HUANYAO RONG

ronghua@iu.edu
Website ◇ Github

EDUCATION

Imperial College London *October 2016 - July 2019*
BEng in Computing
Department of Computing First Class Honor with Overall Percentage: 75.25

Indiana University Bloomington *August 2020 - Present*
Advised by Prof. Xiaofeng Wang
Computer Science PhD GPA: 3.95

EMPLOYMENT

Pangu Team, Qianxin *July 2019 - October 2020*
Security Researcher

Browser Security Research.

RESEARCH INTERESTS

System Security, Vulnerability Discovery, Fuzzing, Program Analysis

PROJECTS

JsTainter *Year 2019*

· Dynamic taint analysis on JavaScript program based on dynamic instrumentation framework, Jalangi2.
· Source Code and Thesis.

Fuzzilli Extension *Year 2019-2020*

· Extension of famous IR-based JavaScript fuzzer, Fuzzilli.
· More mutation rule and IR are added to try to generate more thorough JavaScript test cases.

Graph-based JavaScript Fuzzer *Year 2020-2021*

· Similar to Fuzzilli, the project is a JavaScript fuzzer that represents JavaScript program with graph-based IR. Similar analysis and mutation are implemented.
· The project also tries to embed JavaScript test case using Graph Neural Network to aid fuzzing.

Directed Fuzzer AFLRun *Year 2022*

· It proposes a novel coverage metric for directed fuzzing in order to improve path diversity for already-covered targets.
· It also has a more effective seed scheduling algorithm that serves such new coverage metric.
· The work is currently in submission of Usenix Security 2023.

TECHNICAL SKILLS

Programming Languages
C/C++, Assembly, Python, Java, JavaScript, PHP, Haskell

Security
Reverse Engineering (e.g. GDB and IDA Pro)
Binary Vulnerabilities and their Exploitation
Operating Systems (e.i. Windows and Linux) and their Security (e.g. Linux Kernel Exploitation)
Compiler (e.g. LLVM and JavaScript JIT Optimization Bugs)
Software Protection (e.g. Obfuscation and Packing)
Program Analysis (e.g. Fuzzing)

ACHIEVEMENTS

CTF

With EmpireCTF.

- Team Write-ups
- CSAW Europe 2018 Finalist

With cr0wn.

- 3rd place at CONFidence CTF 2019 Finals (remote help)

With r3kapig.

- Organizer of XCTF 2019 Final and XCTF 2020 Final (Link to Challenges)
- HITCON CTF 2019 Finalist
- 4th Place at 0CTF/TCTF 2020 Quals
- 12nd Place at Defcon CTF Final 2022 (3-4 Place in LiveCTF)
- Writeup Competition Winner of Google CTF 2021 and Google CTF 2022

Bugs Reported

- *Chromium.* Issue 1020538, Issue 1057008, Issue 1104608 (reward $5000)
- *WABT.* CVE-2022-44407, CVE-2022-44408, CVE-2022-44409
- *Binutils.* CVE-2023-25584, CVE-2023-25585, CVE-2023-25586, CVE-2023-25587, CVE-2023-25588

TEACHING EXPERIENCE

Instructor of Reverse Engineering, XMan Summer Course 2019 at Fudan University