

REPRODUCE (FROM SCRATCH)

what the artifacts do

Our artifacts include three components, type inference, fuzzer and coverage collecting.

For the type inference component, our tool uses differential analysis to reason about the type information of the binding calls in PDF Readers.

For the fuzzer component, our tool uses the type information to guide the generation of test PDFs.

For coverage collecting component, our tool uses DynamoRIO to collect the coverage information when running test PDFs.

where to get artifacts

You can download the source code of our artifacts from [software heritage](#).

We have also prepared a VirtualBox virtual machine with all the test environment for easier reproduction. The virtual machine can be downloaded from [zenodo](#).

how to reproduce

For the reproduction of RQ1 and RQ2, please refer to the type inference component of our tool. which are `C:\Users\wxy\TypeOracle\Tools\TypeInfer\adobe\README.pdf` for type inference in Adobe Reader and `C:\Users\wxy\TypeOracle\Tools\TypeInfer\foxit\README.pdf` for type inference in Foxit Reader. After getting the type information, you can compare it with the ground truth, which is located in `data/ground_truth` folder, please refer to

`C:\Users\wxy\TypeOracle\Evaluation\RQ1_TypeAccuracy\README.pdf`. As for other type inferring methods, please refer to `C:\Users\wxy\TypeOracle\Other\TypeInfer`.

For the reproduction of RQ3, please refer to the fuzzer component and coverage collecting component of our tool. First, you need to run the fuzzer for 48 hours to generate some PDF files, please refer to `C:\Users\wxy\TypeOracle\Tools\Fuzzer\README.pdf` to use the fuzzer of TypeOracle. As for other fuzzers, please refer to `C:\Users\wxy\TypeOracle\Other\Fuzzer`. After executing the fuzzer for 48 hours, you need to use the coverage collecting component to collect the coverage information. For the coverage collecting, please refer to `C:\Users\wxy\TypeOracle\Tools\Coverage\README.pdf`.

For the reproduction of RQ4, please refer to the fuzzer component of our tool. The PDFs which can cause PDF Readers to crash will be stored in `save/crash` folder, please refer to `C:\Users\wxy\TypeOracle\Evaluation\RQ4_FuzzingCampaign\README.pdf` for manually check.

For some tips that may be helpful for the reproduction, please refer to `C:\Users\wxy\TypeOracle\Other\Tips.pdf`

