安全小课堂第124期【Reckfulyx的白帽子之路】

京东安全应急响应中心 2018-12-24

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124期**，邀请到**Reckfulyx**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。

成为一名白帽子的心路历程？

京安小妹

Reckfulyx：

我是16年10月份左右才开始接触网络安全的，对于这个行业来讲，其实我也算是个萌新了，而且真正的零基础入门。。所以感觉入门=入坑这句话确实非常有道理。。开始啥都不会，跑个sqlmap就感觉很黑客，然后随着自己“越陷越深”，越来越感觉自己知识不够用，然后发现很多大佬用python写工具，自动化渗透、域名监控等，就开始学习python。。折腾了一段之后，又看到沦沦各种手工绕waf的注入十分骚气，于是又开始接触数据库。最后的结果是。。。睡的越来越晚，效率越来越差。。。。所以现在开始养生学习法，白帽子，就要爱自己多一点~

一句话概括下，我还是很菜，但是明白了如何在学习与挖洞与生活之间自如切换。

在成长中印象最深刻的事情有哪些?

京安小妹

Reckfulyx:

我第一次提交src漏洞就是在jsrc，提交了9个漏洞，前八个都被忽略了，第九个给了低危。

然后三月份加入网络尖刀团队，认识了一系列真正大佬，比如@沦沦 @黑色键盘。

后来又收到团队内部人的一些影响 比如我的好友@Cy，他经常挖掘一些国外漏洞。然后我学习了一下流程与姿势，今年陆陆续续挖到了几个国外大厂的漏洞

讲师

挖掘漏洞过程中遇到过什么技术难点吗?

京安小妹

Reckfulyx:

其实难点有很多，而且每个人的见解不同，我个人认为难点其实也是最基础的一点---信息收集。在相同的技术水平下，信息收集的程度可以完全影响到最终的结果。

我觉得这个东西其实真的是重中之重，比如各大src的各种平台，很多都需要反复的权限或者账号，你如果进去了，那岂不是...

我平时挖掘漏洞的时候也是花大量时间在这个上面，如果能收集到一些别人不注意或者忽略掉的细节，你就赢了~

讲师

第一次在JSRC提交漏洞时是什么感想?

京安小妹

Reckfulyx:

当时真的很兴奋 我觉得第一次提交是个云平台的弱口令 然后被忽略了

第二个是反射xss 重复了

第九个通过了 当时觉得 太幸福了... 因为这是我src中的第一个有效漏洞

然后随着时间推移，开始慢慢的有了中危 高危

总结一下感想，就是要坚持，一定要坚持，而且不到最后一秒，绝对不能高兴，因为你永远想不到这个漏洞被忽略的理由是什么 嘿嘿

讲师

对JSRC有什么建议或者想说的吗

京安小妹

Reckfulyx:

1.积分兑换商城更新商品

2.JSRC官网手机端优化

讲师

对于将要踏入信息安全行业的新朋友们提一些建议?

京安小妹

Reckfulyx：

我觉得新朋友分为两类吧，一种是相关专业的或者是程序员 另一种是跟我一样的萌新。

萌新的话 多接触点漏洞类型，丰富一下自己的知识库。 始终让自己保持着学习的激情与乐趣。然后用兴趣使自己能学习到开发及数据库相关技术这类技术能让自己在src的道路上走的更远

如果本来是程序员的话，直接丰富自己的姿势就好了～

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。

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