安全小课堂第114期【Vulkey_Chen的白帽子之路】

京东安全应急响应中心 10月15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114期**，邀请到**Vulkey_Chen**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。

分享一下你的成长历程吧（从如何接触信息安全，如何对它产生兴趣，如何进行深入研究，到为何成为一名白帽子的）

京安小妹

Vulkey_Chen：

我的起点其实很普通：

小时候喜欢打FPS射击类游戏，技术不够，“邪门歪道”来凑，于是走上了寻找外挂之路。偶然间加入一个外挂交流群，下载了一个软件，软件标题是“CF遁地+飞天+穿墙+自瞄.exe”，年少无知，感觉自己捡到了宝贝，欣喜若狂，等待下载完毕，带有仪式感的点开，熟悉的Windows关机声响起，然后重启了电脑。当打开的时候，我慌了，电脑的用户名变成了“解锁+Qxxxxxx”。后来被我爸教训了一顿之后，他一下子就解锁了电脑。

经历的事情多少也算精彩和幸运：

- 抓鸡

后来多多少少也自己学了点东西，自己也学会做锁机的软件了，开始“纵横”，后来跟一些网友聊天得知“抓鸡”，花了当时唯一的50块钱大洋买了教程，学了起来，当学会之后，才发现这是免费教程，被骗了，然而自己只懂理论却没成功过。

- 钻阔

接触到了很多的网友，也加入了所谓的“黑客团队”，在里面聊天吹牛，知道了原来体验一个人QQ价值的地方在于QQ钻多不多，于是踏上了刷钻的不归路，曾经也是QQ钻全开的小伙子哈哈。

- 渗透

最开始接触渗透的时候是13年，那时候到处的“啊D、明小子，南方精良批量教程”，用这几招也曾“到处留名”。后来荒废了一段时间，“潜心”学了一段时间编程（PHP），懂了点皮毛之后学习并熟练使用各种脚本，14年偶然间得知“360库带计划”，便开始了人生第一次的漏洞挖掘之路，那时候任何一款工具都可以“日”遍各种企业，漫游各种内网。后不甘现状，也因现实所迫将挖洞放下了一段时间，16年年初才重见“挖洞”天日，那时候圈内已经变化太多，SRC、漏洞平台也兴旺发达，漏洞赏金也越来越高，花了一年时间重新学习，从脚本编写到漏洞原理的系统化学习，后有幸跟随启蒙老师加入米斯特安全团队，与团队核心交流，技术日益增长。

虽然是一名年轻的白帽子，但是从初中就开始接触信息安全，你认为学习技术最快的成长方式什么？

京安小妹

Vulkey_Chen：

“实战”是提升最快的捷径，有条件的情况下尽量多“实战”，这里的“实战”不是指拿你已会的姿势，多尝试多思考，带着问题去“实战”，抛弃被固化的挖掘思维，既然是做黑盒测试，那么就要知道没有什么是不可能的。

“基础”是学习最重要的一环，大概有很多人根本不知道自己挖的这个漏洞原理是什么，何谓原理？后端代码如何处理，为什么这样处理，这样处理为什么会有漏洞？其实就是所谓的处理逻辑，“基础”要打好。

“基础”+“实战”=“SzS”

“SzS”=骚姿势，有足够的基础知识，然后抱着学习的心态去实战，去尝试和突破，就会有新的姿势能诞生，而这种姿势往往是很“骚”的。

讲师

信息安全求知的道路可谓是路漫漫其修远兮，探索路上难免碰到挫折，你一般是怎么克服这些困难寻求到突破的

京安小妹

Vulkey_Chen：
静下心沉住气。
每个人都会有瓶颈，这个瓶颈来自“哎，挖不到漏洞，为什么别的师傅能挖到那么多？”，我也这样抱怨过，为什么别人可以，而我不行？是我哪里不够？这时候我会去问“师傅”，大多得到的都是一些“道理我都懂”的话语。其实也是，人家凭什么教你自己吃饭的本事呢？那么自己怎么突破这个瓶颈？我建议的是多“看”，
多“想”，多“动”，既然别人不告诉你，那么你就自己去探究跟别人差了什么。

我会经常问自己如下的问题：
“乌云公开漏洞库这么多漏洞姿势你都知道吗？”
“你都知道，那么你都挖到过吗？”
“你都挖到过，那么你能知道原理吗？”
“你知道了原理，你能熟练掌握吗？”
“你能熟练掌握，你能教给别人吗？”

有一句话叫“最好的学习是教会别人”，对这门技术、姿势是如何理解的，写成文章录成视频，让别人也能懂，“分享”很重要，只有“分享”了，才能引起讨论交流，通过交流也会提升。

讲师

作为经常在各大SRC刷榜的师傅，能跟大家分享一下：如何才能在SRC既赚到钱又提升自己技能

京安小妹

Vulkey_Chen：
师傅算不上，这个在问题2也说了，主要是怎么去做，这很重要。

讲师

有没有什么自己的挖洞小诀窍跟大家分享一下

京安小妹

Vulkey_Chen：
我是一个数据控，我喜欢收集数据，在做SRC挖掘的时候我会有一个表格，这个**表格存储了如下的信息**：
域名、标题、容器/中间件、程序、敏感地址、备注
为什么收集，多想想就知道了，例如一个新漏洞爆出，你能快速的找到src存在问题的资产，又是一堆漏洞的产出~
同时我也会做一个**漏洞库**，这里的漏洞库是一些鸡肋、低危的漏洞记录，不提交留着以后打组合拳也可以的~

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。

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