安全小课堂第八十三期【v清风的白帽子之路】

原创：京东安全 京东安全应急响应中心 1月29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 **安全小课堂第八十三期**，邀请到**v清风**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。

你接触SRC的时间也不久哈，除了能挖洞赚外快之外，你觉得SRC这种模式还有哪些地方吸引你的？

京安小妹

v清风：

一方面是src的各种福利丰富，逢年过节送礼物啥的，家里人收到各个厂家送的礼物都是蛮开心的。毕竟我当初是听说src送月饼才想挖漏洞的，囧
另一方面是遇到了一群可爱的人，src提供了一个白帽子交流学习的平台，让我有机会能够跟大家接触，交流学习。
还有我目前接触的src运营都超nice的，为白帽子争取福利，忙里忙外~
例如：我们可耐的jd小妹

讲师

大多数人在初接触一个平台的时候可能会有一个适应期，你在初接触SRC挖洞的时候适应期大概是多久，你是怎样迅速熟悉这种挖洞模式的？

京安小妹

v清风：

这个的话根据每个人实际情况时间不一样
我个人情况是经历有三个阶段：
第一个阶段是从零到一即第一个漏洞被确认，一开始嘛什么东西都当作漏洞交上去，结果当然是被忽略和驳回，这是挺沮丧和尴尬的。后来就会看一些wuyun案例进行学习，然后就是坚持提交，突然发现有一天被确认了，当时还是很高兴的，虽然漏洞危害不大，但是也算一种认可，一点点进步。
第二个阶段是第一个高危，觉得找到了src高危才会有真正意义上“找到漏洞”的感觉，比如说：可以影响到用户和服务器的一些漏洞，突然之间就像开了上帝视角。拥有所谓“超能力”的人更容易滥用超能力。例如：能够登录任意用户账户。这个时候就需要管住自己内心的小恶魔，不做损害企业和用户的事情。
第三个阶段是所谓的瓶颈期。就是会感觉“自己挖不到漏洞”的阶段，会觉得：自己投入了这么多时间怎么都还是什么都找不到了，郁闷的是又看见别人的分数刷的又超高，囧。
这个时候做了自我反省，发现自己掌握知识的广度和深度都不够，自己的思路太僵硬。这些地方都有待完善。我自己的解决办法是：一方面自己回炉重造，另一方面多跟大佬们交流，向他们学习新的姿势。当能够突破时候就会发现柳暗花明又一村。

讲师

你是如何在半年时间之内就在JSRC平台迅速崛起的呢，有什么秘诀吗？

京安小妹

v清风：

首先感觉我距离崛起还是差距很远，毕竟jsrc大牛太多，比不过比不过。
至于我的话，只能说是多一些耐心多花一些时间吧，毕竟笨鸟先飞~
吾尝终日而思，不如须臾之所学也，站在巨人的肩膀上，多看前辈们的文章，关注大佬们的blog。
至于具体操作的话：主要还是资产范围收集，对业务的熟悉程度还有对漏洞的理解，这三个方向都需要花时间和精力去做。当然最重要的是贵在学习和坚持
另外提到对于漏洞的理解。一直都说挖漏洞挖漏洞，实际上呢，挖漏洞是挖掘所有能影响业务的问题，将这些问题归纳就成了我们常见的这些sql注入，XSS

讲师

前段时间有个很火的词“佛系白帽”，大概就是描述白帽子提交漏洞之后会遇到的问题，包括忽略啊审核评级与自我评级不一致这种，你是怎样看待并处理这种情况的呢？

京安小妹

v清风：

首先我觉得漏洞审核难免会有争议。拿我个人经历来说：最开始交了一个漏洞，我是满心欢喜，每隔几小时就登录src看一下审核状态，结果等到花儿都谢了，最后一看。一般就是“忽略”或者“重复，已有白帽子提交此问题”，当时我也是觉得有些愤愤不平，自己花了这么长时间提交的漏洞等了半天怎么就这样一个结果？！

但是逐渐了解之后才发现，我们白帽子提交一个漏洞并不是审核小哥一看存在这个漏洞就立刻确认，而是需要审核小哥先初步确认，然后需要业务部门核实，如果是高危和严重甚至需要主管最终确认，我们看到的在页面上显示出来的核实原来是src通过多方协商之后的结果。

我当然也遇到漏洞评级有争议的时候，一般是高危和严重之间有争议或者低危和忽略之间有争议，一个是对于漏洞危害程度大小的争议，一个是对于是否认可存在漏洞有隐患的争议
。遇到这种情况一般都会找运营小姐姐沟通，跟她说明情况，然后等待src内部反馈结果。

其实现在src这么多，如果觉得不满意完全可以换一家，src根本刷不完，只能说选择最适合自己的src。

讲师

上次峰会领奖没发表获奖感言，现在采访一下当你拿到**5位数**的奖金时心里啥感受啊鸡冻不老铁

京安小妹

v清风：

首先是非常非常感谢jsrc让我有机会能参加jd安全峰会，对我来说完全是惊喜，就像是突然告诉我上个月不经意间买的一个彩票中奖啦。
因为自己的分数跟其他几位师傅之间差距还是很大的，当时jd小妹告诉我时候确实炒鸡开熏。觉得主要还是运气比较好，自己的情况跟这个奖比较贴近，或许这个就是猿粪吧哈哈哈

讲师

对白帽子以及想要成为白帽子的小伙伴有什么好的建议？

京安小妹

v清风：

1、调控自我学习和挖洞时间。多撸代码，不会开发的黑阔就像不会游泳的海盗。我感受到的巨大差距在于，我还在用木剑一个个打怪的时候，大佬们已经远控机器人自动化地使用激光剑批量刷怪了
2、扩展自己知识边界。多归纳总结，完成属于自己的思维导图
3、锻炼身体。身体是革命本钱，每周坚持锻炼，才能让自己更加持久，头脑保持清醒，在信息安全这条漫长道路上走的更远~路漫漫其修远兮
大概就是酱紫啦

讲师

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