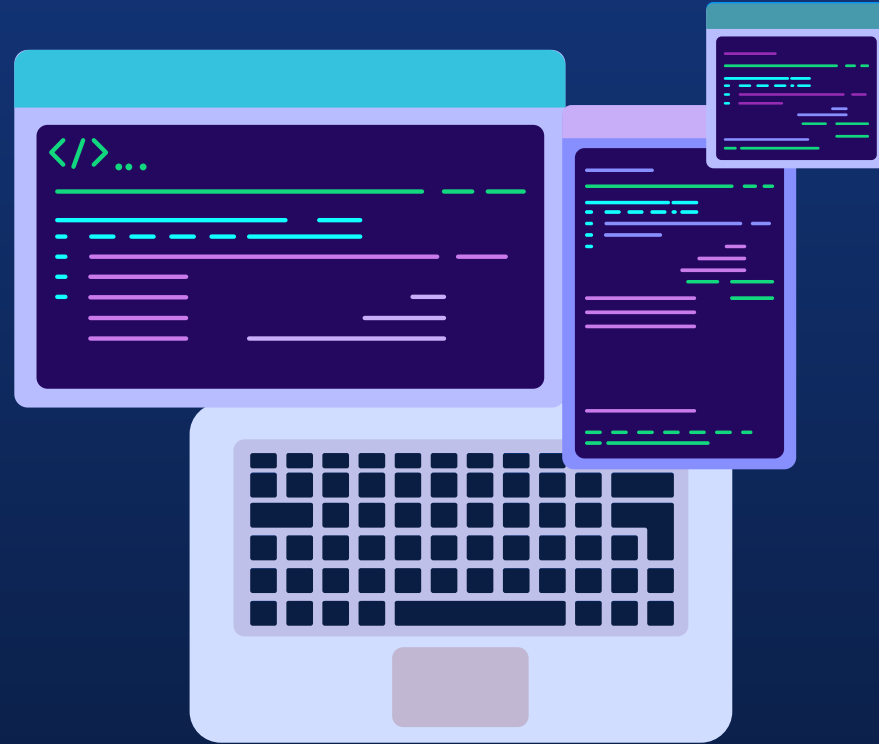


A test suite for smart contract vulnerability analysers

Susan Ștefan Claudiu
Arusoaie Andrei
23.03.2023





Overview

- Develop a smart contract **test suite** that can be used as a **benchmark**
- **Evaluate** analysis tools for smart contracts
- Part of my PhD thesis - apply analysis techniques to detect and mitigate vulnerabilities in smart contracts (supervisor: Dorel Lucanu, co-supervisor: Andrei Arusoaie)

Goals



Improve our knowledge


Gain in depth knowledge of vulnerabilities in smart contracts.

Create a benchmark

Using our test suite as a benchmark for analysis tools.

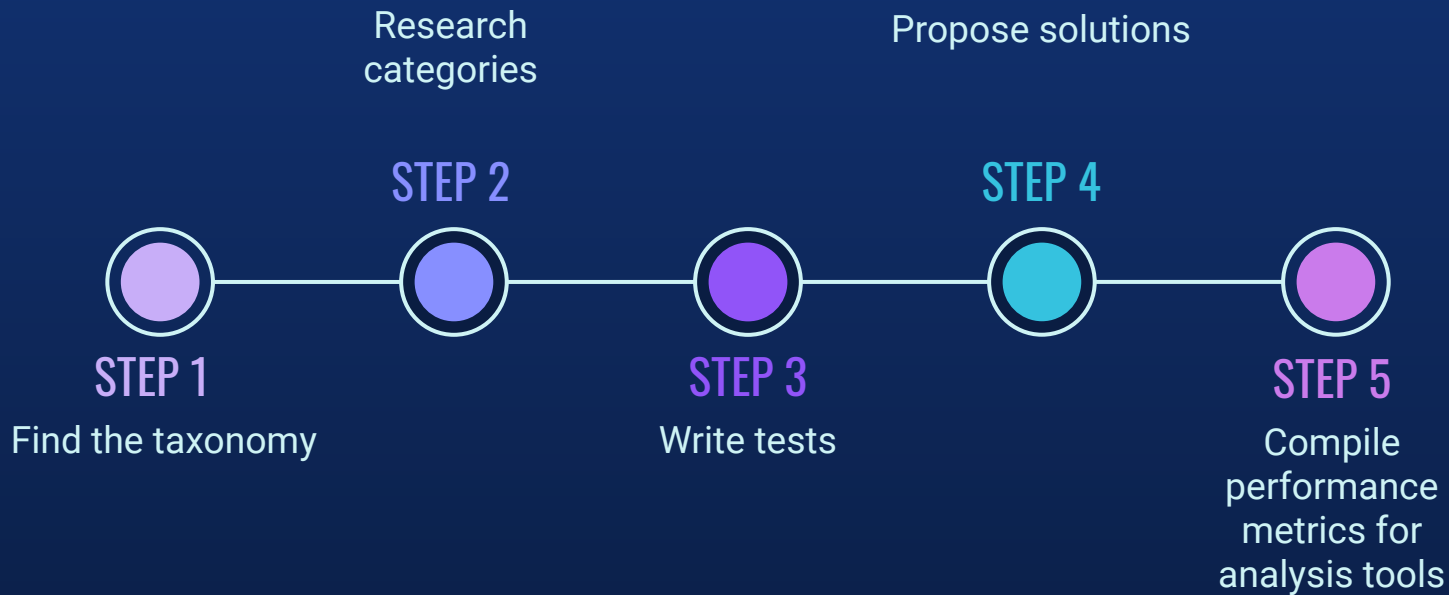
Gather useful information

Compare analysis tools/methods and find their limitations.





Test Suite Development



Test Variations



Positive Variation

Tests that feature the vulnerability. The analysis tools should report the desired issue.



Negative Variation

Tests that do NOT feature the vulnerability. The analysis tools should NOT report the desired issue.



Data about our test suite, so far

204* Contracts

And 47* different categories





Challenges

CHALLENGE 1

Deciding which taxonomy to use.

CHALLENGE 2

Researching and developing scenarios for each vulnerability.

CHALLENGE 3

Deciding which scenarios can be classified as vulnerabilities.

CHALLENGE 4

Deciding which vulnerabilities can be reasonably detected by a tool.



Preliminary comparisons of Static Analysis Tools

01

Slither

Version 0.9.1

02

Solhint

Version 3.3.8

03

Mythril

Version 0.23.13

04

Remix Static Analysis Plugin

Remix Version 1.3.6

05

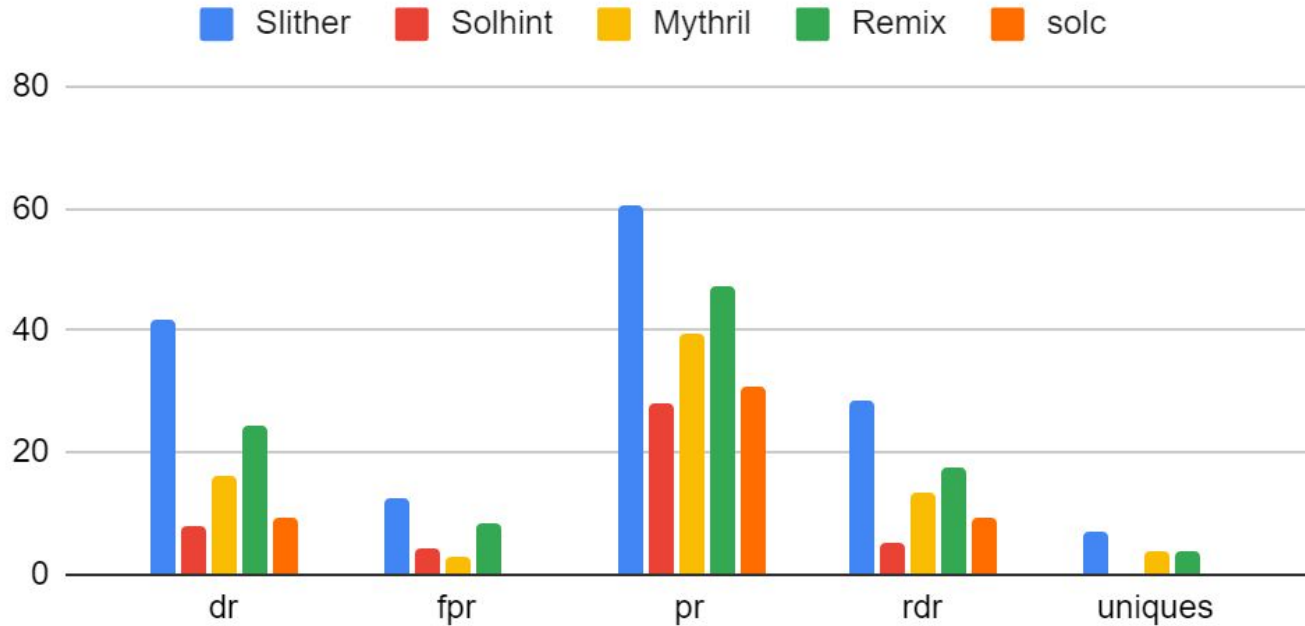
Solidity Compiler

Version 0.8.17



Comparison Results

dr, fpr, pr, rdr and uniques



Different rates computed for each analysis tool

Conclusions



The test suite

We already have a test suite which covers almost all documented vulnerabilities.



Preliminary results

We used the test suite to compute some performance metrics of various tools.



Future plans

The test suite, tools suite and metrics suite can only get bigger.