杨源盛

求职方向：软件安全 / AI for Security / 漏洞挖掘

0xbeac@gmail.com · 131-2050-2601
github.com/BeaCox · beacox.space

个人简介

上海交通大学网络空间安全硕士在读，现于网络与系统安全实验室（NSSL）在陈力波老师指导下开展研究。长期关注 AI for Security 与系统软件安全，研究兴趣包括程序分析、自动化漏洞挖掘与二进制安全；具备 IoT 设备、开源软件和 AI 网关等场景的漏洞研究与工程实践。

教育经历

上海交通大学 · 网络空间安全 · 工学硕士　　2025.09 – 2028.03（预计）

上海交通大学 · 信息安全 · 工学学士　　2021.09 – 2025.06

实习经历

中国电子科技集团有限公司 · 安全研究实习生　　2025.06 – 2025.09

参与 fuzz 测试与自动化漏洞挖掘系统研发，开展目标程序测试、漏洞分析与验证。

上海戎磐网络科技有限公司 · 安全研究实习生　　2024.06 – 2024.09

参与静态污点分析平台测试与规则编写；结合逆向工程和固件模拟挖掘 Tenda、D-Link 设备漏洞。

研究与项目

gdb-mcp · Python / GDB/MI / MCP　　2026.06 – 至今

开发面向 AI 编码工具的多会话 GDB/gdbserver 调试服务，支持本地与远程调试、core dump 分析和 rr 反向调试，并以默认安全策略隔离危险操作。

面向复杂软件的智能化安全审计平台　　2026.01 – 2026.06

- 融合 IDA Headless、CodeQL/自研污点分析与 LangGraph ReAct，将确定性静态分析结果转化为可追踪证据，驱动智能体完成跨函数推理、漏洞确认与结构化报告。
- 设计可插拔分析后端与分层知识增强机制，统一二进制和多语言审计流程；通过两级上下文压缩、知识库沉淀与人机复核，提升长链路审计的持续性、可解释性和规则复用能力。

典型网络设备安全研究与漏洞挖掘　　2025.03 – 至今

- 深入分析典型网络设备固件架构与核心组件，围绕认证机制、管理接口、网络服务、守护进程和进程间通信等关键攻击面开展研究。
- 复现多项历史 CVE，其中包括多个无公开 PoC 的漏洞；梳理漏洞成因、触发条件与利用链路，独立挖掘多个 0-day RCE，完成漏洞验证与利用代码编写，形成从漏洞分析到稳定利用的完整实践经验。

漏洞与竞赛成果

- **IoT：**获得 TP-Link、Tenda、TOTOLINK、D-Link 等厂商 CVE/CNVD 编号 20 余个。
- **开源软件：**向 brpc、Tabby、Deskflow、pupnp 等主流开源项目披露多项漏洞，获得 CVE/GHSA 编号并推动上游修复。
- **阿里安全响应中心（ASRC）：**提交 Higress AI 网关等产品的安全漏洞。
- **竞赛：**第八届“强网杯”全国网络安全挑战赛线上赛第 1 名；SJTU CTF 2024 第 6 名；pwn.college 蓝带。

专业技能

- **安全研究：**静态代码审计、静态污点分析、动态调试、二进制分析与漏洞利用、IoT 固件漏洞挖掘、模糊测试、CTF Pwn；熟悉 ARM / x64。
- **Agent 与工程：**Agent 开发、LangGraph/ReAct、CodeQL、IDA Headless；Python、C、Go，熟悉 GDB、Angr、Linux；英语六级。