

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

转载

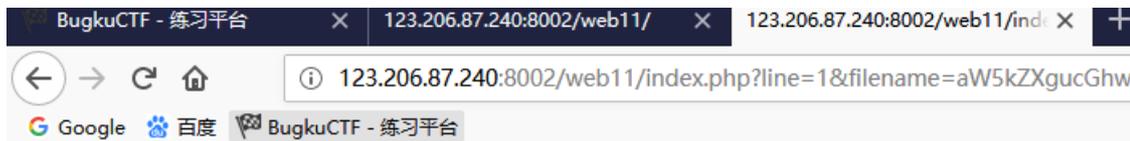
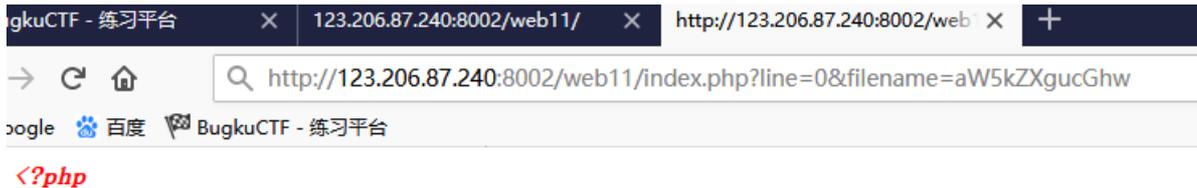
weixin_30721077 于 2019-06-20 17:52:00 发布 167 收藏

文章标签: [php](#) [javascript](#) [爬虫](#) [ViewUI](#)

原文链接: <http://www.cnblogs.com/cnmnnn/p/11060250.html>

版权

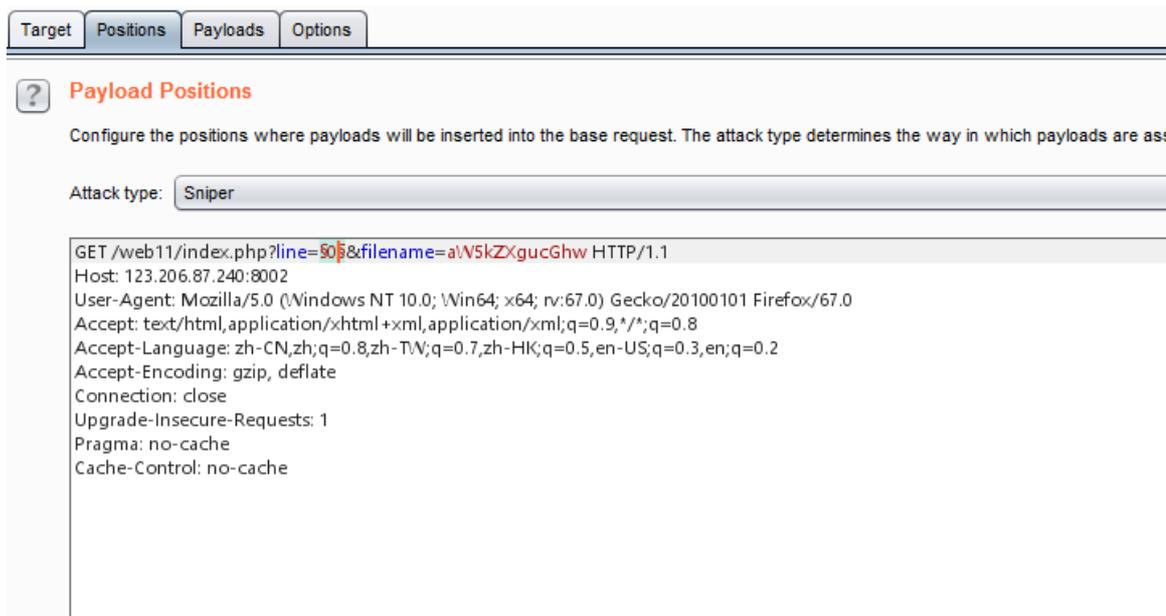
这题里想读取index.php只能一行一行的读，通过控制line参数的值。如下：



```
error_reporting(0);
```

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

Target Positions Payloads Options

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack customized in different ways.

Payload set: 1 Payload count: 31
 Payload type: Numbers Request count: 31

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: Sequential Random

From: 0
 To: 30
 Step: 1
 How many: []

Number format

Base: Decimal Hex

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。

Burp Suite Professional v1.7.37 - Temi

Define extract grep item

Define the location of the item to be extracted. Selecting the item in the response panel will create a suitable configuration automatically. You can also modify the configuration manually to ensure it works effectively.

Define start and end

Start after expression: []
 Start at offset: 135

End at delimiter: \r\n
 End at fixed length: 25

Extract from regex group: []
 [] Case sensitive

Exclude HTTP headers Update config based on selection below

Refetch response

```

HTTP/1.1 200 OK
Server: nginx
Date: Thu, 20 Jun 2019 09:04:39 GMT
Content-Type: text/html
Connection: close
Content-Length: 27

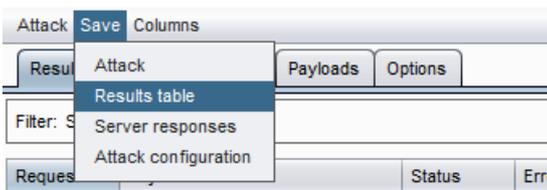
$file_list(2)='keys.php:'
  
```

选中

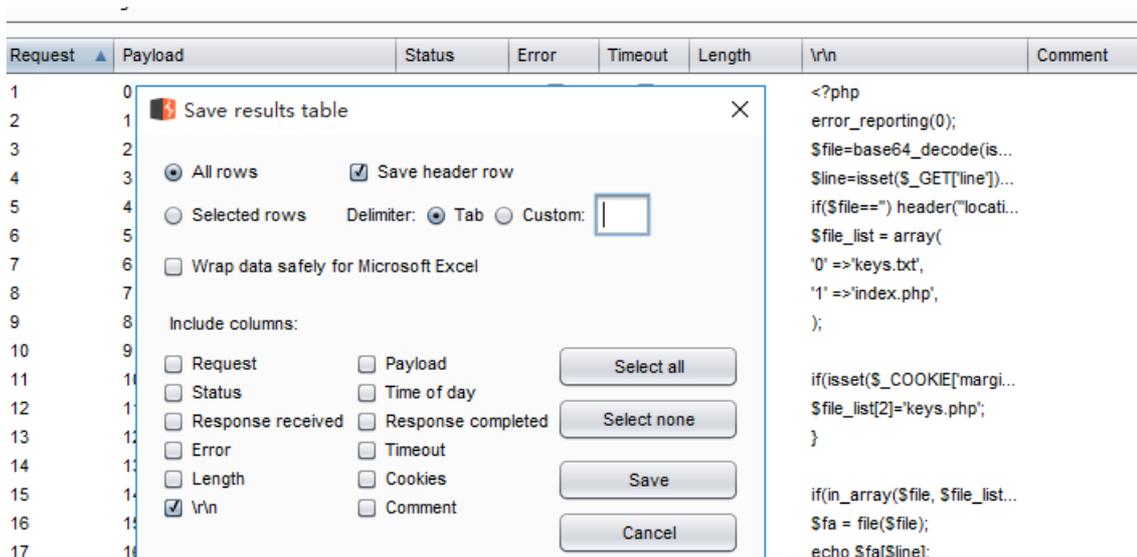
4. 然后点击最上面的开始攻击，攻击结果就会单独显示咱们筛选的内容：

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



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)