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（11月8日出最终成绩，12月邮寄学位证）
北京科技大学 · 信息安全
本科 / 2015.07 - 2019.06

【【【博客】】】
Github - refate
cielwaath@outlook.com
+44 7529933842
+86 13126588677

经历

梆梆安全 - 移动渗透实习生 实习
2018.10 - 2019.04
前安全服务部（北京）

- 对移动应用（Android/iOS）或Web应用进行渗透测试
- 根据所发现的漏洞撰写测试报告并提供修复意见

Royal Holloway - 授课型硕士 上学
2019.09 - 2020.09
部分笔记，预览成绩（50及格，非最终版）：

- 安全管理：51；密码学：46（补考成绩未出）
- 网络安全：61；OS安全：65
- 软件安全：81；安全测试：57

？？？ 玩耍
世界唯二找到所有秘密宝藏的人

- Unity逆向 、 ARM修改
- 长期蹲点&信息搜集、已有资源的充分利用
- 灵感和运气

项目

Frider 毕设
研究生Final Project；Ant Design的Frida版XServer

- + APP基础信息
- + 一键脱壳到PC
- + 支持NativeFunction

近期计划

- 了解自动化测试
- 改进Frider
- 学AI

技能

移动渗透

- 了解部分hook技术的原理(Dalvik, ART, Xposed, Frida)
- 了解Android组件常见漏洞及修复
- 了解ProxyDroid、mitmproxy原理
- 熟悉安卓7以上https抓包，证书绑定相关
- 了解baksmali/smali, smali修改
- 了解常见x86和ARM指令与operand修改
- 了解apk签名原理, 了解scheme v2和v3

Web

- OWASP Top 10
- HTTP 、DNS原理及漏洞
- 简单的Web题（改包、shellshock、XSS、CGI）

二进制

- 了解shellcode, buffer overflow
- 简单的pwn题

开发

- Python, JavaScript用得最多, 也做过PyQt
- 做过Android应用、微信小程序

其他

- 英语：雅思7.0；日语：待考级
- 信息搜集：Censys、shodan、crt.sh、dns.bufferover.run ...
- 熟悉Git、MarkDown、 vscode remote