

专业技能

- 熟悉OWASP Top 10安全漏洞原理与利用方法，熟练进行NDAY漏洞快速复现与利用
- 具备独立代码审计能力，曾挖掘emlog、帝国CMS、CakePHP等系统0day漏洞
- Python/PHP: 熟练掌握，能够独立编写漏洞POC与自动化利用脚本
- Java/Node.js: 基础扎实，能够结合AI工具快速修改POC并实现漏洞利用
- Docker: 熟练使用容器技术，能够独立编写Dockerfile进行应用部署与环境搭建
- 熟悉常见内网横向移动技术
- 熟悉传统AD域攻击手法，包括DCSync攻击、委派攻击、ADCS攻击、NTLM中继攻击、RODC攻击
- 截止目前参加过近百场ctf竞赛，具有独立出题能力。曾为ctfshow、SU、赛宁网安、永信至诚等平台、战队或公司供题，具有较为丰富的讲课经验（ctf）。

工作经验

- 上海云众凯科技

红队初级渗透工程师

2025.7.3--2025.7.17
- 负责外网打点以及传统AD环境的内网横向渗透
- 上海得物信息集团有限公司

应用安全实习生

2025.8.28-至今
- SDL小组成员，负责漏洞推修

项目经历

- 学校内网渗透

红队
- 通过黑盒测试发现学校某服务器系统存在未授权访问，泄露大量信息。某服务器系统存在越权访问，到后台getshell。
- 2024年某攻防演练

红队
- 通过任意文件上传getshell，系统文件中泄露大量配置信息，且同网段服务器有heapdump泄露、信呼OA等Nday漏洞，最终getshell*3，获取数据库权限*3

教育经历

- 成都大学

软件工程 · 本科

2023/9/15 - 2027/6/30
- 担任CDUSEC战队队长

获得的奖项

- 国内知名联合战队SU队长
- 2024年第十六届四川省大学生信息安全技术大赛二等奖
- VNCTF2025Web单方向第二名，总排7th
- 第九届XCTF分站赛ACTF2025团队排名11th
- 2025数字中国创新大赛数据安全产业积分争夺赛铜奖，全国排名10th
- dasctf2024最后一战三等奖全国6th
- dasctf2025上半年赛冠军
- XCTF-L3HCTF 2025 冠军
- 春秋云境排名TOP3，熟悉域渗透基本流程。

- 首届CCF 智能汽车大赛（CCF IVC2025） “汽车安全攻防赛” 初赛 季军 决赛二等奖