陈浩天

渗透测试实习生，
安全工程师实习生

邮箱：1457677580@qq.com
电话：15534453751
学历：本科

意向城市：北京
年龄：22
出生年月：2004

教育经历

中北大学 软件工程 本科

项目经历

Web 安全渗透测试实践 针对模拟 Web 应用进行完整渗透测试流程 2024-01 至 2026-01

对目标进行完整的渗透测试，使用 Nmap 进行端口扫描和服务识别，基于开放端口和服务使用 nmap 进行漏洞扫描，对于不同的端口服务进行详 细分析测试，找出漏洞并利用，针对不同的操作系统进行相应的提权操作，如对于 linux 系统进行内核提权，计划任务提 权， sudo 提权。
成就: 独立完成对 vulnhub 之中的简单靶机的渗透，如 Tr0ll,w1R3S 等靶机。

自动化安全扫描工具开发 用于 Web 安全学习与测试的 Python 脚本集合 2025-01 至 2026-01
https://github.com/haotian123861/pytool

项目涵盖 HTTP 请求操作、目录扫描、暴力破解、常见漏洞检测、Socket 通信等常见功能。
成就: 通过目录爆破工具发现隐藏 Web 路径，为后续渗透测试提供关键信息，利用暴力破解工具成功获取靶场账号权限， 验证了工具在渗透测试场景下的实用性项目经验

ai+网络安全 开发ai智能体，编写skill，辅助完成渗透测试工作 2026-03至今
https://github.com/haotian123861/penetration-testing-skill

沉淀渗透测试核心流程与常用命令速查手册，可支撑独立完成信息收集、漏洞利用、权限维持与内网横向移动；

梳理 30 + 主流安全工具（端口扫描、抓包改包、漏洞利用、提权工具等）的实战用法，形成可复用的工具链；

整理 10 + 主流中间件与 1000 + 常见 CVE 漏洞知识库，包含漏洞原理、利用条件与修复方案；沉淀 2000 + 项标准化漏洞检查清单，覆盖 OWASP Top10、业务逻辑漏洞、配置缺陷等场景，保障测试覆盖度；

搭建多语言代码审计指南（PHP/Java/Python/JS），掌握从源码层面挖掘安全缺陷的方法。

证书

网络信息安全工程师（NISP一级）

网络信息安全工程师（NISP二级）

大学英语四级（CET-4）

技能

渗透测试工具链：
熟练运用 Nmap、Metasploit、Burp Suite、Sqlmap 等主流安全工具，可根据场景灵活组合使用；

自动化与脚本能力：
掌握 Python 编程，可独立编写目录扫描、暴力破解、漏洞检测等简单的自动化脚本。

渗透测试全流程能力：
熟悉从信息收集、漏洞利用、权限维持到内网横向移动的完整流程；可独立完成靶场渗透测试项目。

AI + 安全应用：
具备 AI 智能体开发能力，编写渗透测试 Skill 工具；实现了安全工具调用、漏洞知识库检索的自动化辅助，提升测试效率。