安全小课堂第九十八期【mmmark的白帽子之路】

京东安全应急响应中心 6月4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 **安全小课堂第九十八期**，邀请到**mmmark**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。

第一次与“网络安全”结缘是什么时候（偶然性 引起共鸣）

京安小妹

mmmark：

小学的时候开始接触计算机，从红警到魔兽，从石器时代到魔兽世界，可以说是个深度的游戏网瘾少年。第一次和安全结缘还记忆深刻，当时是自己家电脑中了一个CNNIC的蓝屏病毒，那个时候就开始各种查资料，解决方式，用过超级兔子，卡巴斯基，金山毒霸，瑞星，还是解决不了，最后只有重装系统才解决。

讲师

传闻你曾与“网络安全”两次擦肩而过，能不能讲一讲其中的故事（趣味性）

京安小妹

mmmark:

因为那一次中病毒的经历，我第一次对“黑客”，“病毒”产生了兴趣。当时也了解过什么是肉鸡，灰鸽子，冰河木马之类的。还看过一些抓鸡教程，不过看着看着又中毒了，23333333.当时是没有什么计算机基础和网络基础的，更别谈编程之类的了，一无所知。再加上魔兽世界这款游戏的到来，很快就放弃了学习安全，投入到游戏世界中，这是第一次与安全擦肩而过。大学开始学习计算机专业，突然有一天魔兽世界的账号一直被盗，什么密保卡，改密码，改邮箱密码，都不起作用。我又开始重新关注安全，不过很快我又爱上了街舞，第二次与安全擦肩而过。

讲师

如何进入安全行业，成为一名安全从业者，又是怎样成为一名白帽子的

京安小妹

mmmark:

15年底终于开始投身安全行业，很幸运当时看到了Freebuf，从关注文章，到看书学习，看教学视频，很荣幸后来加入了斗象科技，成为了我安全行业的领路人。说起来有太多的人值得感谢，有太多的同事给予我帮助和学习的机会，在斗象的一年半我储备了一些安全基础。17年开始白帽之旅，很幸运遇到了我的大师傅（低调不愿意透露ID），他真的帮了我太多，我们一起挖各大SRC，一起讨论漏洞，一起讨论绕过，一起思考如何更有效率的挖洞。也是他介绍我参加17年的一次JSRC双倍活动，加入了JSRC。同时17年底加入了一家金融甲方公司，开始全面的接触安全体系，一个人的安全部有苦有甜（听说有个群，求拉）。

你为许多家 SRC都提交过漏洞，也都取得过相当不错的成绩，在JSRC上次的沙巴行活动中不仅以总积分第二的成绩赢得沙巴游大奖，还赢得第二时段加码活动的2.5倍积分奖励，在这里能不能跟大家分享一下，你是怎么做到的？（偏个人技巧 可附实例 个人建议可以讲一讲你在挖到第一个高危时的情形 这个我都记得非常清楚哈哈 怎样经过破冰期）

京安小妹

mmmark：

在技术方面我还处于学习和强化阶段，每一次挖SRC都是一个学习和强化的过程。当时挖到第一个高危漏洞的时候，因为技术比较菜，对某些漏洞类型理解不深，最开始误以为是这个漏洞类型。然后就被忽略了，然后我就不服气，继续研究，查资料，请教师父，在师父的帮助下，我才准确的判断了漏洞类型，然后转换思路，重新提交。还有一个案例我印象也比较深，我本地复现成功了，审核有一些异议给驳回了，然后我继续不服气，又是一顿查资料，请教师父，最后找到了绕过方式。这两个漏洞可以说是我参加这次活动最大的收获，完善和强化我对一些漏洞的理解。我是属于努力型选手，经常以数量取胜。我会关注每一个大大小小的漏洞，常见的漏洞类型我都会去学习，认识一些白帽子小伙伴，他们只会挖掘某一种类擅长的漏洞，或者只去挖某一种类的漏洞。这样的话会错过很多漏洞，数量方面就无法战胜我啦. 说到这个有些漏洞会用同一种防御方式，比如URL跳转，CSRF验证Referer，都是属于用正则对URL进行验证。虽然跳转和CSRF通常都是低危漏洞，但是在学习绕过姿势的过程中，其实是对这一种防御姿势的理解。当遇到SSRF也是用这一种防御方式的时候就是高危漏洞了。除了擅长的漏洞类型全面以外，资产收集也是非常重要的，这里我还是用的比较“土味”的老工具，在大师傅的帮助下，我们对一些老工具进行了简单的改造升级，改造成更适合自己思路的升级版“土味”工具。最后就是付出大量时间和精力了。

讲师

前面你也有提过，现在一家金融甲方工作，“一个人的安全部”这样的经历对你的白帽子之路有什么影响或帮助吗，有没有引发你的一些思考？

京安小妹

mmmark：

一个人的安全部可以帮助我拓宽安全的知识面，我最开始只会web应用安全，只会挖web漏洞。但是这在甲方是远远不够的，很喜欢猪猪侠前辈的一句话，做安全应该是有很多基本版，一项或几项长版。一个人的安全部就是帮助我去完善更多的基本板。同时白帽经历，会反补甲方，我们在挖漏洞的时候会遇到很多业务场景，防御方式，可以从一些大厂那里发现他们一些很有意思的解决方案，防御手段，体会到攻防对抗。把一些好的思路学过来，用来解决企业的安全问题。

：

讲师

对JSRC有什么意见、建议（这个随便说 好的坏的都行）

京安小妹

mmmark：

1.开启现金兑换。

2.白帽子礼品关怀。

：

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