

Woke Fuzzer

EthPrague 2022

Dominik Teiml, Michal Převrátíl

Contents

- Intro 3
- History of Woke 4
- Existing fuzzers 8
- FAQ 8

Intro

- [Ackee Blockchain](#) is a blockchain security firm based in Prague, Czech Republic.
- Dominik Teiml: Ethereum Tech Lead @ Ackee Blockchain.
 📄 Fml. Gnosis, CertiK, Trail of Bits
- Michal Převrátíl: Woke Developer @ Ackee Blockchain.

Beginning

I think we all feel the immaturity of existing Ethereum tooling.

This is usually NOT the fault of the developers of those tools.

Making great tools requires:

- a lot of experience with Ethereum,
- experience with the implementation language,
- a lot of expended effort,

and the gains (at least for the developer) are not immediately super high.

Sometime in October 2021, Dom saw enough possible improvements for Slither to warrant building a new tool.

Ideation

So originally, the idea was just to build a better Slither.

Later, we realized that if we have that, we can easily implement a lot of other features:

- a state-of-the-art language server,
- research new methods of contract visualization, both on the static level (source code) and dynamic (transaction execution)
- a line-by-line debugger for Solidity contracts,

and many others. We got to work.

Woke Fuzzer

First, we implemented a config parser, a Solidity version manager, a regex parser for versions and imports, and a compilation manager.

Sometime in March, Dom implemented a simple fuzzer during a smart contract audit.

We then used it during several audits and it found several high-severity bugs.

The Fork



In May 2022 (a few weeks ago) Dom decided to fork the project.

- to explore new methods of symbolic execution and contract visualization

The original Woke team at [Ackee Blockchain](#) will focus on the Language server. 🥰

The Merge?



Existing fuzzers

Echidna

Echidna is powerful, but we think the following are very real issues:

*

FAQ

How can I get help?

https://t.me/+n7Z37eJ1_hMOZmJk