

刘英达

渗透测试工程师 | 网络安全工程师

男 / 1997.03  
伦敦大学皇家霍洛威学院 · 信息安全  
硕士 / 2019.09 - 2020.09 (预计)  
北京科技大学 · 信息安全  
本科 / 2015.07 - 2019.06

我的技术博客  
Github - refate  
cielwaath@outlook.com  
+44 7529933842  
+86 13126588677

经历

梆梆安全

2018.10 - 2019.04

于技术服务中心（北京）提供安全服务

- 对甲方移动应用（Android/iOS）或Web应用进行远程/现场渗透测试
- 根据所发现的漏洞撰写测试报告并提供修复意见
- 搭建可移动的渗透测试环境
- 担任实习生的部分技术培训

娄底轮子科技

2018.04 - 2018.08

负责微信小程序的前端开发，包括：

- JavaScript逻辑代码实现
- html、css的UI设计
- 与后端对接，管理测试版本

Ever404团队

作为北京科技大学信息安全社团的一员，参加CTF比赛并荣获：

- 第11届全国大学生信息安全竞赛创新能力实践赛 全国三等奖
- 2017-2018全国高校“西普杯”信息安全铁人三项赛第一赛区 二等奖

本科生创新训练项目(SRTP)

作为《基于忆阻神经网络的网络保密通信平台》项目负责人。项目核心在于调用Python科学计算库，使用Qt进行UI设计，将学校实验室的科研成果以软件工程实现。

- 在2019年1月荣获北京科技大学颁发的校级一等奖

技能

Web渗透

- 熟悉Nmap、BurpSuite、Sqlmap、NetCat等工具
- 熟悉Chrome、Firefox控制台(HackBar)
- 了解Metasploit的使用

移动渗透

- 熟悉Adb、Apktool、Frida、Xposed、Drozer、Jeb等工具的使用
- 熟悉加密函数的定位以及解密hook的编写
- 了解脱壳技术

网络协议

- 掌握互联网基本运行机制，TCP与UDP协议
- 掌握HTTP协议，对HTTP/2也有了解

数据库

- 掌握关系型数据库基本概念与SQL
- 会操作MongoDB

其他

- 英语：雅思7.0；日语：掌握，待考级
- 熟悉Git、MarkDown、Docker
- Kali Linux初级用户
- 关注看雪论坛、安全客、长亭技术专栏等网站
- 读过2018 OWASP Top 10和Mobile Top 10

计划

- (近期) 补习栈溢出、二进制与逆向分析的原理知识
- (实战) 从Hack the Box 实验平台开始
- (长期) 研究在5G、物联网背景下，满足安全需求的未来网络架构

