

# HUANYAO RONG

hr1316@ic.ac.uk

Website: <https://mem2019.github.io/> ◇ Github: <https://github.com/Mem2019/>

## EDUCATION

---

**Imperial College London**

*October 2016 - July 2019*

BEng in Computing

Department of Computing

First Class Honor with Overall Percentage: 75.25

## EMPLOYMENT

---

**Pangu Team, Qianxin**

*July 2019 - Present*

*Security Researcher*

- Famous security team focusing on vulnerability research. I am currently working on vulnerability discovery of V8 JavaScript Engine.

## RESEARCH INTERESTS

---

System Security, Vulnerability Discovery, Fuzzing, Program Analysis, CTF

## PROJECTS

---

### **Wacc Compiler**

A simple compiler project, I have implemented the transformation from IR to ARM assembly, and I also designed a custom WACC executable file format and a virtual machine that run such executable.

### **Pintos**

Operating System kernel, including thread scheduling, syscall handler, virtual memory management.

### **LV8 Sport**

Machine learning related project. Project that processes the video of a tennis play, with vision analysis(e.i. pose estimation, ball detection and court detection), and compute relevant metrics about the play(e.g. step counting and shot quality evaluation).

### **JsTainter**

Dynamic taint analysis on JavaScript program based on dynamic instrumentation framework, Jalangi2.

Thesis: <https://github.com/Mem2019/JsTainter/blob/master/docs/JsTainter.pdf>

### **Fuzzilli Extension**

Extension of famous IR-based JavaScript fuzzer, Fuzilli(<https://github.com/googleprojectzero/fuzzilli>).

More mutation rule and IR are added to try to improve coverage and find more vulnerability.

## TECHNICAL SKILLS

---

### Programming Languages

C/C++/Java/Intel assembly/Python  
JavaScript/ARM assembly/PHP/Haskell

### Security

Reverse Engineering  
Binary Vulnerabilities and Relevant Exploitation Techniques  
Experience of Analyzing CVEs  
Operating Systems(e.i. Windows and Linux) and Relevant Security(e.g. Linux Kernel Exploitation)  
Web Security Basics  
Compiler(e.g. JavaScript JIT Optimization Bugs)  
Android Reverse Engineering Basics  
Software Protection(e.g. Obfuscation and Packing)  
Symbolic Execution and Taint Analysis Basics  
Virtualization Technology Basics

### Third Year Courses

Computer Vision, Information and Coding Theory, Robotics, Introduction to Machine Learning, Network and Web Security, Advanced Computer Architecture

## ACHIEVEMENTS

---

### CTF

Co-founder of First CTF Team at Imperial College, EmpireCTF(<https://ctftime.org/team/57176>)  
Team Write-ups(EmpireCTF): <https://github.com/EmpireCTF/empirectf>  
CSAW Europe 2018 Finalist (as EmpireCTF)  
Member of cr0wn(<https://ctftime.org/team/48976>) and r3kapig(<https://ctftime.org/team/58979>)  
3rd place at CONFidence CTF 2019 Finals(remote help as cr0wn)  
3rd place at Cloud Security Challenge in Geekpwn 2019 Shanghai(as r3kapig)  
Organizer(as r3kapig) of XCTF 2019 Final, Final Event of the largest CTF League in Asia  
HITCON CTF 2019 Qualifier(as r3kapig)

### Bugs Reported

Chromium Issue 1020538

## TEACHING EXPERIENCE

---

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