安全小课堂第130期【ch1st的白帽子之路】

京东安全应急响应中心 2月25日

JSRC从2013年成立到现在，白帽师傅和我们共同经历了6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130期**，邀请到**ch1st**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。

和大家分享你挖掘JSRC的心灵路程吧

京安小妹

ch1st:

我是在18年7月底的时候开始与各位师傅开始并肩在JSRC上战斗。还记得那个阳光明媚的下午，我跟清风表锅还@清风 有十八哥@jkwolf18 一起约定好去2018年的京东白帽子大会，因为先前我们三在武汉匆匆见了一面，感觉到激情未尽。hhhh～

当时的我进入JSRC的时候一脸懵逼，师傅们或许会有同感，面对一个大目标无从下手，而且还会有种感觉，JSRC都这么多师傅在挖了，肯定自己也挖不到什么漏洞了。想到这个时候我就想起来在补天跟我的伙伴们刷专属SRC的时候，因为当时专属SRC很久没上新的了，所以自己也很迷茫，挖不动咋子搞。

后来我的队友@伤心的金毛七哥对我说了一句话让我一直记到了现在，也是我现在每次挖不到漏洞时候的勉励。就是“你挖不到的原因就是你很浮躁，你要静

下心来，要静，要细”。

所以呢，对于JSRC的第一个漏洞我找了一下午，找到了一个存储型XSS，还获得cookie，当时我去溯源的时候发现自己插入的payload在页面上并没有触发，但是确确实实的拿到了后台cookie，这个漏洞我记忆犹新，开始了我的挖掘漏洞之旅。

可是好景不长，在之后的半个月里面，我的漏洞的通过率就越来越低了，漏洞原因重复重复，像极了爱情。

后来转眼一想，这么搞不是个事情，然后自己开始把自己提交过的漏洞仔细看了一下，发现自己挖掘的都是大伙能挖掘到，而且这么点分离我跟两位老哥定的目标简直是毫无希望，后来我就开始转变方向，不再把一个站点一看而过，而是把站点的每个业务的功能点尽可能的看全，burp一开，铁头娃上线。

刚开始的两三天还是发现没有挖到漏洞，但是慢慢的坚持了一段时间，发现自己也能慢慢的把漏洞的质量提高了。

后来，我终于挖到了第一个高危，终于破冰了，终于能站上JSRC的月榜了，这毫无疑问是对我最大的一个激励。然后就开始越战越勇，挖不动了就睡一觉明天挖。在JSRC上，我认识了很多师傅，这些师傅给予了我很多的帮助。

毫无疑问，在我为JSRC上提交漏洞的这段时间，冷静仔细是我一贯秉承的原则。要是今天挖不到了，就感觉很烦的时候，自己就去干其他的事情，等心情好的时候在继续来搞。

将自己的提交的漏洞看了一遍，发现提交的最多的类型还是逻辑类型的漏洞，常规的注入呀命令执行呀啥的少之又少，可能是每个师傅擅长的手法不同，而我偏偏热衷于逻辑漏洞类型的挖掘，所以对于挖掘SRC自己也有一套自己的准则了。先试着怼某一种类型的漏洞去对收集的资产快速进行挖掘，然后若是挖掘不到，就开始每一个域名每一个域名的去看，了解这个站的业务是干嘛的，有哪些地方会出现用户与后端交互的地方，再挨个的去进行测试。这样仔细的轮下来，是会有收获的。

而且自己对于自己也是经常性的阿Q精神安慰自己，例如只找到了一个反射型XSS，虽然是低危，但是自己就感觉今天有收获了。即使这一天没有在此挖到漏洞也不会很气馁。当然了，我也经常对自己立flag，说自己的勋章18年一定要有个钻石勋章。还好，达成了~

所以自己这一路发现在JSRC上也有挖不到洞的焦虑尤其是月底不在榜单的时候尤为甚，也有挖到高危时候的喜悦。

所以呢，很感谢JSRC这个平台让自己有一展拳脚的机会，还能认识这么多志同道合的师傅，实乃一大幸。

那你认为学习技术最快的成长方式是什么呢?

京安小妹

ch1st:

自己会每天去sec-wiki.com，wiki.ioin.in，freebuf，去看一下最新的安全文章和新闻，去了解自己与别人的差距，然后遇到了文章的好tips，自己也会去记笔记，归纳总结。

感觉开发的能力尤为重要，自己也是学习Java出来的。所以会对漏洞的原理会理解的更加深刻，现在自己会每天去cve.mitre.org去搜索自己感兴趣的CVE，然后尝试着自己去复现，一步一步跟着Debug，这样自己对于触发点的来龙去脉理解的会更深刻。

还有最重要的，就是组建自己的一个小圈子，多交点跟自己水平不相上下的朋友，时不时的去讨论技术问题，大部分的师傅们对于技术上面的活是相当认真的，毕竟安全这块领域都是大家擅长的领域，我自己也很庆幸自己能在网上结交到这么多师傅，共同努力，一起学习。

再一个，如果有条件的话，尽量去加入一个团队，特别是对于学生党而言，像我这种现实中只有我一个搞安全，接触不到其他的搞安全的师傅来说这点尤为重要。加入一个团队，你会碰到形形色色的人，你们会一起努力为一个目标奋斗，这其中的斗志或许你这辈子都忘不了，然后分享最新的CVE，碰到难题有伙伴们给你去解决。如果没有环境，一定要自己去构建环境，不然就会一直原地踏步，我曾经在这个阶段踏了好几年，对于漏洞的挖掘一直都是懵懵懂懂的状态，挖不到漏洞的时候自己还会去百度谷歌搜索"如何挖掘到SRC漏洞"此类的字眼，但是看到其他师傅的挖掘SRC文章发现道理我都懂，可我就是挖不到。当时这个阶段还是处于我在补天刚挖掘专属的时候，自己就每天去看乌云漏洞库，然后记笔记，然后再去SRC上看下有没有类似的业务场景。

在我的学习经历中，自己认为时不时给自己鼓励是重要的，只要心态不崩，那么迟早我们都能成为我们想要成为的人。

讲师

在工作后技术的转变，以及对于一个SRC你关注的点

京安小妹

ch1st:

实习参加工作后，因为工作性质的问题会碰到很多网站需要测试，我工作了半个月的时候把自己参加工作之后提交的漏洞都给看了一遍，发现确实自己在挖掘漏洞的时候存在大量重复的操作，于是就萌发了效率简化操作的想法，就是开始写自己的脚本写自己的插件，让自己的效率快一点。但是在写脚本的过程中，你会发现你能想到的其实师傅们都想到了，几次轮子都造好了，然后去GitHub转了一下，我天，有师傅都已经写了，还写的比你好。这个时候我就拾人牙慧了，把GitHub上很多脚本都下载下来，然后按自己的渗透顺序排好，然后直接写个类似总开关的脚本，第一步先调用那些脚本对目标进行探测，第二步啥的～

对于一个新的SRC，重中之重就是先把它的规则给看清楚了，然后自己会首先去乌云漏洞库查找相关的漏洞，记笔记，把已公开漏洞的一些域名，内网IP，员工邮箱都记录下来。然后就开始进行域名搜集，跟师傅们差不多的套路，搜集子域名，最常用的是Teemo\subdomainbrute\layer\sublist3r,然后拉下来去重，再跑一遍三级域名。

然后自己首先会去看一个厂商的单点登录这块的是否存在缺陷，是否存在劫持。再去挖掘常见的漏洞。特别是对于一些域名业务上就只有一个系统登录口的时候，这个时候就应该尤其关注一下，记下笔记，想办法进去。因为一般这类的系统，进去的话大部分都会出现惊喜。

再一个就是关注SRC出的新业务，一般新业务系统，出现的问题会更明显一些，这就是考虑到手速的问题了。

而且现在开发领域中前后端分离的开发方式越来越多了，一般我碰到这种开发方式的目标就是F12一开，找到webpack，然后把接口相关的源码给拔下来，清洗一下，把所有接口以及请求方式和参数都给提取出来，用burp去手测。这种漏洞大部分出现在后端接口校验不严，导致未授权访问～

讲师

谈谈最近一次印象深刻的渗透测试

京安小妹

ch1st:

最近比较有印象的一次测试，是碰到了一个架cloudflare这个厂商CDN的一个目标，自己从其他途径将目标一套的源码给拿到，然后进行审计，发现了一个排序注入。师傅们碰到过的都知道，cloudflare这个玩意是会拦截很多SQL语句的，所以当时自己找各种资料都没找到，问朋友也没有有效的方法绕过，这个时候就自己去研究发现了cloudflare的注入通过参数污染的方式可以绕过[现在还能用～]，

再丢进SQLMAP去跑，发现这玩意是盲注，权限是挺大，但是找不到真实路径写不进shell.然后那段时间刚好TP的任意代码执行漏洞出现，发现了这套源码也是TP5.0.23的，去找了一堆exp打都打不进，于是这个时候就体现了py的重要性，去

问pnpoop师傅，他改了一下payload，然后成功对目标站点执行了代码。

但是cloudflare这个尿性，写入shell的时候，phpinfo()此类的函数全部拦截，eval啥的也拦截，<?php不能连接在一下否则也拦截，然后自己就改了用<??>这种短连接方式去写，发现自己手上的大马和小马都ban了。然后自己去对照了一个另外一个一套程序的站点，发现disable_function拦截了好多东西，最后通过TP的代码执行漏洞写入一个下载马，在用pcntl_exec反弹出shell结束了这次渗透。

虽然这个过程不复杂，但是在渗透的过程中，自己也费了很多心思～ 在我认为，真的，像极了爱情。（漏洞提交是初恋的味道，漏洞重复是失恋的滋味，热恋就是被师傅们带我飞的时候）

讲师

对白帽子小伙伴们的建议

京安小妹

ch1st:

一定要养好心态，还有身体。不要以为自己年轻可以为所欲为，当你身体出毛病的时候你就会感觉当一个正常人是多么幸福的一件事情。

环境，朋友，自己的上进心和求知欲尤为重要，我们都要时时刻刻保持着一个学习的心态，自己要是真挖不到洞了，就是自己的大脑告诉自己该学习了，挖洞可以放一放了。

希望能与各位师傅做朋友 hhhh~

讲师

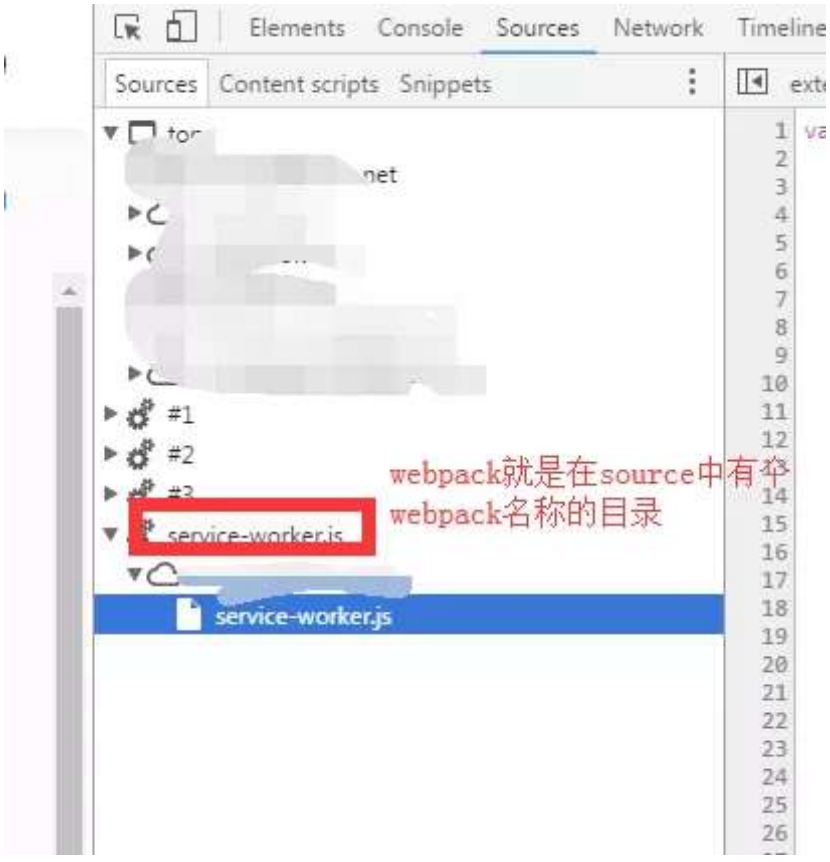
互动问答环节：

1. 三级子域名怎么跑?

讲师:1.二级域名为基础输入域名；2.也可以用在线子域名查询，写脚本批量跑；3.自己本地架构302跳转，然后用下图递归，一般第二天打开看就行。

2.webpack就是webpackjs吗?

讲师:根据下图提示，



然后去展开，里面会有js文件，文件里面会有这个网站的对应业务的大部分ajax请求，把它提出来，一步一步的测试（暂时我也没想到更好的办法，因为很多是restful风格，需要不时的更换请求方式或者带参数）。

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

文章已于2019-02-25修改