

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	技能
<div><div>梆梆安全 - 移动渗透实习生 2018.10 - 2019.04 前安全服务部 (北京)</div><div><ul style="list-style-type: none">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</div></div>	<div><div>移动渗透</div><div><ul style="list-style-type: none">Frida、Xposed、ProxyDroid、mitmproxy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</div></div>
<div><div>Royal Holloway - 授课型硕士 2019.09 - 2020.09 部分笔记, 预览成绩 (50及格, 非最终版):</div><div><ul style="list-style-type: none">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</div></div>	<div><div>Web</div><div><ul style="list-style-type: none">OWASP Top 10HTTP、DNS原理及漏洞简单的Web题 (改包、shellshock、XSS、CGI)</div></div>
<div><div>??? 世界唯一找到所有秘密宝藏的人</div><div><ul style="list-style-type: none">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</div></div>	<div><div>二进制</div><div><ul style="list-style-type: none">了解shellcode, buffer overflow简单的pwn题</div></div>
项目	其他
<div><div>Frider</div><div>研究生Final Project; Ant Design的Frida版XServer</div><div><ul style="list-style-type: none">+ APP基础信息+ 一键脱壳到PC+ 支持NativeFunction</div></div>	<div><div>开发</div><div><ul style="list-style-type: none">Python, JavaScript用得最多, 也做过PyQt做过Android应用、微信小程序</div></div>
	<div><div>其他</div><div><ul style="list-style-type: none">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</div></div>
近期计划	
<div><ul style="list-style-type: none">了解自动化测试改进Frider学AI</div>	

