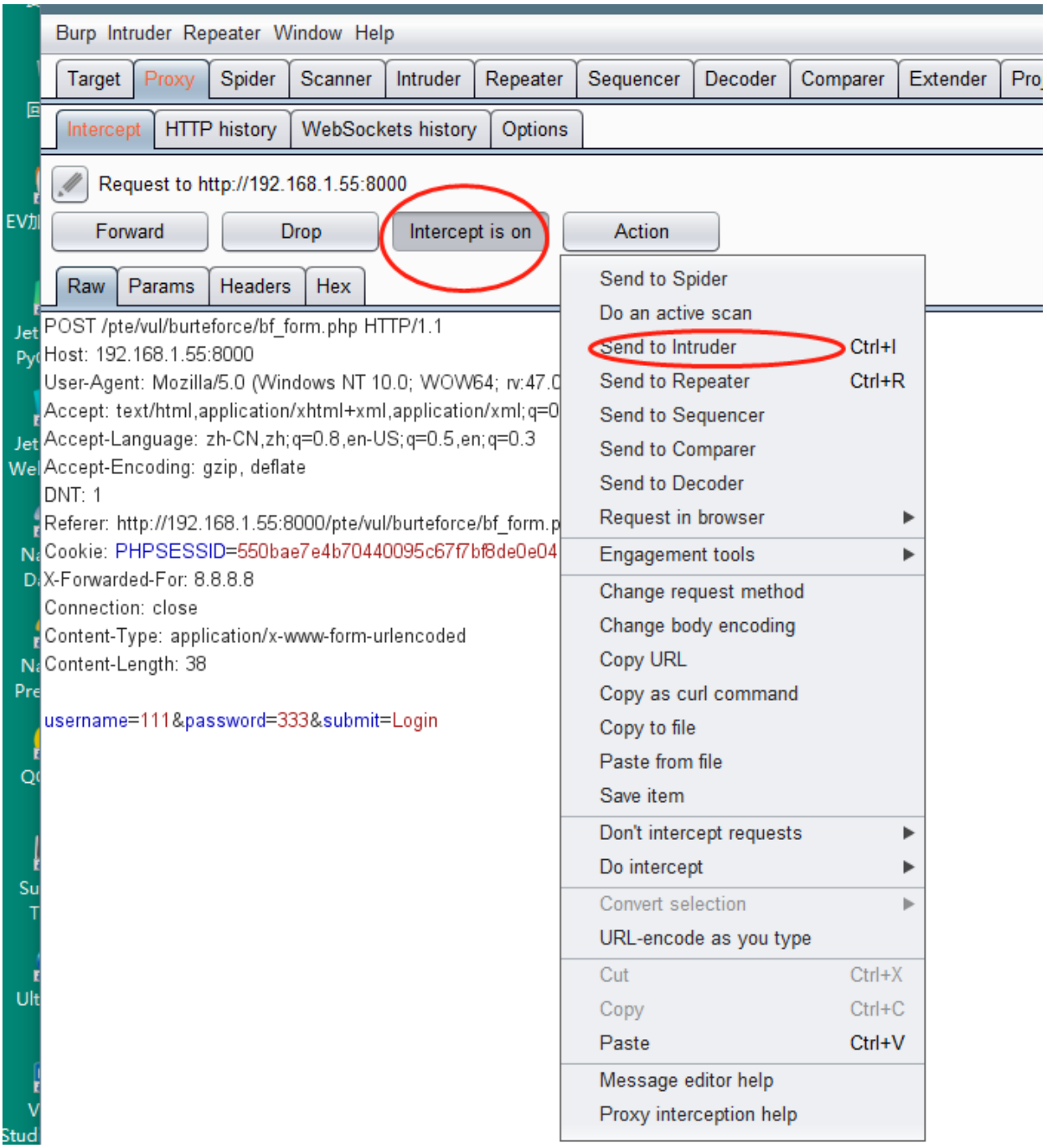
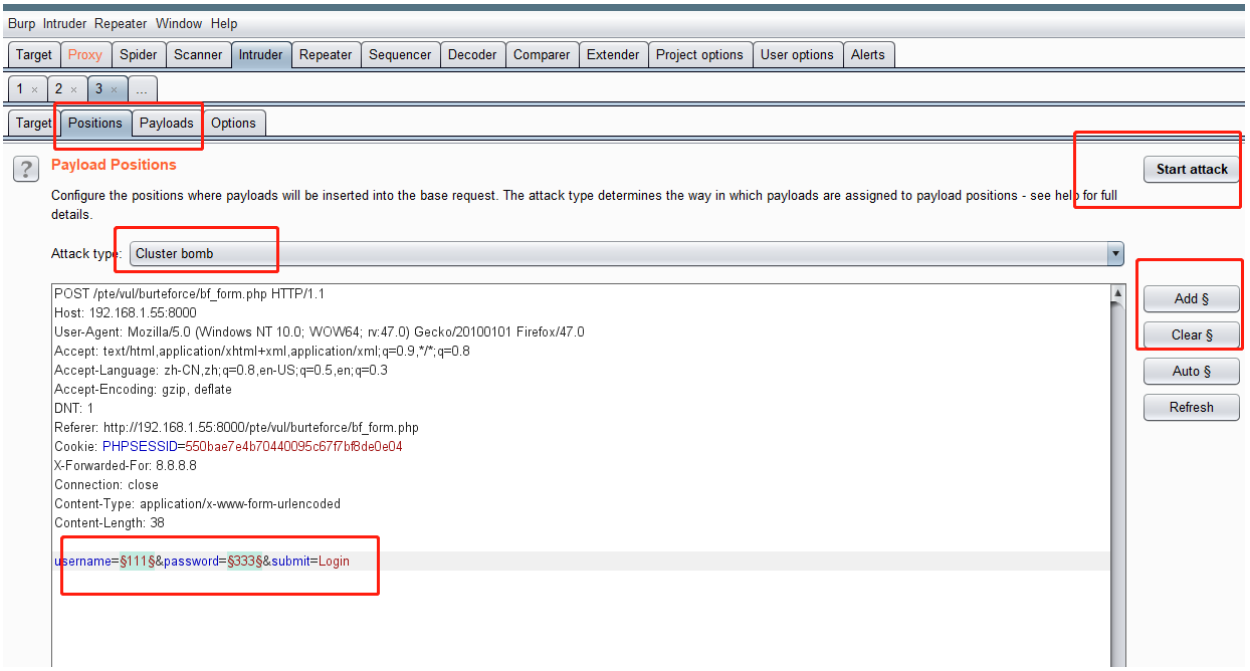
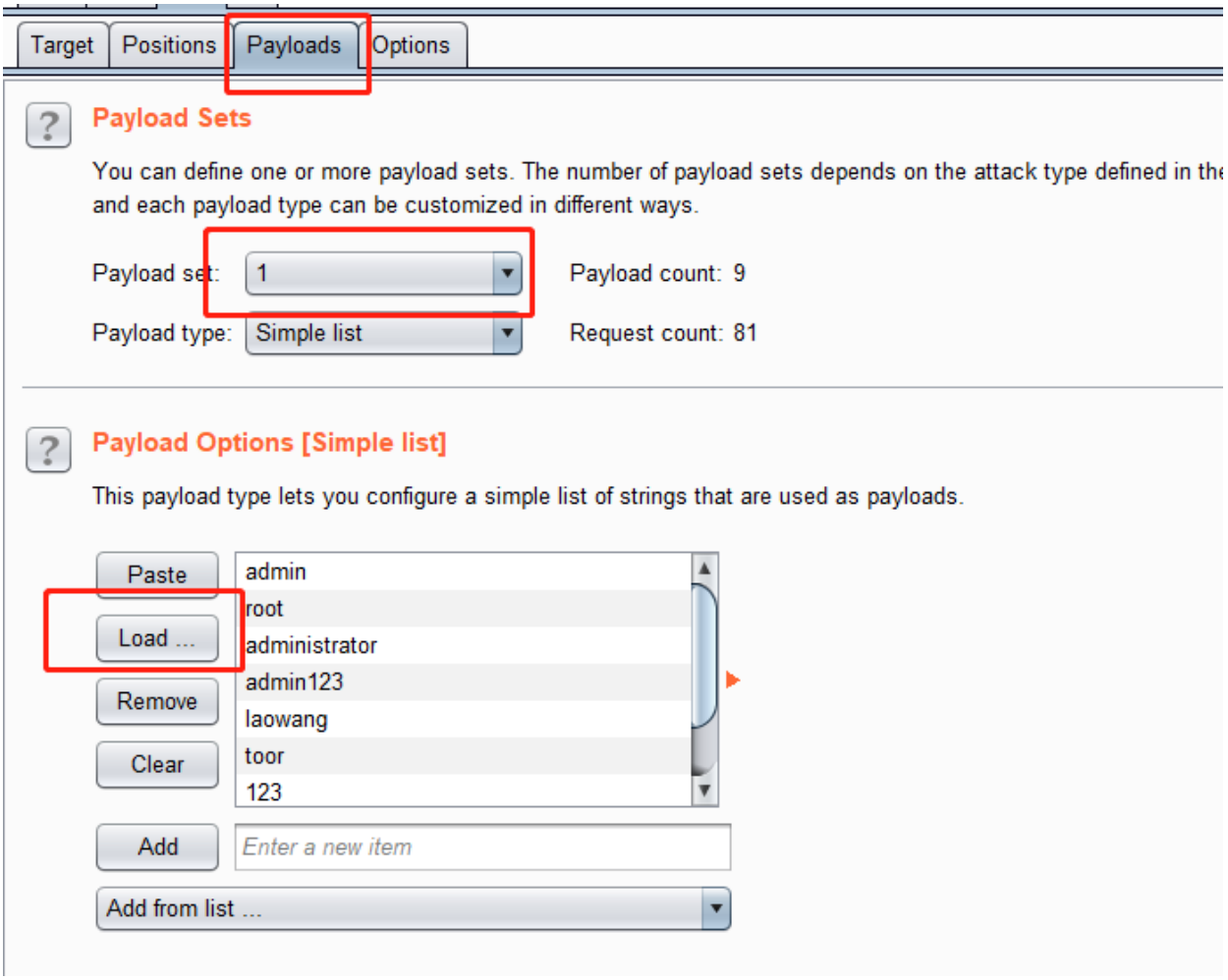
爆破流程：

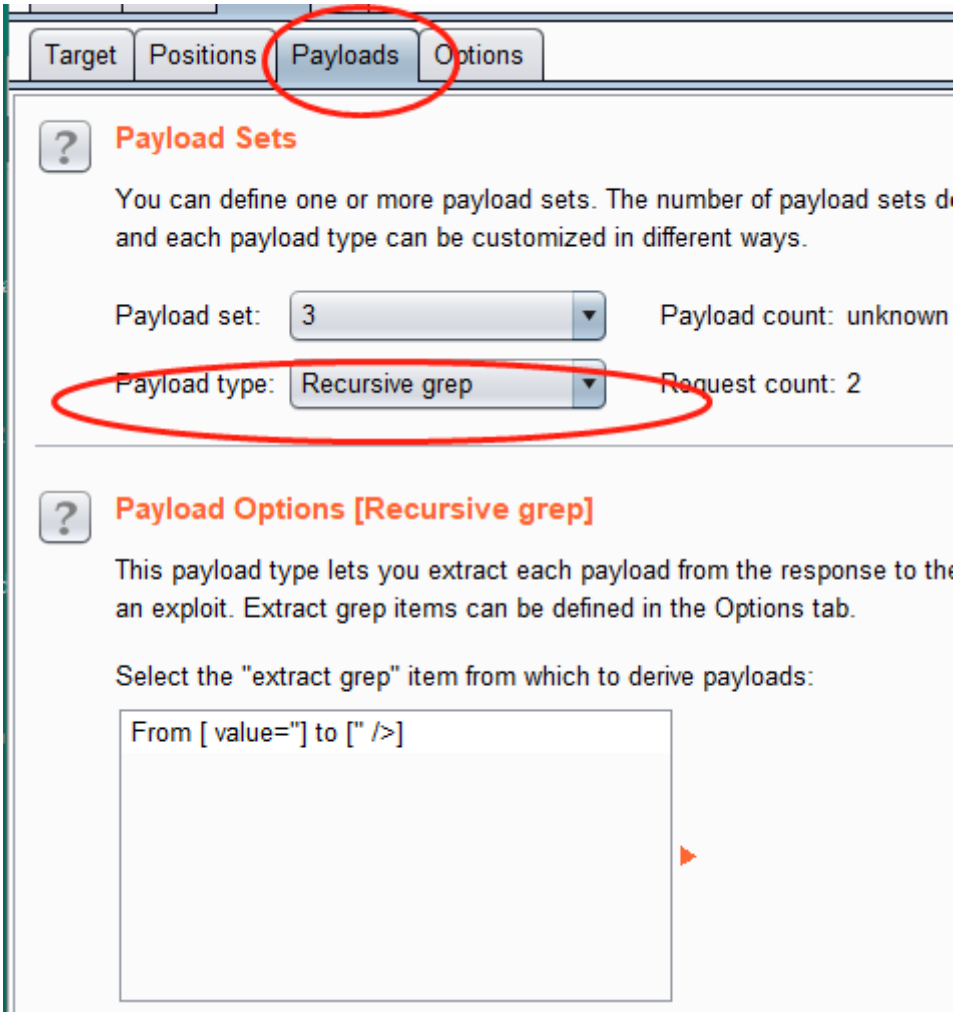
firefox设置代理-》burpsuit-》sropy-》intercept is on -》 action-》send to intruder->clear$-》选择可变字段 点击 add$ ->attack active 选择爆破模式-》payloads->payload set 选择参数->load 选择爆破字典-》右上角 start acctck-》length排序，找出不一致的行选中-》response-》render最下面



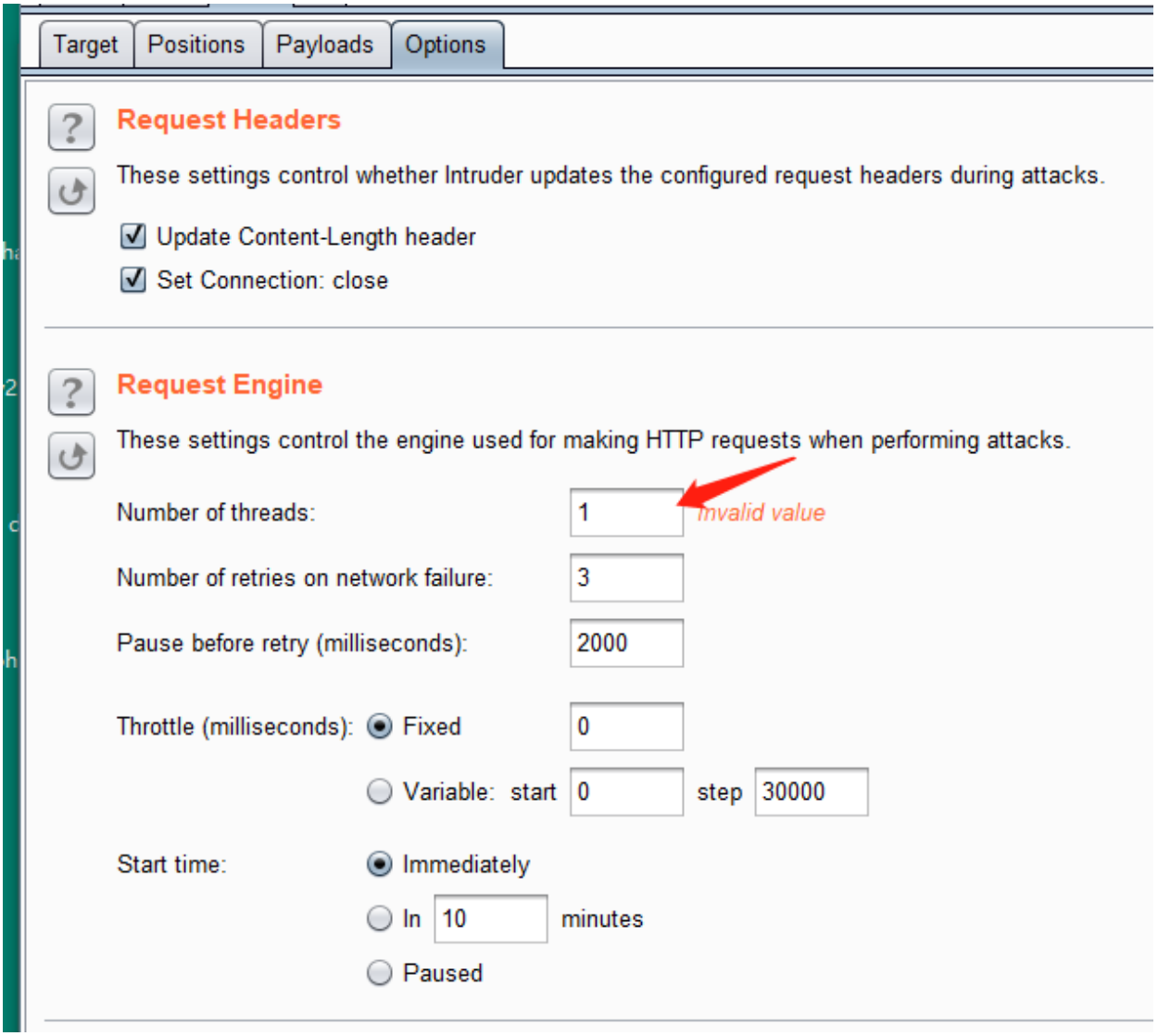




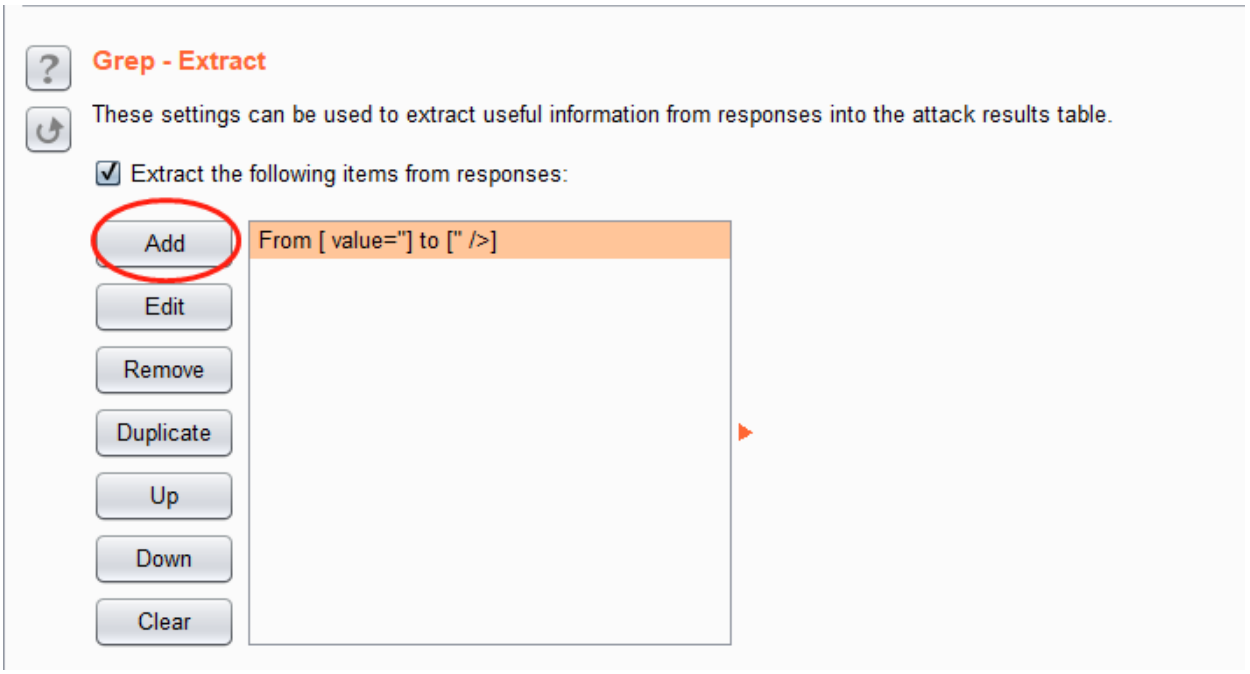
ttoken攻击：和密码一样，只是token参数为自动从网页获取，需要修改payload type

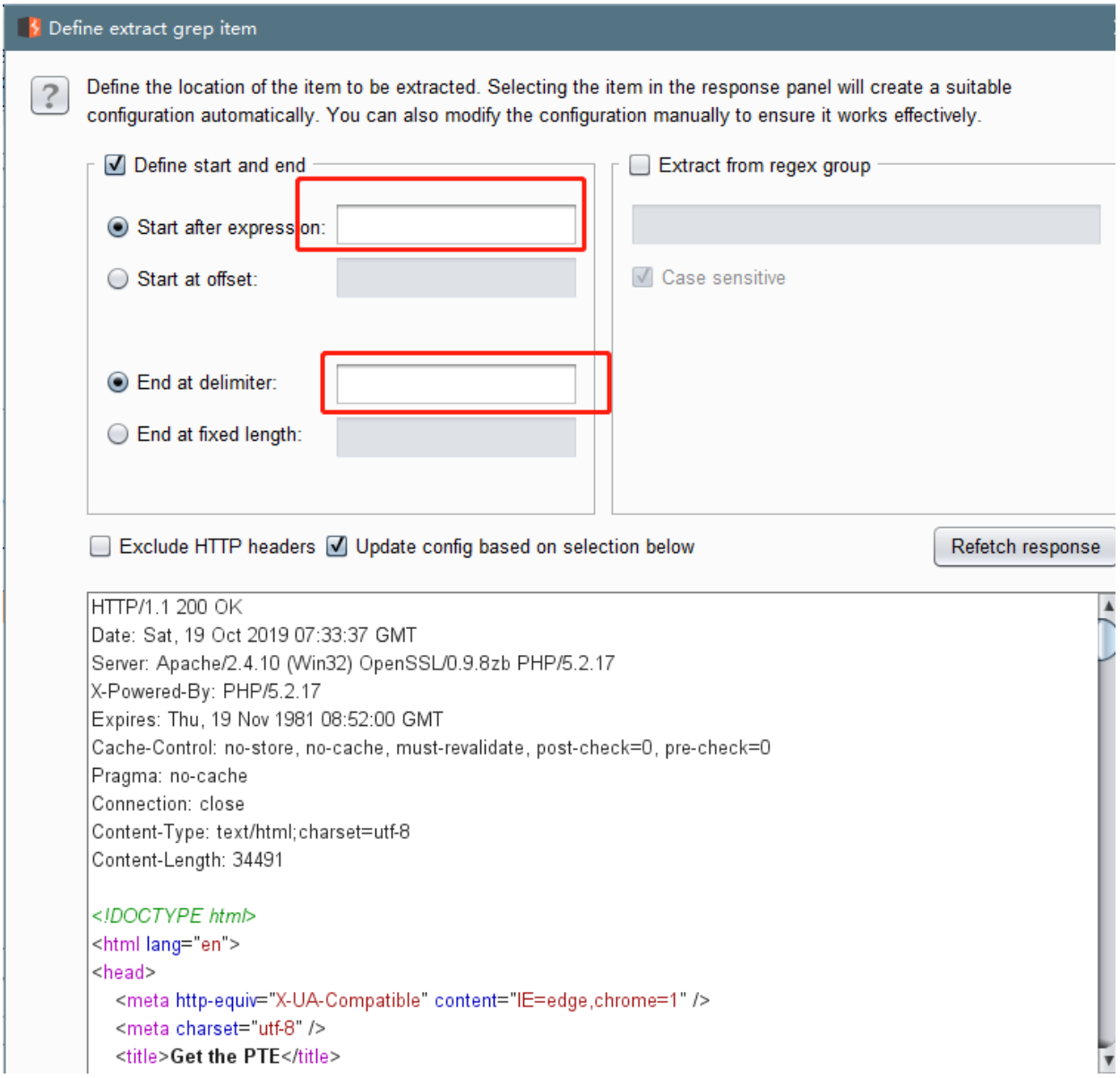

Target
Positions
Payloads
Options
Payload Sets
You can define one or more payload sets. The number of payload sets d
and each payload type can be customized in different ways.
Payload set:
3
Payload count: unknown
Payload type:
Recursive grep
Request count: 2
Payload Options [Recursive grep]
This payload type lets you extract each payload from the response to the
an exploit. Extract grep items can be defined in the Options tab.
Select the "extract grep" item from which to derive payloads:
From [value='] to [" />]

设置爆破线程数为1



添加正则表达式，获取token




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:
End at delimiter:
End at fixed length:
Extract from regex group
Case sensitive
Exclude HTTP headers
Update config based on selection below
Refetch response
HTTP/1.1 200 OK
Date: Sat, 19 Oct 2019 07:33:37 GMT
Server: Apache/2.4.10 (Win32) OpenSSL/0.9.8zb PHP/5.2.17
X-Powered-By: PHP/5.2.17
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Connection: close
Content-Type: text/html;charset=utf-8
Content-Length: 34491
<!DOCTYPE html>
<html lang="en">
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
<meta charset="utf-8" />
<title>Get the PTE</title>