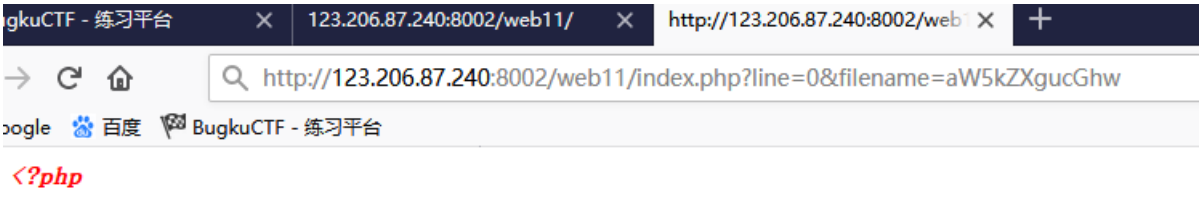
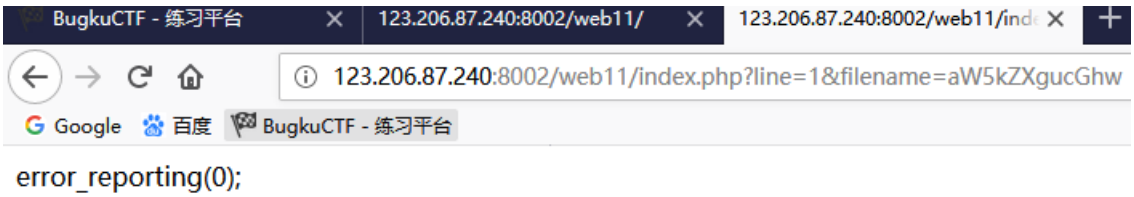
BurpSuite intuder里保存所有网页的特定内容：以bugku的cookies欺骗为例题

转载

weixin_30721077 于 2019-06-20 17:52:00 发布 167 收藏
文章标签： php javascript 爬虫 ViewUI
原文链接：http://www.cnblogs.com/cnnnnnn/p/11060250.html

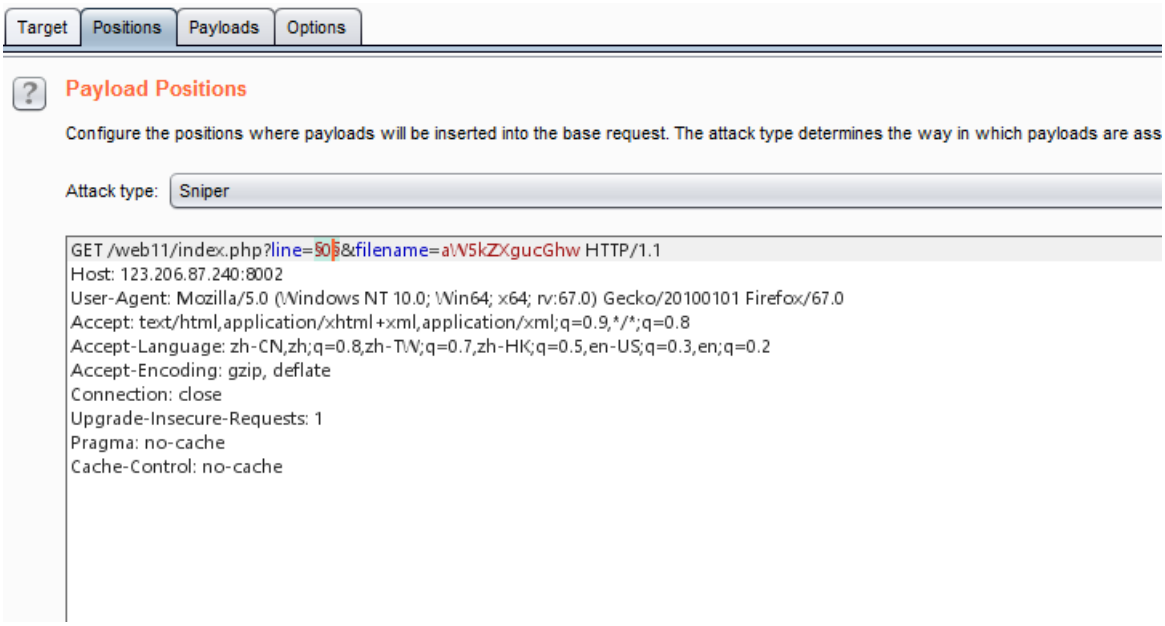
这题里想读取index.php只能一行一行的读，通过控制line参数的值。如下：



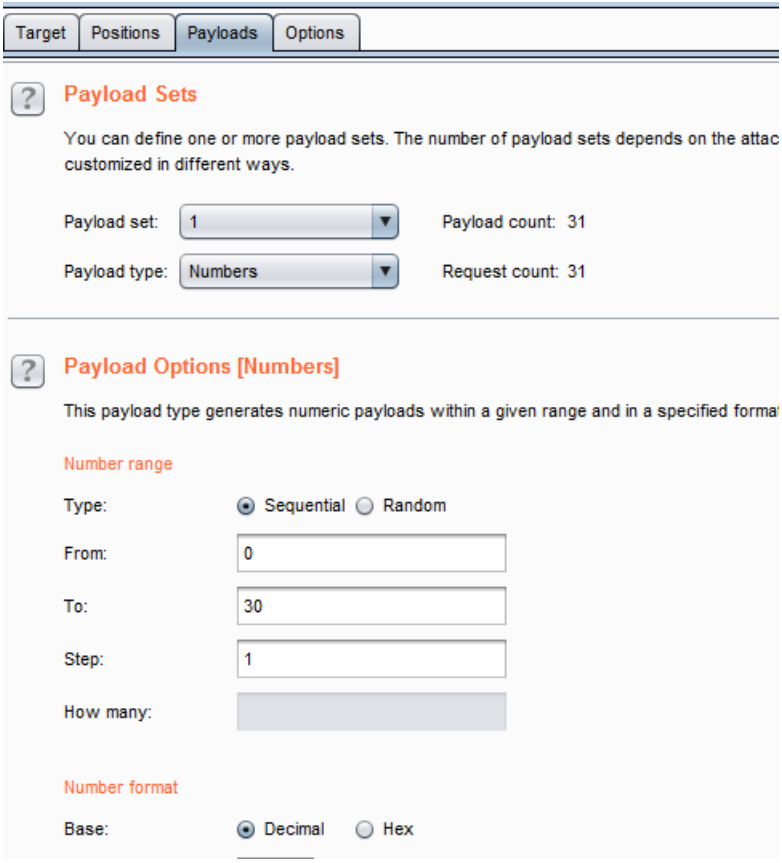


正常的writeup都是写个爬虫，但我觉得burp肯定有自带这种功能，不用重造轮子。经过学习后发现以下步骤可以实现。

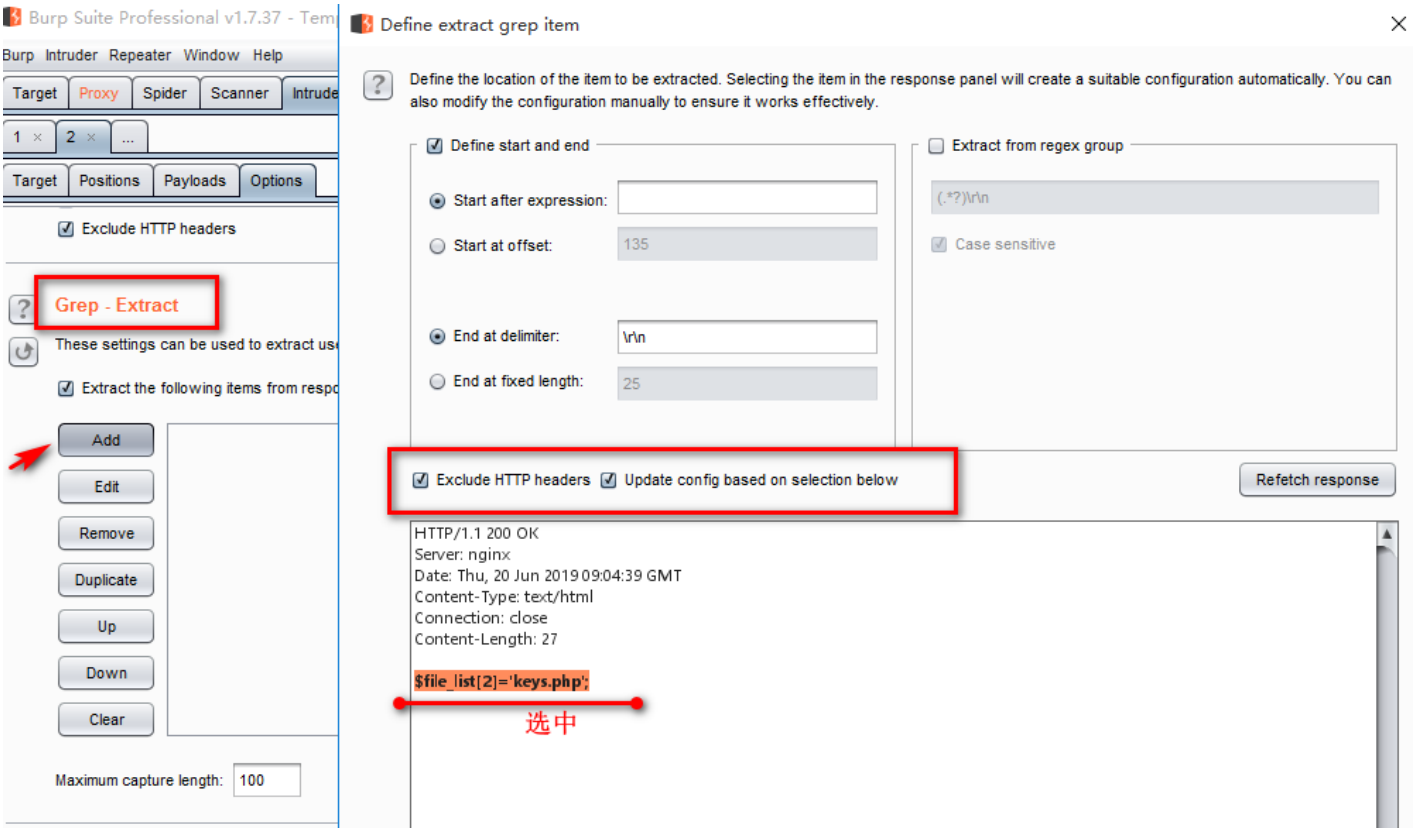
1. 抓包，发到intruder，给line添加$



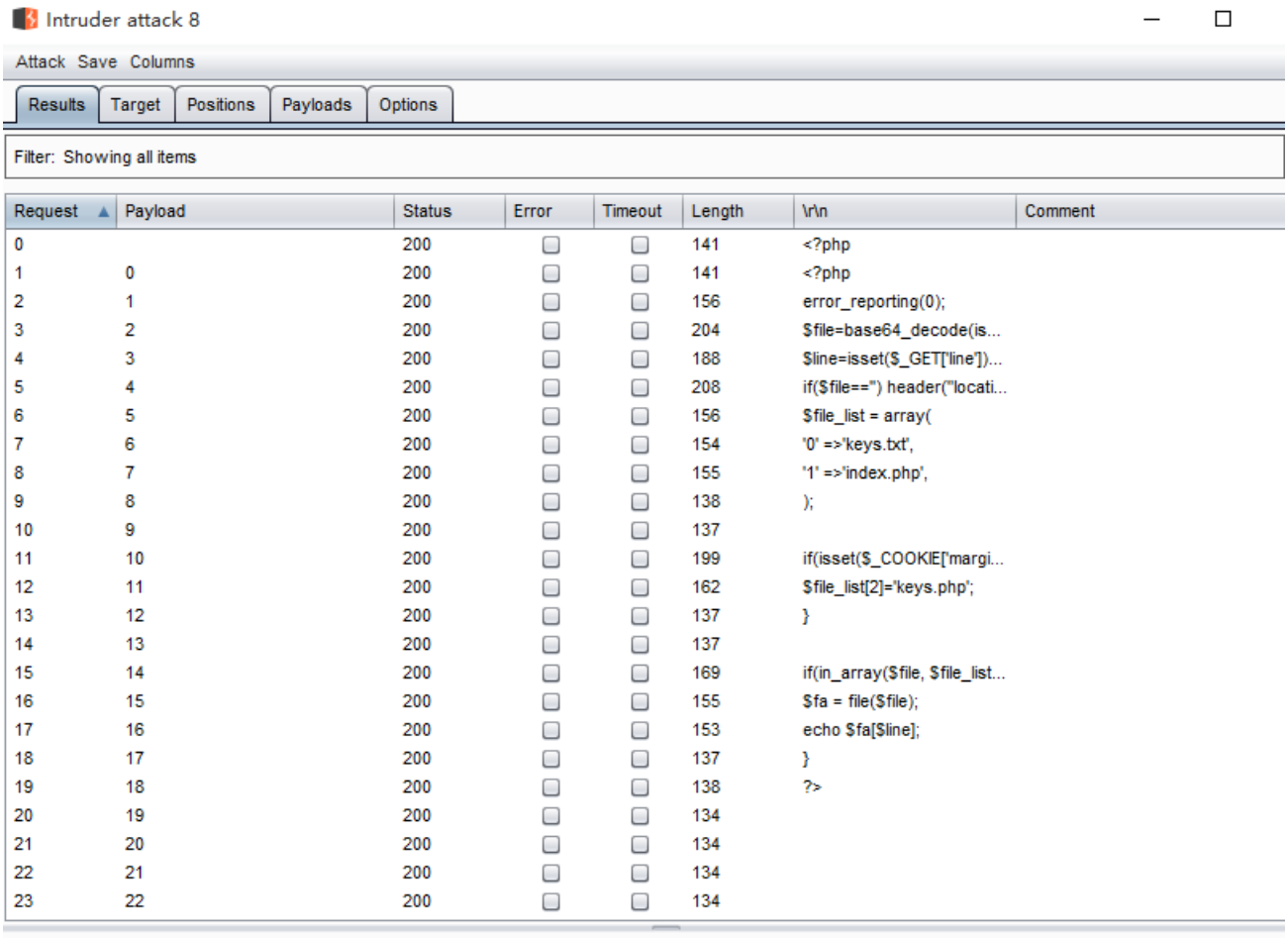
2.payloads当然设成number



3. 重点：在options里的Grep- Extract里，点击add，勾选exclude HTTP headers(排除请求头)，另一个是默认勾选，然后下面选中你需要的内容，上面的start和end就会自动设置好。

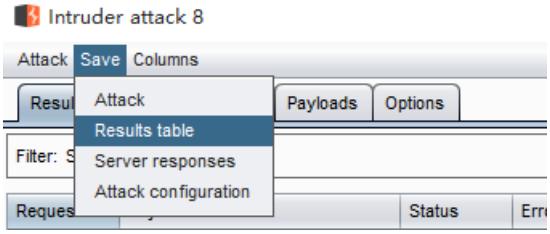


4.然后点击最上面的开始攻击，攻击结果就会单独显示咱们筛选的内容：

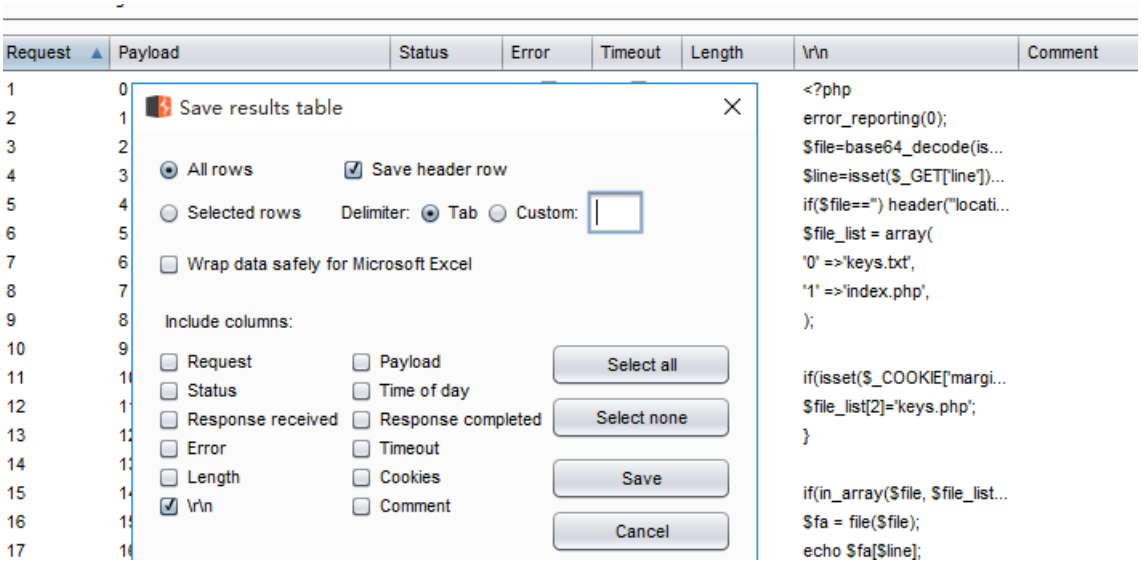


Request	Payload	Status	Error	Timeout	Length	\r\n	Comment
0		200			141	<?php	
1	0	200			141	<?php	
2	1	200			156	error_reporting(0);	
3	2	200			204	$file=base64_decode(is...	
4	3	200			188	$line=isset($_GET['line'])...	
5	4	200			208	if($file=='') header("locati...	
6	5	200			156	$file_list = array(	
7	6	200			154	'0' =>'keys.txt',	
8	7	200			155	'1' =>'index.php',	
9	8	200			138	);	
10	9	200			137		
11	10	200			199	if(isset($_COOKIE['margi...	
12	11	200			162	$file_list[2]='keys.php';	
13	12	200			137	}	
14	13	200			137		
15	14	200			169	if(in_array($file, $file_list...	
16	15	200			155	$fa = file($file);	
17	16	200			153	echo $fa[$line];	
18	17	200			137	}	
19	18	200			138	?>	
20	19	200			134		
21	20	200			134		
22	21	200			134		
23	22	200			134		

5.这样还没完，因为通常咱们需要把那一列保存到一个文件后续编辑。点击最上面的save->result table



在下面勾选竖行的名字，点击save。我这里名字是\r\n。这样就会输出一个文件，只包括这个列。



---

end

转载于:https://www.cnblogs.com/cnnnnnn/p/11060250.html