安全小课堂第九十一期【web漏洞之敏感信息漏洞挖掘】

京东安全应急响应中心 4月16日

一个微小的漏洞，经过攻击者的利用，也会对企业和用户造成巨大的危害。
JSRC **安全小课堂第九十一期**，邀请到**Vulkey_Chen**作为讲师就**web漏洞之敏感信息泄露**为大家进行分享。感谢白帽子盆友的精彩提问与互动~

敏感信息泄露漏洞的成因是什么?

京安小妹

Vulkey_Chen:
排除安全性的缺陷以外原因有很多，例如网站的一些配置错误，也可能是网站历史遗留导致，目前更多的问题都是企业员工的安全意识不足导致，例如有些用户为了方便对自己的账户设置了简单的口令导致口令容易被攻击者直接破解，有时候一些程序员为了图个方便会把代码托管在github这样的平台，会全部放上去，并且有些时候一些包含账号密码这样敏感信息的文件也会存在...

讲师

敏感信息泄露漏洞的分类及利用?

京安小妹

Vulkey_Chen:
a.安全性缺陷 - 安全性缺陷有很多问题了，SQL注入、越权等等，
b.备份文件 - 包含敏感信息的文件被下载 -> %host%(www|_www|backup|_backup|...).(zip|rar|7z|gz|...) 这里仅仅举一个网站备份方面的，其实还有很多例如sql、mdb文件之类的，见过一些程序员直接在服务器上调试使用的一些编辑器会自动生成%filename%.bak，那就更方便被发现问题了，如果想了解更多可以去参考一下其他扫描器的扫描备份字典，说一个小tip，对这种问题你可以写一个爬虫对目录进行爬取(也可以使用AWVS)，然后一个一个的使用字典去扫描~
c.目录遍历 - 网站在做目录方面配置的时候会出现目录遍历的问题，如果没有设定的主页(index.html...)就会显示当前目录下的所有文件给访问者，这类问题也可以使用目录发现工具去扫描，运气好还是能碰见一两个的，也可以自己去测试一些敏感的地方，例如上传身份证的地方，去看看删除url中的(身份证图片的文件名.文件后缀)是否能遍历~
d.第三方(代码托管、外包厂商) - 第三方的问题，在乌云上有一堆代码托管导致的各种案例了(xxx泄露#可内网漫游~)，发现的方法也很简单了，使用强大的谷歌进行搜索(site:github.com intext:website password ...)，也可以使用开源的一些检索工具(https://github.com/UnkL4b/GitMiner、https://github.com/repoog/GitPrey)。很多大型厂商因为任务多，所以也会找一些外包来帮忙做事情，但是外包公司是不可能具备大公司的安全意识的，所以在开发的时候也会存在一些安全性问题，而且一些外包公司也喜欢留下自己的指纹，可以通过在第三方代码托管平台去搜索这些对应的指纹来看看是否有信息泄露的问题~

讲师

能否列举一些敏感信息泄露的案例?

京安小妹

Vulkey_Chen:

a.在一次对某邮箱系统进行测试的时候，偶尔对文件后缀名进行了fuzz，原url->http://www.xxx.com/mail/index.php，在index.php如果添加一些特殊字符串，可以直接下载index.php的源码~有了源码可以进行审计或者找配置文件进行下载更省事~

b.一些厂商也会有历史遗留问题，比如某平台由PHP转换到了ASPX，但是历史站点被遗留了在一个目录下，而PHP已经不再被解析，所以源码就直接可以看见了~

能否推荐一些检测敏感信息泄露的工具和小脚本?

京安小妹

Vulkey_Chen:

这里推荐这几款： weakfilescan、GitMiner、GitPrey、dirb、FUZZDB

讲师

敏感信息泄露漏洞的修复和防范手段?

京安小妹

Vulkey_Chen:
不知攻焉知防，可以根据我列出的攻击手段直接来排查~主要的还是定期对员工进行安全意识的培训。

:
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