个人简历

姓 名： 洪 玄 泉 · **电 话：** 15665162218 · **求职意向：** 安全研究员
学 历： 硕士研究生 · **邮 箱：** 1242472741@qq.com · **GPA：** 3.45/4

教育背景

- 2017.9~2021.6：中国矿业大学　计算机科学与技术学院　信息安全（学士）
- 2021.9~2024.6：四川大学　网络空间安全学院　网络空间安全（硕士）

技能清单

- 安全研究：熟悉 Fuzz 技术，精通 AFL、libfuzzer 等主流模糊器，能够针对特定测试的目标来对fuzzer进行二次开发。熟悉主流Linux漏洞和常见Web漏洞原理；
- 开发语言： 熟悉C\C++、python等语言，熟悉x86架构下汇编，掌握windows和linux系统下的C/C++开发；
- 计算机基础：熟悉计算机网络、操作系统、数据结构等基础知识；

实习经历

2022.5~至今 上海安般科技有限公司

职责：兼职助理研究员

主要职责：

1. 负责模糊测试相关课题的可行性验证（POC）项目；
2. 提供AFL等模糊器相关工具技术支持，完成fuzz工具的部分开发和对接测试；
3. 负责课题调研并确认基本技术路线，开源工具改造，后期对接并交付。

项目经历

2023.03~2023.07 基于状态转移的协议模糊测试工具优化

项目描述：

- 灰盒协议测试模糊测试（AFLNET）主要被用于对开源服务器的实现进行测试，本项目就AFLNET的状态引导的不足，设计了新的状态机实现方法，在代码覆盖率、crash数量上有一定的提升。

主要职责：

- 负责项目的开发、实验、论文产出。主要思路是利用状态转移来引导协议模糊测试的状态选择、种子保留以及能量调度。

2022.04~2022.10 基于文法变异的灰盒协议模糊测试

项目描述：

- 现有的灰盒协议模糊测试变异算法无法满足特定格式的协议需求，本项目针对该问题增加了可以描述协议格式的变异算法，使得生成种子的质量方面有比较大的提高，能更好提升测试覆盖率。

主要职责：

- 前期针对结构化变异算法调研，协助开发，编写协议模板，后期测试。

其他

- 论文《AFLNeTrans：基于状态转移引导的灰盒协议模糊测试技术研究》，在投；
- github: LeeHun9 (leehung) (github.com)
- 个人开发项目：
    - windows平台下的小工具：PE解析器，加密壳，进程监控等；
    - Linux平台下C++高并发WebServer；