安全小课堂第九十期【局外人的白帽子之路】

京东安全应急响应中心 4月2日

JSRC从2013年成立到现在，白帽师傅和我们共同经历了5个春秋，在这些不长不短的日子里，JSRC积累了一箩筐的白帽子成长故事。这些白帽子故事，有些感人，有些励志，也有些坎坷。看上去，白帽子们的日子很美好，每个重要节日都能收到JSRC送的节日礼品，能从JSRC挖掘漏洞换取苹果三件套，一年能从JSRC兑换多达十几万的礼品卡。

但JSRC知道，每一个白帽子走到今天都不容易，知道他们的付出，知道他们的心酸，知道他们一直在努力学习。

JSRC **安全小课堂第九十期**，邀请到**局外人**师傅为大家分享自己的白帽子之路。同时感谢白帽子们的精彩讨论。

大学是信息安全专业吗？还是仅仅是因为CTF爱好者而走上信安之路呢？

京安小妹

局外人：

我大学不是信安专业，学校里没有这个专业，我是测控专业的，不是那种扛着三脚架的测绘，是那种修电饭锅的专业。当初是看到别人拿站很酷，后来被麦香学长指引开始接触CTF，到后来被团队的师傅们带着打各种CTF，慢慢的对信安感兴趣，也想往这个方面发展，就走上了信安之路。

讲师

我们群里也有不少朋友玩打CTF的，能不能分享一下你对CTF和挖洞的观点 京安小妹

局外人：

现在国内有很多CTF比赛，参加CTF比赛不仅可以提升自己的能力，也可以证明自己的实力。在大学里，参加CTF获得奖项还可以去加分的，并且奖金也很诱人，参加CTF还可以捞一点茶水钱。除此之外还可以认识很多大佬，每场CTF都会让每个人有收获，发现自己能力的缺失点。很多人觉得CTF为了比赛而各种脑洞，我们在挖洞的时候不是也有很多独特的脑洞么，CTF玩的好的大佬，一般挖洞都不会差。

讲师

你觉得在你的成长路上有什么主要的难点，你都是如何突破的？

京安小妹

局外人：

我在成长的道路上遇到的难点非常多，也感谢帮助我解决难题的师傅。个人难点第一是开发能力太弱，大佬们都用半自动化挖洞了，这也是我挖洞效率低下的原因，目前就是努力提高开发的能力；第二是目前挖洞进入了迷茫和瓶颈期，四处寻找大佬的学习姿势，请大佬们多多指教。

讲师

挖洞过程中有哪些小tips可以跟大家分享的?

京安小妹

局外人：

那我说说自己的一点经验吧，第一：挖洞要坚持，挖洞开始难免会遇到挖不到漏洞的情况，多去乌云、论坛、博客等看大佬挖洞的姿势，一定会有收获。第二：信息收集很关键，子域名，IP段等，第三：细心，多测试别人觉得没问题的地方，多测试逻辑漏洞。

讲师

作为JSRC的新朋友，觉得在JSRC挖洞有什么开心或是不满意的?

京安小妹

局外人：

做为刚入JSRC的新人，我觉得JSRC是一个非常活跃的SRC，一个大佬非常多的SRC，一个良心的SRC，活动都是炒鸡厉害的。在JSRC的一个多月里，个人觉得在JSRC挖洞是比较开心的，不仅认识了很多大佬，在挖洞过程中，尤其是给运营大佬们点赞，每次遇到问题，找京东小妹后，小妹站在白帽子的角度维护白帽子的利益，任何问题都会得到专门的回复。这个月的活动也是很刺激，大佬们都纷纷发力，让我看到了自己的不足，还是要继续努力。满意还是非常满意的，有一点点小建议，新提交平台已经测试了希望可以尽快上线，审核的速度可以稍微提高一点点。

讲师

是滴是滴！**漏洞有问题有异议**请找小妹~我们的**官网2.0马上就会跟大家见面啦**，希望大家稀饭~

京安小妹

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，点击菜单栏进入“安全小课堂”即可浏览。

最后，广告时间，京东安全招人，安全开发、运营、风控、安全研究等多个职位虚位以待，招聘内容具体信息请扫描二维码了解。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心