安全小课堂第八十期【Sven的白帽子之路】

原创：京东安全 京东安全应急响应中心 2017-12-04

JSRC从2013年成立到现在，白帽师傅和我们共同经历了四五个春秋，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 **安全小课堂第八十期**，邀请到**Sven**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。

你是如何定义白帽子以及白帽子这个群体的？

京安小妹

Sven：

安全能力是双刃剑，只是看大家用他来做什么，这几年里见过最后很成功的安全人员，也见过走进黑暗的。白之道，在于出奇而守正，如果不能出奇那能力是无法提高的；如果不能守正，那能力越强，对社会危害越大，许玉玉事件还历历在目，**没有想要保护的人，枪也就成了无用的玩具**。总体来说，荣耀与压力并存，是成就自己的一条打怪升级之路，但也需要注意不要迷失了方向，成就时不浮躁，失落时不放弃。

讲师

在JSRC所向披靡的挖洞诀窍是什么？

京安小妹

Sven：

第一是行动，第二是坚持，第三是出奇（少有人走的路）。学会一个道理，就去实践一下，不贪多，做了大于一切。最初的时候最难，因为很多漏洞可能会被拒绝，因为不熟悉什么样的漏洞是在接收范围，需要一段时间的磨合，坚持的同时不知不觉的就会有能力的提升，速度不是很明显但是厚积薄发。这个阶段非常的重要，坚持的阶段也是一个了解业务与提升能力的最佳时机。

讲师

你在白帽子成长之路上是否有遇到过瓶颈，是怎么解决的？

京安小妹

Sven：

第一个漏洞、第一个系统以及第一个严重。首先，在没有被确认第一个漏洞之前，一直被打击，这个时间很容易放弃，坚持到第一个漏洞被确认，是一个很大的成功。有时候会挖到感觉比较高危的问题，但是对业务来说其实不重要的，这个需要一次重新认知。坚持的同时，也是为了积累更多的经验。分享一个我之前写的关于学习与坚持的知识：

讲师

作为一个有着数年挖洞经验的白帽子，你对白帽子这个群体的未来职业发展有什么想法或者建议？

京安小妹

Sven：

最初的话，成为白帽子并拿到好的排名，是一条光环耀眼的成功之路，很多人因此直接进了大公司。在之前做安全的学历普遍都不高，如果没有这个光环，大公司是不会开特例的。所以没有名气之前在JSRC好好的坚持，努力打出名气来；而已经有一定名气的同学，就要好好的策划未来的方向了。这是我有点积累之后写的一个文：
http://mp.weixin.qq.com/s/Cj7ZG5xPStJtHKJ9F1Jqxw
大体是两个方向，一个是继续深入研究技术，一个是转向带队。特别注意的是，在光环最亮的时候进行选择是最好的，职业规划一定要做好，在最适当的时机进行选择，光环这东西过期作废。进行新的方向之后，放下之前的一切，静心努力前行，再次努力积累，等待第二次的爆发。

讲师

作为一个从15年就开始在JSRC提洞并且活跃至今的老朋友，这一路来你对白帽子对JSRC有什么评价或者寄语吗？

京安小妹

Sven：

对白帽子：未来是你们的，我的选择一条横向之路。每个人都是一个奇迹，每一次沟通都是一次修行。选择之后，坚定信念，永不后悔。对JSRC：JSRC近二年多的安全水平进步很快，是非常值得肯定的。作为守护千万人购物安全的团队，任重道远。同时我也是购物者之一，代表千万购物者，为JSRC点赞。

讲师

白帽子提问：出奇怎么理解？是不是可以理解为“运气”？

Sven：我个人的理解是进入别人不常去的功能，记得我去过一个供应商管理系统，提交了一大波的漏洞。还有就是，去大家都感觉没有问题的地方，之前提前过一个非常显眼的位置的竞争条件问题。详细的了解业务，也是非常有必要的，长时间坚持在一个SRC，会形成漏洞的直觉。

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，回复“安全小课堂”或者点击阅读原文进行查看。

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