Inception Report

# Enhancement of slither for analyzing smart contracts

ADV TOPS SOFTWARE ENGINEERING

2232-CSE-6324-004

Github link: https://github.com/Sampath2901/6324-Project#6324-project

TEAM - 8

SAI NIKHIL KANCHUKATLA - 1002034488

SAI KRISHNAM RAJU BHUPATHIRAJU - 1002019782

SAMPATH KUMAR MEDIPUDI - 1002032901

FARAZ SHAIK AHMAR - 1002035224

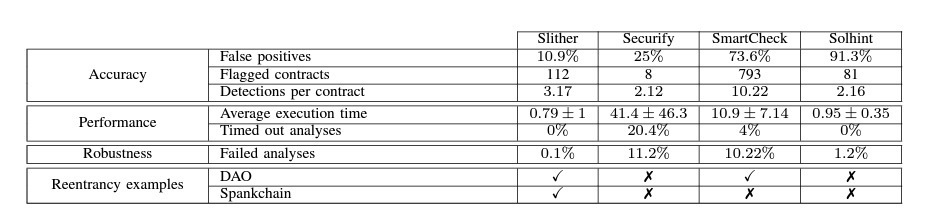
**Competitors for Slither:**

* Mythril and Securify properly detected issues in 6 out of 10 DeFi smart contracts that were vulnerable, and Slither in 5 out of 10. [1]
* Securify classified the majority of the errors as violations, which indicates that the tool has a high level of confidence in its ability to recognize security flaws. Additionally, Securify discovered problems with the usage of low-level calls and the absence of validation for user-controlled data, both of which are against the guidelines for safe development in the Solidity programming language. [1]



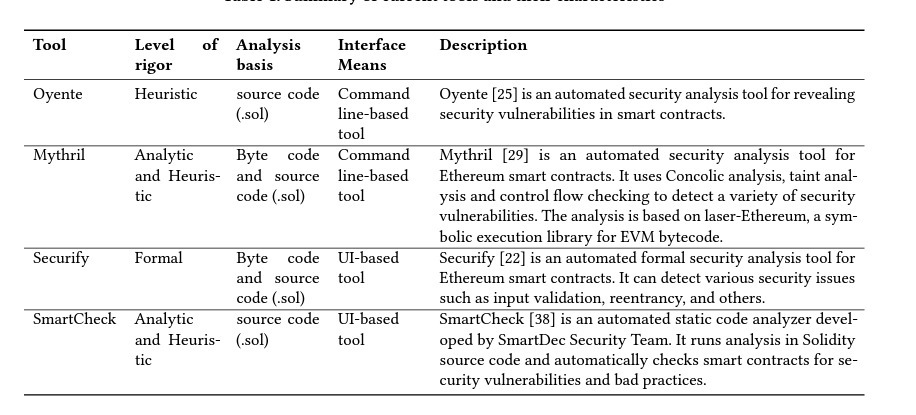
[https://www.h-x.technology/blog/top-3-smart-contract-audit-tools]

* The below table is the comparison of Accuracy, Performance, Robustness and Reentrancy examples of different tools. [2]



[<https://doi.org/10.48550/arXiv.1908.09878>]

* The below table is the summary of current tools and their characteristics. [3]



[<https://doi.org/10.48550/arXiv.1809.02702>]

**Features** [4]**:**

* Detects vulnerable Solidity code with low false positives (see the list of [trophies](https://github.com/crytic/slither/blob/master/trophies.md))
* Identifies where the error condition occurs in the source code
* Easily integrates into continuous integration and Truffle builds
* Built-in 'printers' quickly report crucial contract information
* Detector API to write custom analyses in Python
* Ability to analyze contracts written with Solidity >= 0.4
* Intermediate representation ([SlithIR](https://github.com/trailofbits/slither/wiki/SlithIR)) enables simple, high-precision analyses
* Correctly parses 99.9% of all public Solidity code
* Average execution time of less than 1 second per contract

**Risks :**

|  |  |  |  |
| --- | --- | --- | --- |
| **Risks** | **Major/Minor** | **Solution** | **Current Status** |
| Installation of Slither  (Configuration and setup) | Major risk | For new users to reduce this risk, it's crucial that they thoroughly read the Slither team's documentation. | In Progress |
| Unfamiliarity with the tool | Minor risk | It's crucial for new users to read the material given by the Slither team in order to lower this risk and watch the handson videos on youtube. | In Progress |
| Installation of dependencies(Python) | Minor risk | Users face difficult in setting up compatable version of python to run slither. | Completed |

**Customers and Users :**

**Who are the Slither users and what benefits does it provide for them?**

* Slither is used by **Block chain Developers** to run runs a suite of vulnerability detectors, prints visual information about contract details, and provides an API to easily write custom analyses. Slither enables developers to find vulnerabilities, enhance their code comprehension, and quickly prototype custom analyses. [4]
* Slither helps automate security reviews for **Block chain organizations**. Slither provides an API to inspect Solidity code via custom scripts. We use this API to rapidly answer unique questions about the code we’re reviewing. We have used Slither to:

1. Identify code that can modify a variable’s value.
2. Isolate the conditional logic statements that are influenced by a particular variable’s value.
3. Find other functions that are transitively reachable as a result of a call to a particular function. [5]

* **Block chain developers** uses slither to view high-level information about the contract using predefined printers.
* **Researchers** uses its own intermediate representation, SlithIR, to build innovative vulnerability analyses on Solidity. It provides access to the CFG of the functions, the inheritance of the contracts, and lets you inspect Solidity expressions. [5]

Security researchers uses slither to detect and describe security issues with underlying vulnerabilities, severity, and recommended fixes for our smart contract. [6]

Slither is most useful for the following 4 things: [7]

* Automated Vulnerability Detection: Easily detect vulnerabilities or security bugs in your code with low or no human effort.
* Automated optimization detection: Slither can detect code optimizations that the compiler misses while compiling.
* Slither can help you understand code better by summarizing and displaying contract information.
* Slither also helps with code reviews as its API can be easily interacted with by a user.

**What are We planning to do?**

* We are planning to perform **enhancement** to slither tool.
* We are currently working on the following issues and will provide more info in iteration 1.

Graphical user interface, text, application, email

Description automatically generated

[[https://github.com/crytic/slither/issues/1433]](https://github.com/crytic/slither/issues/1433)

**Graphical user interface, text, application, email

Description automatically generated**

[[https://github.com/crytic/slither/issues/981]](https://github.com/crytic/slither/issues/981)

**References:**

• [1] https://www.h-x.technology/blog/top-3-smart-contract-audit-tools

• [2] <https://doi.org/10.48550/arXiv.1908.09878>

• [3] <https://doi.org/10.48550/arXiv.1809.02702>

• [4] https://github.com/crytic/slither#features

• [5] https://blog.trailofbits.com/2018/10/19/slither-a-solidity-static-analysis-framework/

• [6] <https://medium.com/coinmonks/automated-smart-contract-security-review-with-slither-1834e9613b01>

• [7] <https://www.linkedin.com/pulse/how-secure-smart-contracts-slither-damilare-d-fagbemi/?trk=pulse-article_more-articles_related-content-card>

• [8] <https://github.com/crytic/slither/issues/981>

• [9] https://github.com/crytic/slither/issues/1433