Advanced Topics in Software Engineering(CSE 6324)
Fall 2022

Team 4

Atul Upadhye

Kundana Vaka

Yamini Dhulipalla

Srikar Sai Yarlagadda

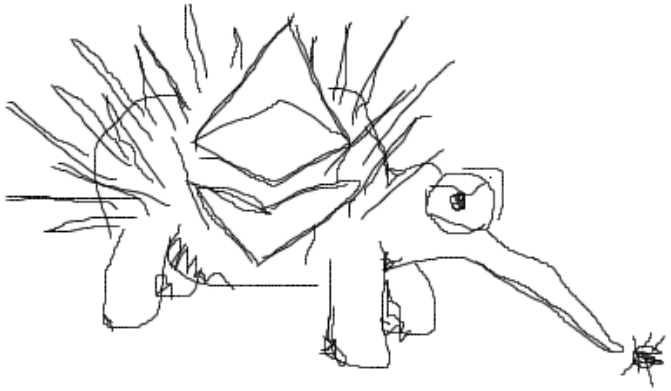
Vigneshwar Selvaraj

Improvements to Existing tools for Analyzing Smart Contracts

Agenda

- Current tools / Competitors
- Features
- Improvements
- Risks
- Customers and Users
- References

Current Tools/ Competitors



Echidna

Manticore

Echidna Features

- Generates inputs tailored to your actual code.
- Optional corpus collection, mutation and coverage guidance to find deeper bugs.
- Source code integration to identify which lines are covered after the fuzzing campaign.
- Automatic test case minimization for quick triage.

Improvements

- Introduce more automation.
- Improve upon code coverage.
- Improving the inputs based on our program.

Risks

- Online resources i.e. documents and community support are still limited.
- Unaddressed security vulnerabilities can turn into existential threats.
- Limitations of the existing tool.

Customers and Users

- Smart contract auditors from the following domains can perform audits whenever requested.
    * Finance , Gaming, Healthcare, Real estate etc;

References

- C, C. (n.d.). *GitHub - crytic/echidna: Ethereum smart contract fuzzer*. GitHub. Retrieved September 12, 2022, from https://github.com/crytic/echidna
- T, T. (n.d.). *GitHub - trailofbits/manticore: Symbolic execution tool*. GitHub. Retrieved September 12, 2022, from https://github.com/trailofbits/manticore

Github

- https://github.com/AtulUpadhye17/CSE-6324-Team4

THANK YOU!