Artifact Evaluation Abstract

Anonymous

May 4, 2022

1 Paper Title

WASAI: Uncovering Vulnerabilities in Wasm Smart Contracts

2 Badge

- Available Badge

3 Artifact Link

`https://github.com/wasai-project/wasai`

4 Environments

- OS: OS: Ubuntu 18.04 64bit
- CPU: x86-64, Intel I9
- Memory: 64GB RAM

5 Getting Started

1) download the code repository from Github.
   `git clone https://github.com/wasai-project/wasai.git && cd wasai`
2) run a docker container to build WASAI.
   `sudo docker build -t localhost/client-eos:wasai .`
   `sudo docker run -rm -ti localhost/client-eos:wasai`
3) execute the bin/fuzz.py in the docker container to get the result.
   `python3 -m bin.fuzz ./examples/batdappboomx/batdappboomx.wasm ./examples/batdappboomx/batdappboomx.abi batdappboomx 300 300 ./rt/ -detect_vuls 020000`
4) WASAI should identifies Bug#2 (Fake Notification) for this example. See `https://bloks.io/account/batdappboomx` for more details of this example.