安全小课堂第八十七期【web漏洞挖掘之前期信息收集】

京东安全应急响应中心 3月12日

工欲善其事必先利其器，漏洞挖掘前期掌握的信息越多，再结合一些其他手段，漏洞挖掘时就会更加的得心应手。因此信息收集这个话题对于漏洞挖掘爱好者来说可谓是不可不谈。

JSRC **安全小课堂第八十七期**，邀请到**Reckfulyx**作为讲师就**web漏洞挖掘之前期信息收集**为大家进行分享。感谢白帽子盆友的精彩提问与互动~也感谢**沦沦**同学积极探讨与无私分享~

如何利用DNS区域传送漏洞收集域名信息

京安小妹

Reckfulyx：
这个主要是DNS区域传送漏洞的利用，如果存在漏洞的话会得到该网站整个域的子域名以及ip。这里给出几个判断是否存在的命令
Win版：
（1） nslookup
（2） server dns.xxx.xx.cn
（3） ls xxx.xx.cn
Linux版：
dig @dns.xxx.xx.cn axfr xxx.xx.cn
另外可以借助工具进行查询，比如nmap和dnsnum
Namp:
nmap --script dns-zone-transfer --script-args dns-zone-transfer.domain=xxx.xx.cn -p 53 -Pn dns.xxx.xx.cn
Dnsenum:
dnsenum dnsnum xx.xx.cn
另外在github找到一个前人整理好的存在漏洞列表，可能一部分已经失效或者修复了，但还是会存在漏网之鱼，小伙伴们可以自行尝试：
https://github.com/lijiejie/edu-dns-zone-transfer/blob/master/vulnerable_hosts.txt

讲师

Tomcat默认安装会出现哪些敏感目录，各自会有什么有价值的信息呢

京安小妹

Reckfulyx：

tomcat默认安装一般存在7个目录，分别是lib,logs,temp,webapps,work,conf,bin。lib用来存放tomcat运行需要加载的jar包，bin目录主要是用来存放tomcat的命令，logs用于存放tomcat的日志文件，temp存放临时文件，webapps存放网站应用，work存放tomcat编译文件。一般来讲，conf目录比较敏感，通常会存在xml和properties文件，这些文件中可以找到用户信息、数据库信息以及其他相关的配置信息。

讲师

burpsuite有哪些被动收集信息的插件

京安小妹

Reckfulyx：

很多burp中的插件可以进行辅助的渗透测试，这里我找到了两个被动信息收集的插件，大家有兴趣的可以试试：

burp-suite-error-message-checks基于java的burp小插件，可以用来被动的收集服务器错误信息，比如Fatal ereor,sql报错等等。攻击者可以使用这个插件收集类似的信息，可能会获取绝对路径或数据库信息等。

Header Analyzer基于python的burp插件，可以收集到一些网站header头信息，比如安全头（http security headers）是否存在配置错误或缺失安全头等问题。

社工对信息收集有哪些帮助

京安小妹

Reckfulyx:

这个问题思路就很多了。对于src来说的话，通过社工可以获取到用户名/邮箱。可以直接google hack搜索或者使用工具，如theharvester，方便实用。另外github信息泄露也是一个方面，通过收集到的用户名，或者爬取网页获得的一些web author进行搜索，可能会找到一些建站人员存放的网站敏感文件；相同思路的还有网盘搜索，这个取决于个人能搜索力以及一些运气了。最后提一点思路相对猥琐的，比如qq群搜索，或者想方设法（自己脑洞大开）获得qq群号码，然后混进去查看群文件（主要提供思路，并不鼓励此做法）。

讲师

自己用的比较顺手的黑科技

京安小妹

Reckfulyx：

下面分享一些个人经常使用的姿势。子域名的收集对于渗透而言是十分重要的，因为可能主站可能防护做的密不透风，而且测试者连真实ip都获取不到。这时对于子域名的挖掘就显得至关重要了。目前最主流的子域名收集方式可能就是通过工具来获取了，比如lijiejie的subdomainbrute，seay的layer，以及一些脚本等等。这类脚本通常原理都是枚举与爆破，但是相对耗时，而且对内存及网络资源占比很大。另外就是通过一些网站直接进行查询，比如强大的微步在线，这个经常能查询出一些三级、四级域名，对我们的挖掘工作十分有利，但是门槛比较高，需要收费。

另外还有些非主流姿势：1.ssl证书查询，可以通过www.chinassl.net直接对域名查询。2.Google C段，使用方法为site:10.10.10.*,直接给出ip查询就好。3.备案查询，通过对网站的备案号查询，获取同一备案号或者同一公司下的域名。这里推荐nosec.org。4.通过app的抓包获取信息或使用工具对app所有链接进行提取。5.crossdomain.xml，这个里面也可能会存在一些平时不易察觉的网址或ip。

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。

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