

安全小课堂第六十六期【Mr.Chou的白帽子之路】

京东安全应急响应中心 2017-07-21

从2013年成立到现在，JSRC在白帽子的陪伴下已经走过了四五个春秋，在这说不长也不短的日子里，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。

现在开始JSRC会将白帽子故事，通过安全小课堂分享给大家。

安全小课堂第六十六期，JSRC邀请了连续两年获得JSRC年度第一白帽子的Mr.Chou师傅，来和大家分享他成为白帽子的故事，和大家分享他是如何学习，如何在JSRC解锁各种成就的故事。



获得2016年JSRC年度排名第一白帽子有什么诀窍吗？

京安小妹



信息收集并将信息关联起来，比如域名、ip、前端表单字段、cookie字段、**单点登录关系**、加密方式等等。

站在产品经理角度考虑业务逻辑、系统架构、功能需求等，了解目标系统架构。

站在开发者角度考虑功能实现，业务关系等，比如**开发测试为了方便写的一些隐藏功能**。

讲师：Mr.Chou



当初为什么会选择成为一名白帽子？

京安小妹



没有特意成为一名白帽子，从事安全很多年，一直很少在各大平台提交漏洞。京东安全是个契机，因为京东买东西配送够快，经常在京东买东西，偶然机会发现漏洞。又听朋友说京东有src，尝试提交后就一发不可收拾。

讲师： Mr.Chou



在和JSRC一起成长的过程中有什么影响深刻的事吗？

京安小妹



深刻影响是，JSRC的人很敬业，并且个个都是技术大咖，很公平公正，你们内部氛围也非常不错。
如有需求都能尽量满足我们白帽子，非常不错的。
逢年过节还有礼物。

讲师： Mr.Chou



你认为学习技术主要难点有哪些？如何突破？

京安小妹



个人感觉选定了方向持之以恒，循序渐进肯定没问题。

讲师： Mr.Chou



能否说一下对JSRC的印象以及建议？

京安小妹



圈子里很多朋友都在给各大src提漏洞，也听了很多白帽子对各大src漏洞定级的抱怨，我目前坚持提交的是JSRC，个人感觉JSRC漏洞定级蛮公正的，真心觉得对白帽子也比较大方，也推荐了很多朋友给JSRC提漏洞，取得的成绩也是非常不错的，JSRC真心不错。

建议增加现金奖励。

建议可以授权给部分白帽子对京东进行全面的安全评估，不限制手段，也就是apt那样。

讲师：Mr.Chou



对白帽子以及想要成为白帽子的小伙伴有什么建议？

京安小妹



成为一名白帽子很容易，随便学习一些攻击方法就能做漏洞挖掘，现在很多新入门的白帽子都是web渗透方向，知识面相对比较薄弱，**不要把精力都花在web攻击上，web漏洞挖掘成本只会越来越高。**

讲师：Mr.Chou

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](#)

[阅读原文](#)