ITERATION - 1 PRESENTATION

Team 9

Abhishek Wadhwani – 10020352719
Mounika Kottapalli– 1002085510
Nitin Raj Thumma– 1002080555
Sai Raghu Rami Reddy Dontireddy – 1002014523

Table of Contents

Issue

Slither-read-storage: add support for Nested Structs #2077

- Enhancing Slither with nested struct support would enable broader Solidity contract security analysis.

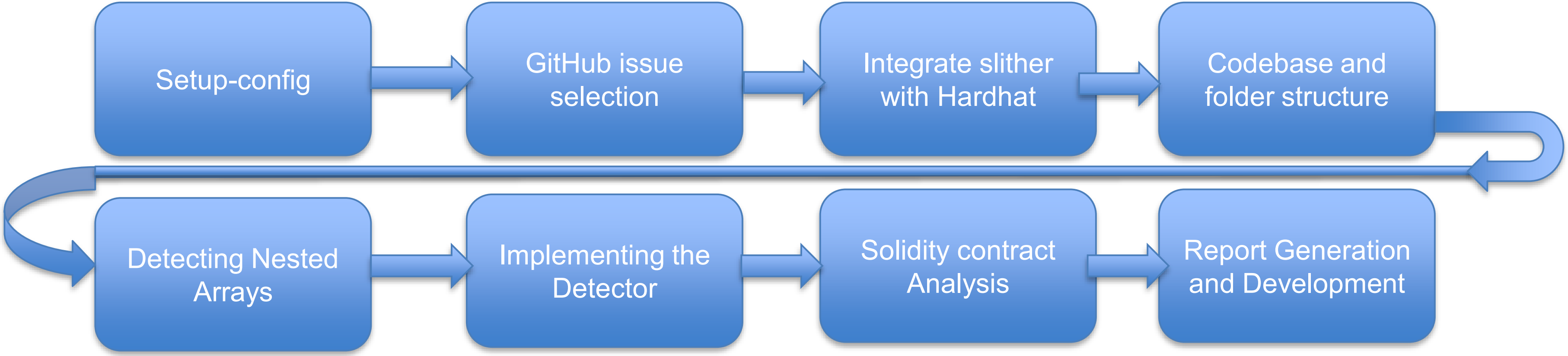
- This improvement will expand Slither's scope and accuracy in evaluating contracts, making it more comprehensive and precise.

- It addresses the current limitation in analyzing security vulnerabilities within smart contracts that utilize nested structs. [2]

About the Detector

- Detection of nested structures.
- Integration with Slither and interpreting solidity code to identify suitable hooks for the detector.
- Designing the detection algorithm to analyze the declaration to point instances where nested structs are employed.
- Implementing and integrating the algorithm's design into Slither and testing its effectiveness across Solidity smart contracts.

Planning



Setup-config

GitHub issue selection

Integrate slither with Hardhat

Codebase and folder structure

Detecting Nested Arrays

Implementing the Detector

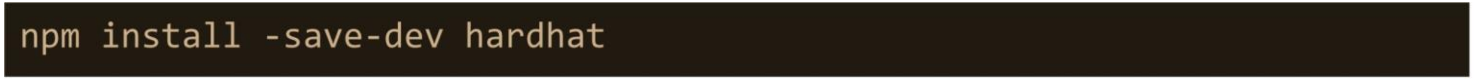
Solidity contract Analysis

Report Generation and Development

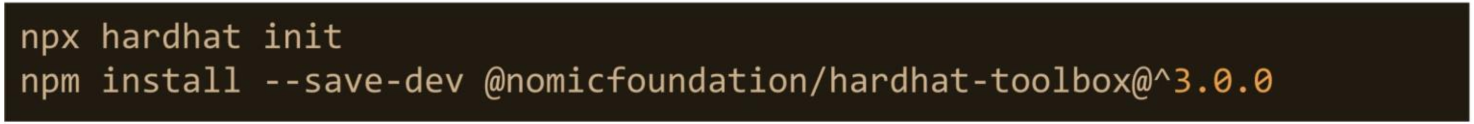
Specification and Design

1. Installation on Ubuntu OS:

a. Hardhat

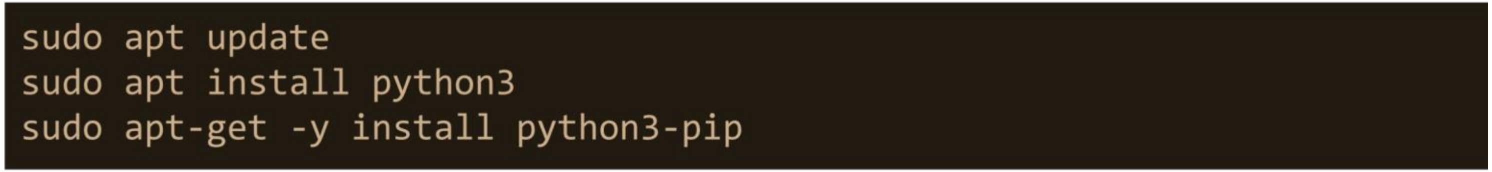


```
npm install -save-dev hardhat
```



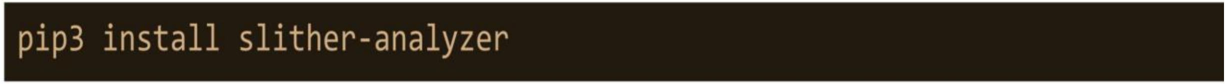
```
npx hardhat init
npm install --save-dev @nomicfoundation/hardhat-toolbox@^3.0.0
```

b. Python



```
sudo apt update
sudo apt install python3
sudo apt-get -y install python3-pip
```

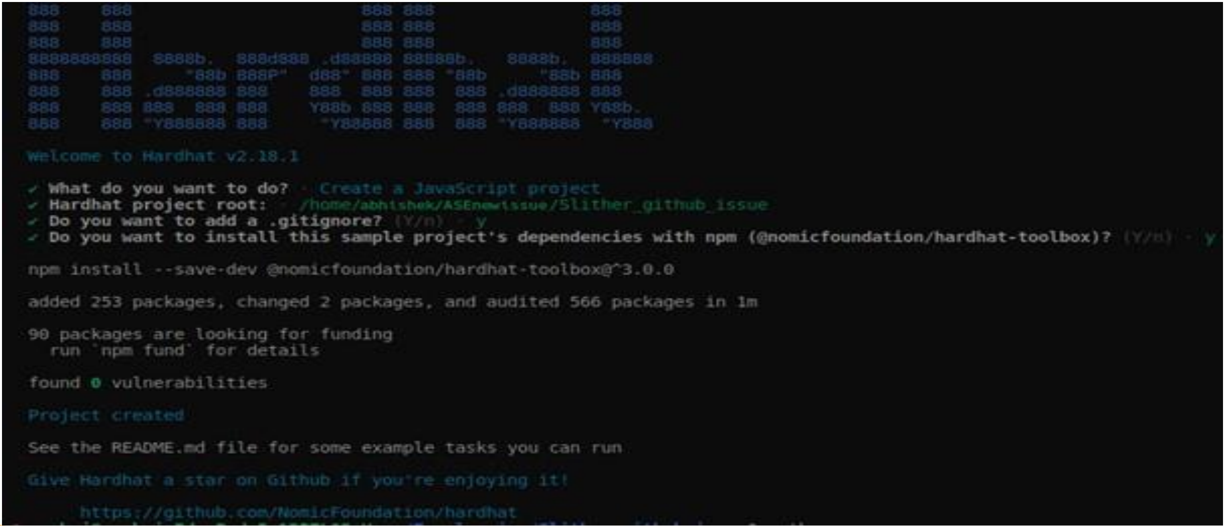
c. Slither



```
pip3 install slither-analyzer
```

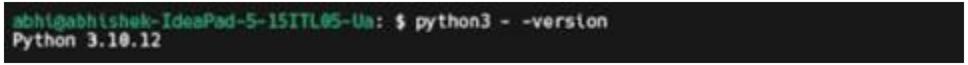
2. Code and Screen Shots

a. Hardhat Installed [4]



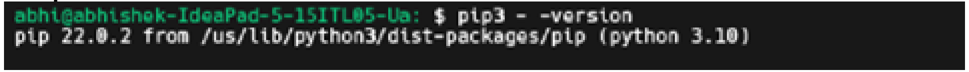
```
888    888                      888 888               888
888    888                      888 888               888
888    888                      888 888               888
8888888888  8888b.  888d888 .d88888 88888b.   8888b.  888888
888    888     "88b 888P"  d88" 888 888 "88b     "88b 888
888    888 .d888888 888    888  888 888  888 .d888888 888
888    888 888  888 888    Y88b 888 888  888 888  888 Y88b.
888    888 "Y888888 888     "Y88888 888  888 "Y888888  "Y888

Welcome to Hardhat v2.18.1

✓ What do you want to do? · Create a JavaScript project
✓ Hardhat project root: · /home/abhishek/ASEnewissue/Slither_github_issue
✓ Do you want to add a .gitignore? (Y/n) · y
✓ Do you want to install this sample project's dependencies with npm (@nomicfoundation/hardhat-toolbox)? (Y/n) · y

npm install --save-dev @nomicfoundation/hardhat-toolbox@^3.0.0

added 253 packages, changed 2 packages, and audited 566 packages in 1m

90 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities

Project created

See the README.md file for some example tasks you can run

Give Hardhat a star on Github if you're enjoying it!

     https://github.com/NomicFoundation/hardhat
```

b. Python Installed



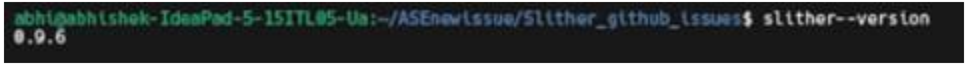
```
abhi@abhishek-IdeaPad-5-15ITL05-Ua: $ python3 - -version
Python 3.10.12
```

c. Pip3 Installed



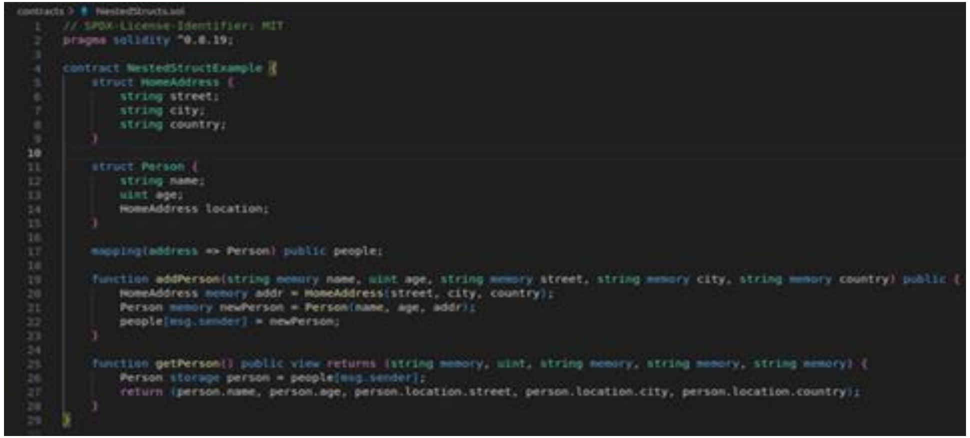
```
abhi@abhishek-IdeaPad-5-15ITL05-Ua: $ pip3 - -version
pip 22.0.2 from /us/lib/python3/dist-packages/pip (python 3.10)
```

d. Slither Installed [5]



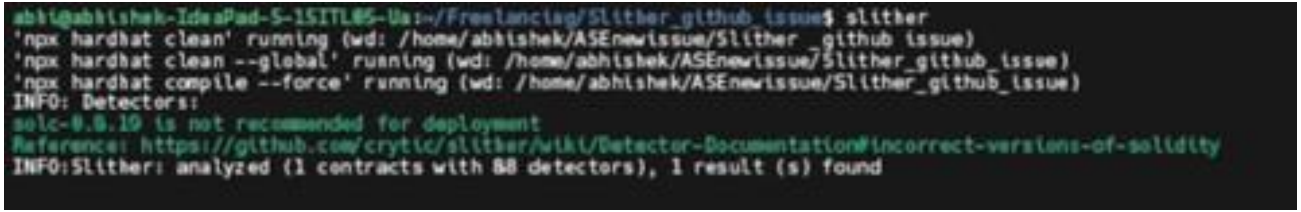
```
abhi@abhishek-IdeaPad-5-15ITL05-Ua:~/ASEnewissue/Slither_github_issues$ slither--version
0.9.6
```

e. Smart Contract



```solidity
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.19;

contract NestedStructExample {
    struct HomeAddress {
        string street;
        string city;
        string country;
    }

    struct Person {
        string name;
        uint age;
        HomeAddress location;
    }

    mapping(address => Person) public people;

    function addPerson(string memory name, uint age, string memory street, string memory city, string memory country) public {
        HomeAddress memory addr = HomeAddress(street, city, country);
        Person memory newPerson = Person(name, age, addr);
        people[msg.sender] = newPerson;
    }

    function getPerson() public view returns (string memory, uint, string memory, string memory, string memory) {
        Person storage person = people[msg.sender];
        return (person.name, person.age, person.location.street, person.location.city, person.location.country);
    }
}
```

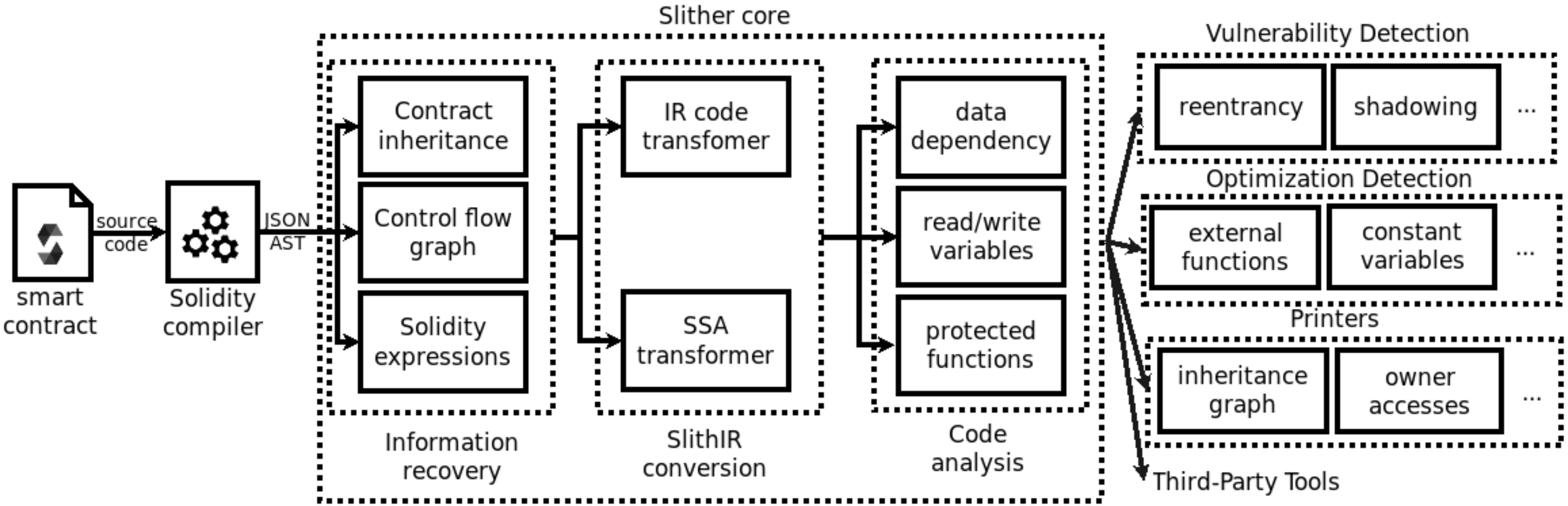
f. Slither command on Smart Contract



```
abhi@abhishek-IdeaPad-5-15ITL05-Ua:~/Freelancing/Slither_github_issue$ slither
'npx hardhat clean' running (wd: /home/abhishek/ASEnewissue/Slither _github issue)
'npx hardhat clean --global' running (wd: /home/abhishek/ASEnewissue/Slither_github_issue)
'npx hardhat compile --force' running (wd: /home/abhishek/ASEnewissue/Slither_github_issue)
INFO: Detectors:
solc-0.8.19 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Slither: analyzed (1 contracts with 88 detectors), 1 result (s) found
```

- The current slither detector is unable to detect the nested structs. We will improve the detector to detect and suggest better!

Architecture



[1]

Risk and Mitigation Plan

Risk/Issue Factor	Mitigation Plan	Risk Exposure
Maintaining and compatibility	Sticking with a fixed version of solidity in the detector.	Risk impact: 2 weeks Probability that risk will materialize: 92% Risk Exposure: 1 week approx.
Thorough Testing and Validation	Create detailed list of tests for the detector	Incomplete.
Technical issue - Inexperience with Python	Learning python via tutorials.	Risk impact: 5 weeks Probability that risk will materialize: 96% Risk Exposure: 3 weeks approx.
Technical issue- Inexperience with Solidity	Learning solidity language concepts by tutorials.	Risk impact: 4 weeks Probability that risk will materialize: 90% Risk Exposure: 4 weeks approx.
Technical issue- Complexity Building the Nested Struct and using in a Function	Finding out how to build nested structs and write them in the smart contracts.	Analyzing existing solidity open-source code and going through Solidity Documentation and relevant work.

Reference

1. Slither: https://github.com/crytic/slither
2. Issue: https://github.com/crytic/slither/issues/2077
3. Solidity: https://docs.soliditylang.org/en/v0.8.21/
4. Install Hardhat:hardhat.org/hardhat-runner/docs/getting-started#overview
5. Install Slither: https://github.com/crytic/slither#how-to-install
6. https://www.immunebytes.com/blog/slither-a-solidity-static-analyzer-for-smart-contracts/

GitHub Repository: https://github.com/Abhismoothie/Slither-Enhancementproject-team-9-CSE6324-001

Questions?

Thank You ☺