Tide安全团队安全测试学习路线v1.2

说明	1、周报主要记录本周的项目实施情况、进度，本周学习的内容、进度等，试用期内每周学习内容请务必记录详细； 2、试用期内在完成相应学习周期后，公司会组织不定期考核，主要针对下面的学习内容相关资料，前六周学习内容为试用期必须掌握知识； 3、请根据每个学习项的重要程度自行安排学习任务，5星代表优先级和重要性最高； 4、下面的资料栏中标识为绿色的均可在网盘的“00学习路线相关资料”中找到,网盘中还有搜集的一些其他资料和工具，供参考； 网盘链接：https://pan.baidu.com/s/1XqtyKBB-lpG9tc5KyjSJOg 密码：2wmt 5、内部资料，禁止外传。

序号	知识分类	学习项	主要内容	参考资料	周期	重要程度	要求
1	引言	入门之前	了解你未来一段时间将要学习的内容	https://sosly.me/index.php/2017/07/17/studywebsec/ http://blog.knownsec.com/Knownsec_RD_Checklist/ https://www.zhihu.com/question/21606800/answer/22268855	一天	★★	评估一下你能否接受这份工作
2	基础知识	理论知识	了解web安全基本概念，熟悉SQL注入、上传、XSS、CSRF、逻辑漏洞等概念	1、《黑客攻防技术宝典Web实战篇_第2版》 2、熟悉公司《web安全测试用例》	一周	★★★★★	对测试用例中的常见漏洞比较熟悉，能简单描述其原理
3		信息搜集	在安全测试前期，搜集网站相关资料	自行百度相关资料和工具：子域名、敏感目录和文件、邮箱信息、C段、操作系统识别、CMS指纹、DNS信息、端口开放、社工库等		★★★	能对目标网站进行信息搜集
4	工具使用	Burpsuite	掌握proxy、repeater、intruder等功能	《burpsuite实战指南》	两周	★★★★★	熟练掌握burpsuite的使用
5		sqlmap	熟悉get、post型注入测试方法	1、《SQLmap用户手册》 2、http://www.vuln.cn/1992		★★★★★	掌握sqlmap并能进行注入测试
6		APPSCAN	扫描器配置、扫描、漏洞验证、报告导出	《AppScan入门指南》		★★★★	能对目标站点进行扫描并整理成结果记录单
7		AWVS	扫描器配置、使用、手工验证	《Awvs详细中文手册》		★★★	能对目标站点进行扫描并对漏洞进行验证
8		Kali系统	熟悉nessus、metasploit、hydra等用法	大学霸 Kali Linux 安全渗透教程		★★	熟悉kali中常见的工具
9	实战操作	web漏洞学习	掌握或熟悉各种漏洞原理、测试方法、加固等	1、《黑客攻防技术宝典—Web实战篇》 2、《白帽子讲Web安全》	三周	★★★★	对注入、上传、XSS等常规漏洞能进行手工挖掘
10		视频教程	根据视频教程详细学习各种漏洞利用方式	《渗透测试安全培训视频教程》		★★★★	熟悉常见漏洞测试方法
11		靶机搭建	利用DVWA、Webgoat、WebBug等搭建测试环境	DVWA参考资料： http://www.freebuf.com/author/lonehand		★★★★★	搭建环境实际测试并记录
12		靶机实战	针对公司靶机进行测试并完成渗透测试报告	公司测试环境http://192.168.1.11		★★★★★	能发现80%的漏洞且报告规范
13		web漏洞学习	深入web漏洞原理、bypass技巧、手动测试技巧	1、《SQL注入攻击与防御 第2版》 2、《Web前端黑客技术揭秘》		★★★★	能进行手工测试，掌握一定绕过WAF的技巧

14	深度学习	移动端检测	APP逆向、篡改、抓包分析等	《Android软件安全与逆向分析》	常态	★★★★	能根据测试用例完成最基础的检测
15		内网渗透	shell反弹、提权、端口转发、域渗透等	1、《Metasploit渗透测试魔鬼训练营》 2、《黑客攻防技术宝典：系统实战篇》		★★★	熟悉内网渗透常用命令和工具
16		Python编程	了解语法、正则、文件、网络等常用库	推荐《Python核心编程》		★★★	能写简单小工具或爬虫
17	广度学习	代码审计	熟悉常用代码审计工具，了解java和php中常见安全函数	1、《代码审计-企业级Web代码安全架构》 2、《代码审计-深入挖掘及代码防御》视频教程	常态	★★	能根据审计报告进行人工复核
18		应急响应	熟悉命令、日志、思路、取证、溯源、逆向等	《Windows取证分析》		★★	能进行应急处理和木马分析
19		逆向分析	熟悉汇编、反编译、动态调试、静态分析	1、《IDA PRO权威指南第二版》 2、《逆向工程核心原理》		★★	能进行程序逆向调试和动态分析
20		CTF练习	了解其中的WEB漏洞、密码学、网络和取证等	http://www.shiyanbar.com/ctf/ https://www.ichunqiu.com/racing http://www.hetianlab.com/CTFrace.html		★★	参加线上或线下比赛
21		安全开发	php编程、java编程等	推荐《PHP与MySQL程序设计（第4版）》		★★	基本语法学习，常见函数
22	其他	关注安全圈动态	最新漏洞、安全事件与技术文章	SecWiki、FreeBuf、安全客、i春秋社区等资讯平台	常态	★★	时刻关注最前沿技术
23		查缺补漏	温习安全技能树	https://zhuanlan.zhihu.com/p/27362112		★★	了解不足