

个人简历

姓名：洪玄泉 · 电话：15665162218 · 求职意向：网络安全
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，熟悉 AFL、libfuzzer 等主流模糊器，能够针对特定测试的目标来对 fuzzer 进行调整。熟悉linux下主流漏洞原理和利用；
- 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、数据结构等知识；

🏢 兼职经历

2022.5~至今 安般科技

职责：协助协议模糊测试等课题研究，帮助调研，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；

主要职责：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~至今 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：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文法的协议需求，项目针对该问题增加了可以描述协议格式的变异算法，生成种子的质量方面有比较大的提高，能更好提升覆盖率。
- 主要职责：前期针对结构化变异算法调研，协助开发，编写协议描述，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研究》，在投；
- github: [LeeHun9 \(leeHung\)](https://github.com/leeHung9).(github.com).
- 个人项目：
 - windows平台下的小工具开发：PE解析器，加密壳，进程监控等；
 - Linux平台下C++高并发WebServer