

Data Flow



Transfer of Data:
Execution Context

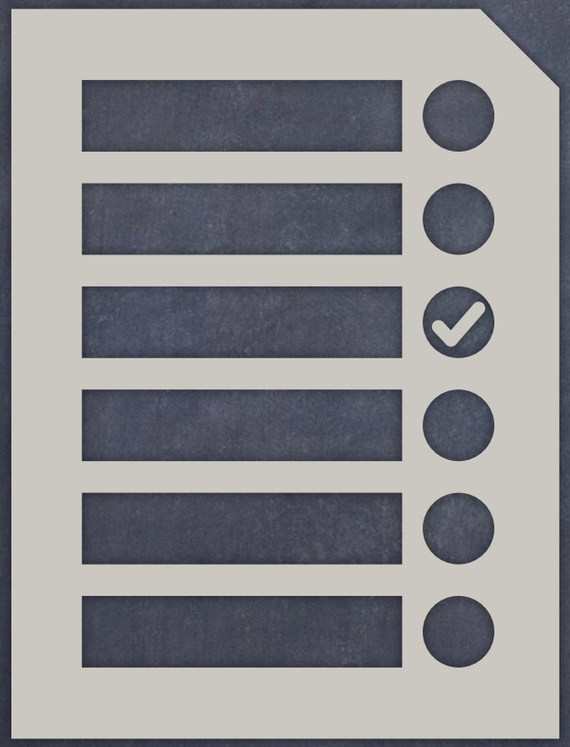
Variables & Constants

Function Arguments &
Return Values

Storage/Memory/Stack/
Calldata

#95

Inferring Constraints



Program Constraints -> Rules/Properties

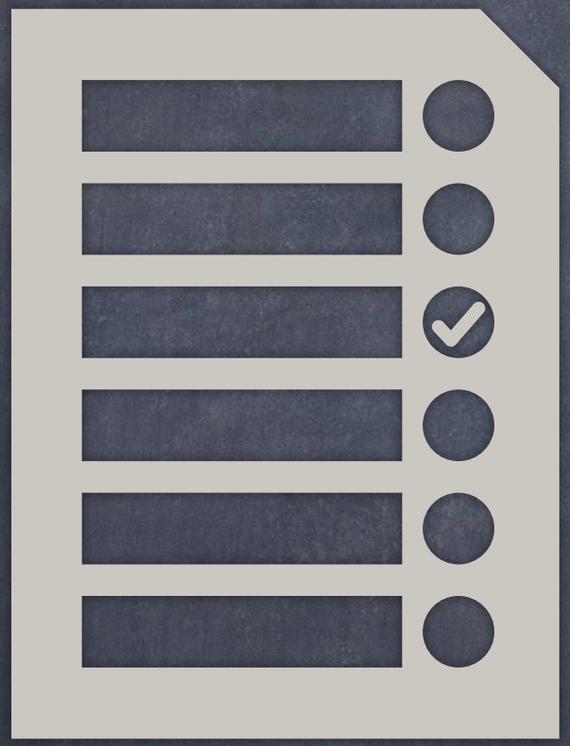
Solidity/EVM vs Application Constraints

Lack of Spec/ Documentation

Maximal Occurrence -> Inference

#96

Dependencies



External Code/Data

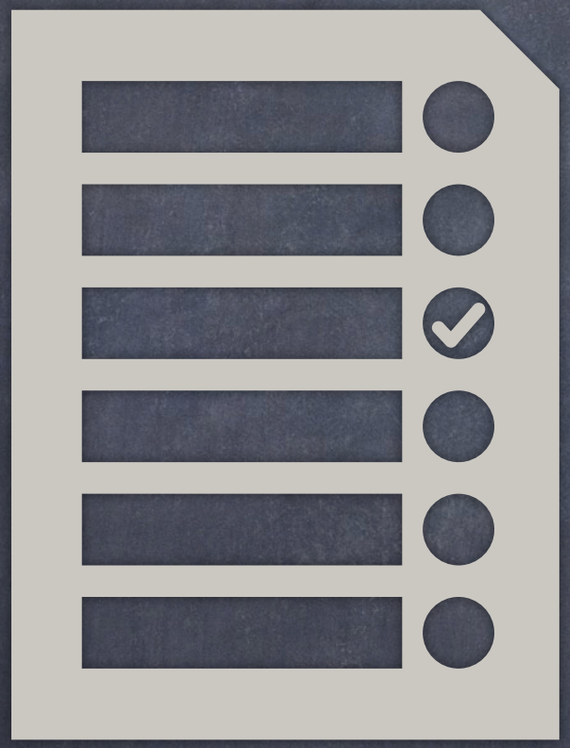
Libraries/Protocols/
Oracles

Composability

Assumptions on
Functionality/Correctness

#97

Assumptions



Incorrect Assumptions

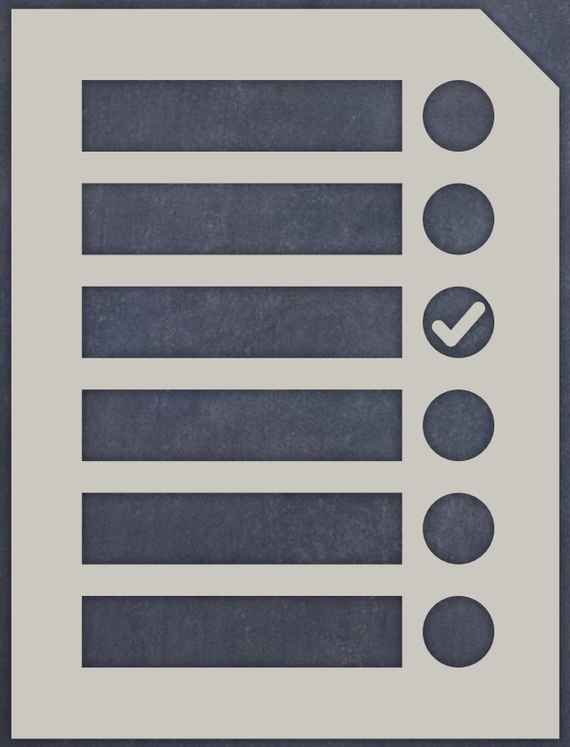
Who/What/When/Why etc.

Verify Assumptions

E.g.: Admins, Input Validation, Return Values

#98

Checklists



Itemized Lists

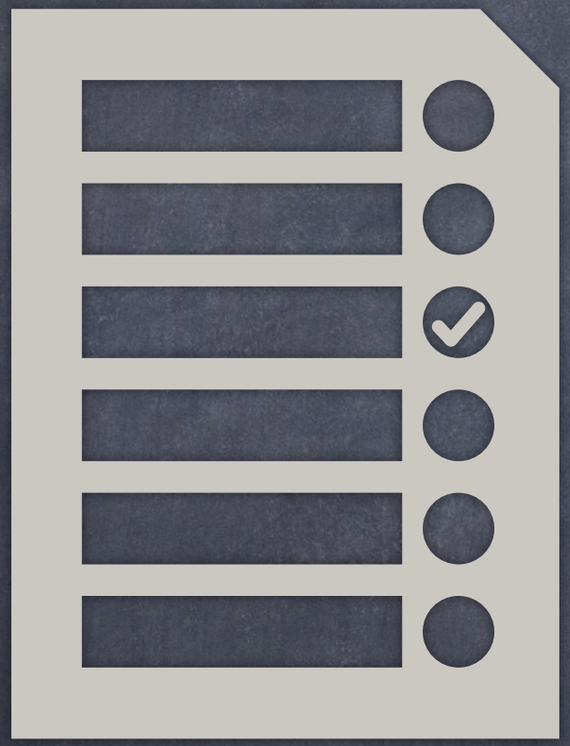
Retention & Recall

Pitfalls & Best Practices

No Missed Checks

#99

Exploit Scenarios



Proof-of-Concept

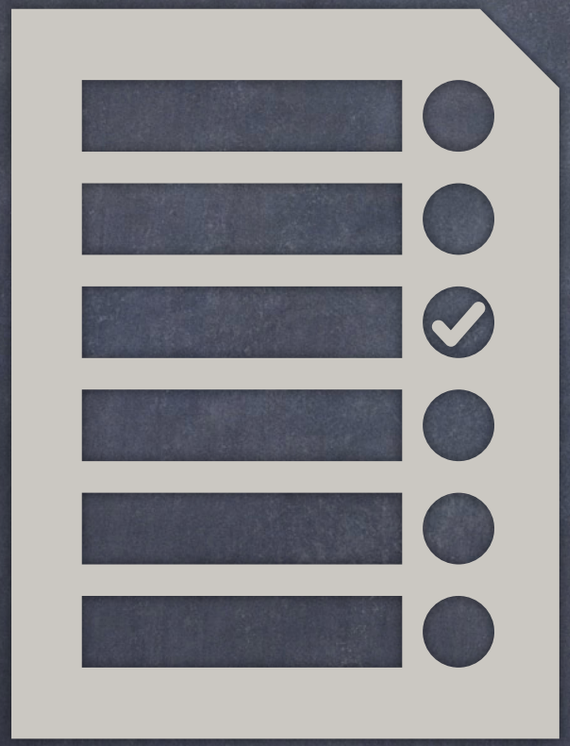
Written Descriptions/Code

Reasonable & Responsible

Realistic & Relatable

#100

Likelihood & Impact



Likelihood: Probability & Difficulty

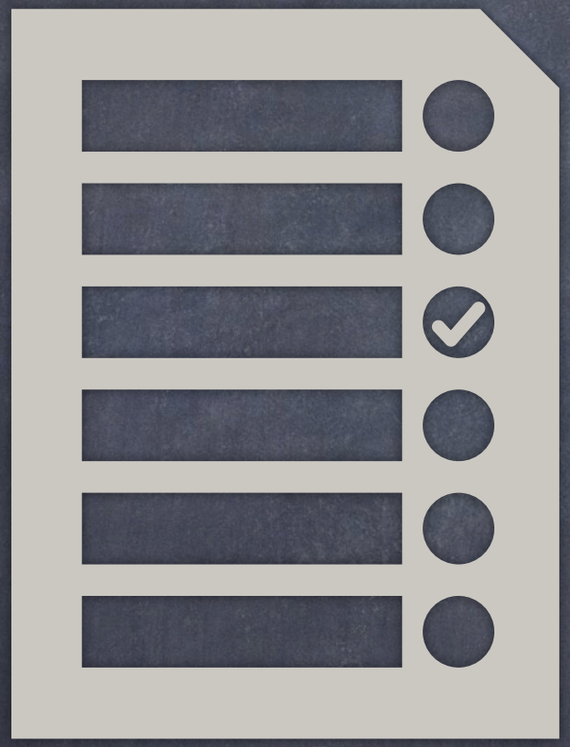
Impact: Magnitude of Implications

Severity = Likelihood + Impact

Access & Assumptions
Funds vs Functioning

#101

Audits
Summary



Bounded Effort
Time|Resources|Expertise

Automated & Manual

Findings: Difficulty/
Impact/Severity

Shows Presence
Not Absence