包中其

baozongwi@outlook.com 19982072710
https://baozongwi.xyz/ 2005.07.23

专业技能

- 熟悉 OWASP Top 10 常见漏洞原理，擅长从源码层面分析漏洞成因，能针对性提出修复方案与安全编码建议
- 曾独立挖掘 emlog、帝国CMS、CakePHP、cshop 等知名开源系统 0day 漏洞，并具备快速复现 N-day/1-day 漏洞的能力
- 熟悉 Python/PHP/Java，具备安全开发能力。曾开发 FastAPI 探活与 Django 平台组件；Jython 编写 Burp 插件实现流量编码与 httpx 脚本转化，熟练构造 POC 及自动化检测脚本；善于利用 AI 协同高效完成前端主题的深度二开（su-team.cn）
- 熟悉 Docker 容器化技术，能够独立编写 Dockerfile 搭建漏洞复现环境及靶场，理解容器安全基础
- 热爱研究 Java 反序列化漏洞体系，熟悉 Log4j2、Fastjson、Hessian、Jackson 等组件的漏洞原理与利用链构造，能独立分析利用 Gadget，并能使用 tabby 挖掘 sink 点
- 了解 Active Directory 域环境攻击手法（如 DCSync、ADCS、NTLM Relay 等），具备复杂网络环境下的横向移动思维
- 参与数十场 CTF 竞赛。具备独立出题与培训能力，曾为 ctfshow、SU、赛宁网安等平台供题，并担任讲师

工作经验

上海沄众凯科技 红队初级渗透工程师 2025.7.3--2025.7.17

- 职责： 负责高强度攻防演练期间的边界突破与内网横向移动，针对目标核心资产进行全链路渗透。
- 成果： 针对某大型目标，独立发现 Weblogic T3 反序列化入口并完成漏洞利用；结合 OSINT 技术获取内网关键凭据，成功突破边界并横向移动至核心 SQL Server 数据库，在不影响业务的前提下，利用数据库触发器（Triggers）技术实现隐蔽权限维持，成功验证核心敏感数据可达性。

上海得物信息集团有限公司 应用安全工程师 2025.8.28-至今

- 负责办公网及业务系统的日常渗透，实战中挖掘出 Apache Flink 任意文件上传（导致 RCE）、Ollama 及多个内部应用未授权访问等高危漏洞。
- 跟进 SAST 静态分析结果进行人工审计，排查出 2 处参数拼接导致的 RCE 及 3 处 SQL 注入漏洞，并完成多处越权风险的复核。
- 参与公司黑盒扫描器建设，独立编写了 20+ 个针对性的 yaml 巡检插件，并开发漏洞管理平台“一键申请复测”插件以提升流转效率；搭建 Docker 环境用于漏洞复现与验证。
- 负责攻防演练后的复盘工作，与组内同事共同推进漏洞修复流程，协助研发定位问题，所在业务线的漏洞修复率达 97%。

项目经历

学校内网渗透 红队 2024.10.26

针对学校某历史业务系统进行黑盒安全测试，发现系统登录反射型XSS漏洞，劫持cookie到后台文件上传getshell

第三届陇剑杯网络安全大赛 出题人&现场运维 2025.09.11- 2025.09.19

负责半决运维渗透赛以及决赛 web 方向测题，决赛web 方向出题

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 CTF 联合战队 SU Captain
- 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
- 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
- DASCTF 2025 上半年赛冠军
- XCTF-L3HCTF 2025 冠军
- 春秋云境排名TOP10，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
- WMCTF 2025 亚军
- 第八届“强网”拟态防御国际精英挑战赛预赛 冠军、决赛 季军
- 第九届XCTF国际网络攻防联赛总决赛三等奖（8th）
- 2025 HKCERTCTF Quals 4th