鑫

男 | 25 岁 | 个人主页：xtar.pages.dev

个人背景

兰州理工大学 2021.09 – 2025.06

网络空间安全（本科）

- 发表论文：*An Interactive Multimodal Tool for Extraction and Verification in Archaeological Reports*（ACM）
- 在 CSDN 上发布多篇技术贴；个人公众号粉丝超八百；语雀技术文档超八万字
- 个人兼职：搭建某企业安全基线，从 0 到 1 负责公司安全体系建设，面向 50+ 台 Windows 终端设计并落地企业网络安全架构，通过 VLAN/ACL 实现办公、生产、生活、Guest 及数据存储区域隔离，基于 Windows Server 2025 搭建 AD 域控并通过 GPO 统一终端安全策略；结合 Sysmon、Wazuh 构建终端行为监控、日志集中分析与安全告警体系，并引入开源 SOAR 平台 Shuffle 实现安全事件自动化编排与响应，将 Wazuh 告警与资产、身份及终端处置流程联动；同时通过自动化脚本实现终端批量入域及安全 Agent/策略部署，围绕 NAS 数据访问、VPN 远程接入、802.1X/RADIUS 网络准入、网络流量分析等方向建立长期演进方案，形成覆盖资产、网络、身份、终端、检测、响应与数据访问控制的纵深防御体系。

专业技能

- **网络安全工具**：熟练掌握 Kali Linux，熟悉 Nmap、Wireshark、Metasploit、Hashcat、Hydra、BurpSuite、SQLmap、AWVS 等工具，多次参加 HW 红队
- **编程语言与框架**：熟练掌握 Python（pygame、Matplotlib、pandas、requests），掌握简单爬虫、数据分析、小型游戏开发；使用 flask，FastAPI 进行后端开发
- **AI 与大模型**：熟悉各个 AI 大模型、智能体框架和本地 AI 应用（MetaGPT、LM-Studio、AnythingLLM），掌握本地大模型部署、知识库构建及简单脚本编写
- **安全技术**：熟悉 TCP/IP 协议，具备 Wireshark 数据包分析能力，掌握 RSA 等加密算法及 CTF 相关工具，了解文件隐写，各类安全脚本等
- **开发与运维**：开发通用型本地大模型知识库系统；熟悉 Linux、Docker、Git，以及 conda 环境配置，有 Docker 部署各类安全靶场、MaxKB、PaddleOCR 等经验

工作经历

中国人民银行征信中心-奇安信驻场 2026.04 – 至今

安全运营工程师

- 参与国产 WAF，天眼等多种安全设备及平台的部署与调优，包括日志采集、告警联动、规则优化及终端安全策略配置的规则调优
- 参与 2026 金融国家级 HW，作为内外部联络人，统筹 HW 期间的人员调配和事务交流，顺利完成项目
- 参与 HW 前期的互联网暴露面资产梳理和渗透测试，使用 AI 进行辅助发现征信系统前端 js 中隐藏的高危漏洞，输出报告及其后续的修复跟踪

- 参与中心的制度建设，多家 SEIM 平台引入、网络准入、国产信创化改造等项目建设，能够迅速掌握双方痛点，应对多种突发情况

观初/云纷（上海）信息科技 2025.10 – 2026.04

安全分析师

- 参与某大型药企 MDR 平台部署工作，独立完成 Agent 下发、策略配置、终端接入及联调测试，推动约 2000 台终端成功上线，使用观初/云纷自研安全平台对 ELK 日志进行关联分析，编写并部署告警规则，实现异常行为检测与安全事件预警
- 参与某能源企业安全基线重构项目，负责 ELK 工具链、日志采集组件及 SIEM 平台的部署、设备日志接入与规则调优
- 日常使用 Splunk、ELK 等日志分析平台进行安全巡检，完成日志检索、异常行为分析、安全日报/周报输出及告警事件跟踪
- 参与企业等保相关安全建设工作，协助编写安全管理制度、资产清单、网络拓扑、安全整改方案及部分测评材料
- 对多个企业 Microsoft Sentinel 平台进行规则优化与日志分析，结合香农熵算法识别 DGA 域名请求及异常网络行为，能够结合实际业务场景进行攻击路径分析与风险评估，对企业安全运营、威胁检测及暴露面治理具有一定实践经验
- 主导多个外企客户的内外网渗透测试项目，负责前期信息收集、漏洞验证、攻击链构建、风险分析及最终报告输出，独立完成项目交付与整改建议跟踪
- 某外企内网渗透阶段，发现 SQL 注入并成功利用，获取到数据库的类型、用户名、多个表及其字段，以及用于证据验证的敏感数据；发现 Swagger 接口文档泄露及其接口未授权访问
- 某项目外部渗透阶段，发现多个数据库存在 SQL 注入，并成功获取到敏感数据；发现其中一个站点的上传功能接口存在任意文件上传漏洞；发现多个系统存在 xss 漏洞
- 某外企内网渗透阶段，发现用户名爆破漏洞，目录浏览，以及敏感信息泄露等漏洞

实习经历

绿盟科技 2025.04 – 2025.09

渗透工程师

- 参与日常金融机构的系统测试，发现漏洞并协助修复；对分配的一些机构互联网暴露面进行系统测试
- 多次在补天和 edu 平台提交中高危漏洞，涉及越权及未授权访问等高危漏洞

国家级金融系统 HW-中级研判 2025.07 – 2025.08

蓝队研判

- 前置准备工作，梳理资产进行风险检查，进行互联网暴露面资产的渗透测试
- 负责研判监测提交的各类告警日均 150 条，追溯到 1 个疑似攻击队信息；利用青藤云、默安蜜罐等设备协助溯源，进行取证溯源等工作

甘肃省教育 HW 2025.06 – 2025.06

红队队员

- 成功进入三所高校的内网，获取数据库及 OA 权限，获取得分超 3500
- 前端 js 审计，发现后台未强行鉴权数据获取接口，从接口遍历到十数万条敏感信息，让某高校出局

兰州市正天合律师事务所正元分立办事处 2024.04 – 2025.04

系统维护与安全实习生

- 负责主系统日常维护，监控操作日志，开展简单攻防演练
- 尝试引入前端新版块，尝试本地部署量化后大模型，优化用户界面与交互体验

上海市福巨物流公司 2024.06 – 2024.09

安全工程师实习生

- 优化后台系统功能，辅助防火墙加固，提升系统安全性
- 编写安全测试用例，检测系统漏洞并提出修复建议

兰州理工大学-甘肃省教育 HW 2023.09 – 2023.10

红队队员，参加甘肃省教育厅护网行动，获甘肃省教育厅颁发的“优秀新星”荣誉

- 访问某高校未弃用的旧登录页面，进入教务系统之后发现未授权访问，可遍历到数万敏感信息
- 某中学招生报名系统，可任意身份注册，头像处可文件上传，获取 shell 进入内网

宁夏网信创安-医疗 HW 2023.07 – 2023.08

红队队员，参加宁夏自治区护网行动，取得成绩：5/13

- 利用 BurpSuite、SQLmap 等工具进行漏洞扫描与利用，协助团队完成攻防任务
- 对小程序和公众号资产进行渗透，发现某医院公众号一个接口存在越权漏洞，可下载其他患者的敏感信息

宁夏回族自治区省级 HW 2022.07 – 2022.07

红队队员，通过 fofa，hunter 进行信息收集，成功找到多个靶标后台、OA 和 CMS 系统

- 发现若干弱口令和历史漏洞，编写 POC 进行漏洞验证利用工作，成功获取到多个数据库的信息并写入 shell，在内网中获得大量物联网设备的控制权限

本科项目经历

兰州理工大学 AIGC 前沿技术——“考古文档提取”项目 2023 – 2024

深度参与 MetaGPT 驱动的多角色智能体开发，负责动态会话模块

- 部署 PaddleOCR 提取纸质考古文档中的文字与关键信息
- 设计并开发数据标注页面前端，引入 Vue 框架优化代码
- 实现单智能体（LLM+ 观察 + 思考 + 行动 + 记忆）功能，支持实景交互
- 项目链接：sjys.lut.edu.cn/info/1039/6814.htm

CTF 比赛与安全实践 2022 – 2024

多次参加 CTF 比赛，擅长密码学、隐写术、数据包分析及 Web 安全

- 比赛成绩：海丰杯（17/46;5/52）、帕鲁杯（前 20%）、DESCTF（前 25%）
- 在帕鲁杯中获密码学二血（RSA 加密解题）、杂项二血（隐写术分析），使用 010、IDA 等工具快速定位漏洞
- 在 DESCTF 中解决 3 道 Web 安全题目，利用 BurpSuite 挖掘 XSS 和 SQL 注入漏洞，利用漏洞成功读取 flag
- 开发 Python 脚本自动化分析 CTF 数据包，提升 30% 解题效率