Week3-<19906767892>

Login to get my gift

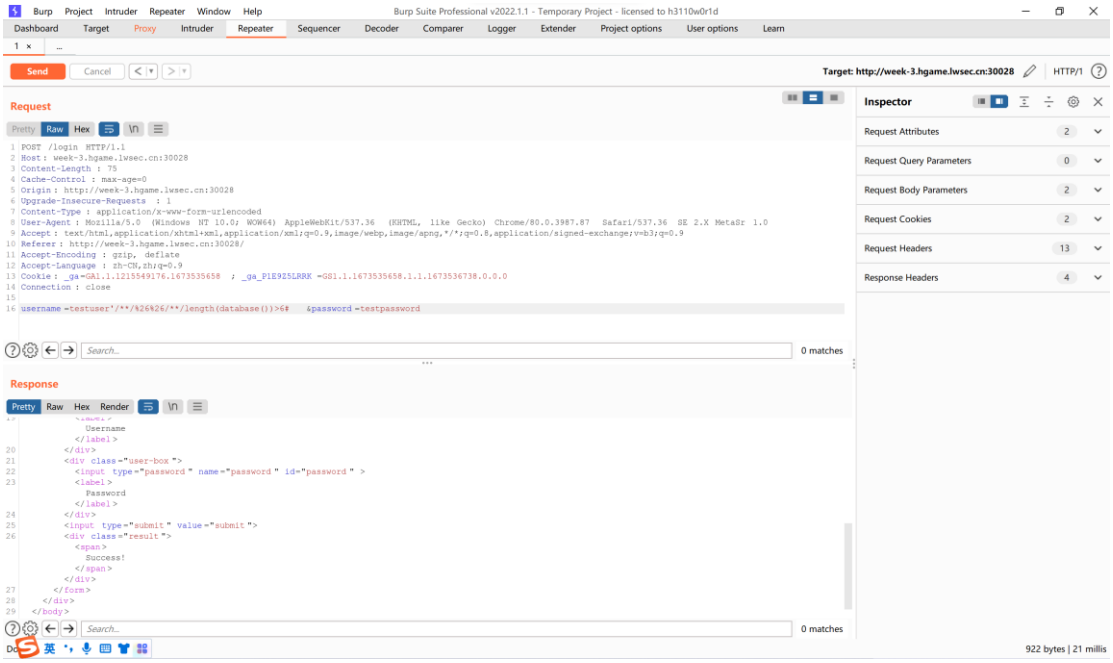
Sql 注入

过滤： ， mid,substr,+,=,and

绕过：/**/,left,right,%26%26,regexp

字符型注入，布尔盲注

暴库名

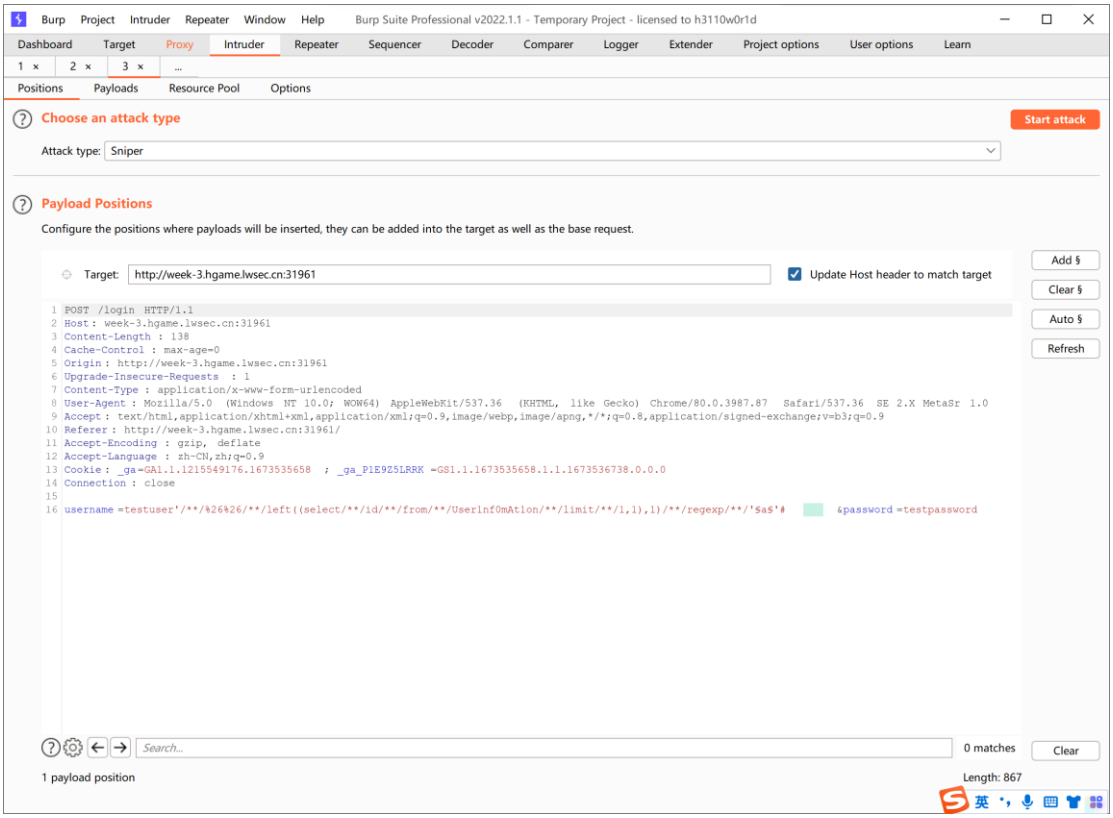


使用 left 和 right 配合进行提取单个字符，套上 ascii(),后面 regexp 之后的数字 send to intruder 进行比较，ascii(right(left(database(),1),1))/**/regexp/**/1,第一个值和第二个值更改，爆出库名 l0g1nme

爆表名，同理进行提取单个字符比较，表名 User1nf0mAt1on

爆列名，同理，为 id,passw0rd,usern4me

爆值



（必须用 left 和 right 提取单个字符比较 asc 码，不然直接字符比较分不出大小写，用 left 不断变大 right 只取最右边一个）同样 left 参数和 regexp 参数变化来爆值，再更改 limit 后一个参数。id 有 1,2；username 是 hgAmE2023HAppYnEwyEAr；password 是 WeLc0meT0hgAmE2023hAPPySqI