

新手福利 | Burpsuite 你可能不知道的技巧

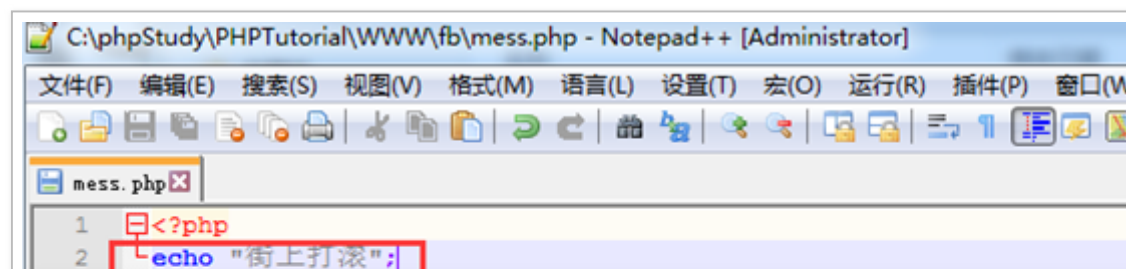
一年一度的 Burpsuite 过期的时间又到了，Burpsuite 作为 Web 安全者必不可少的一件神器，其实有很多实用的技巧，本篇文章的目的是抛砖引玉，通过分享一些渣渣技巧，可能会帮助解决一些 egg hurt 的问题。

看过一些文章，freebuf 中很多文章的评论很可能比文章本身更有技巧和使用价值，欢迎大佬指教。另外，本篇文章不是 burpsuite 的科普贴，并不会介绍各个模块的功能，只是一些小 trick。最后，文末有彩蛋，伸手党可以直达。

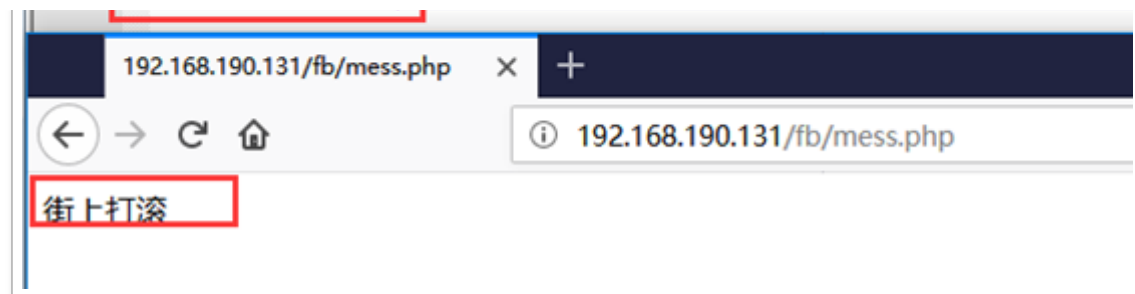
0×01 burpsuite 中文乱码问题

这个是很多初学者会遇到的蛋疼问题。

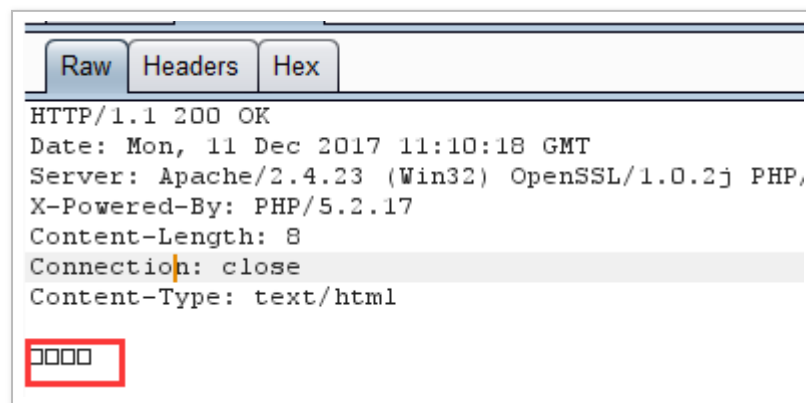
我们新建一个 php 文件，输出“街上打滚”，然后使用 firefox 访问，正常显示中文。



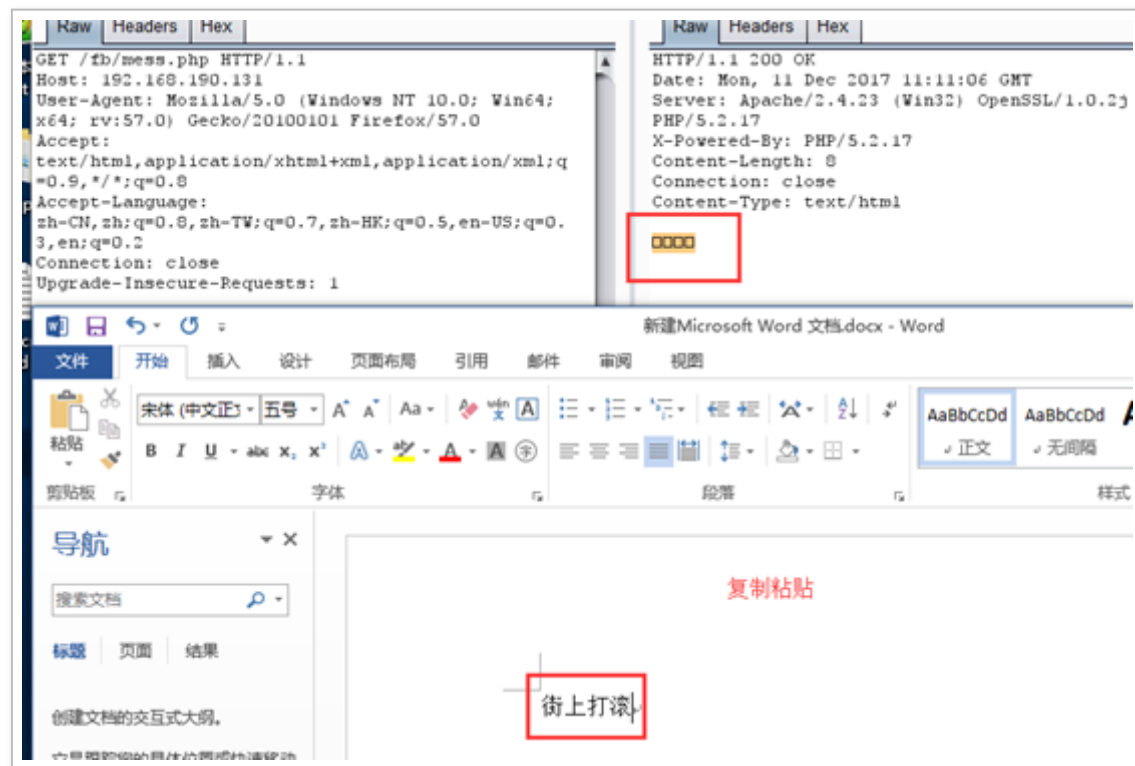
```
C:\phpStudy\PHPTutorial\WWW\fb\mess.php - Notepad++ [Administrator]
文件(F) 编辑(E) 搜索(S) 视图(V) 格式(M) 语言(L) 设置(T) 宏(O) 运行(R) 插件(P) 窗口(W)
mess.php
1  <?php
2  echo "街上打滚";
```



然后我们查看 burp，默认情况下，可以看到显示的是□□□□



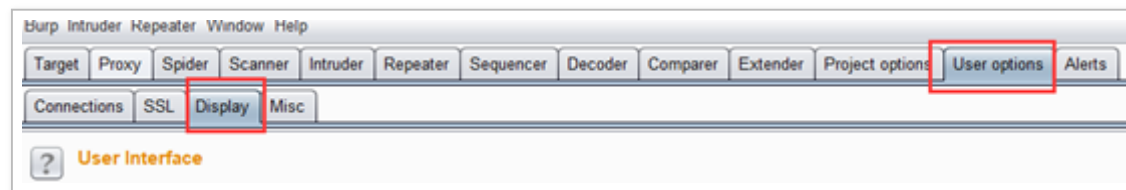
这个难道是字符集的问题吗，实际上，如果大家把这四个框框复制之后粘贴到 word 上，就会显示“街上打滚”。



所以可以知道这个问题其实是 burpsuite 本身界面显示的问题。

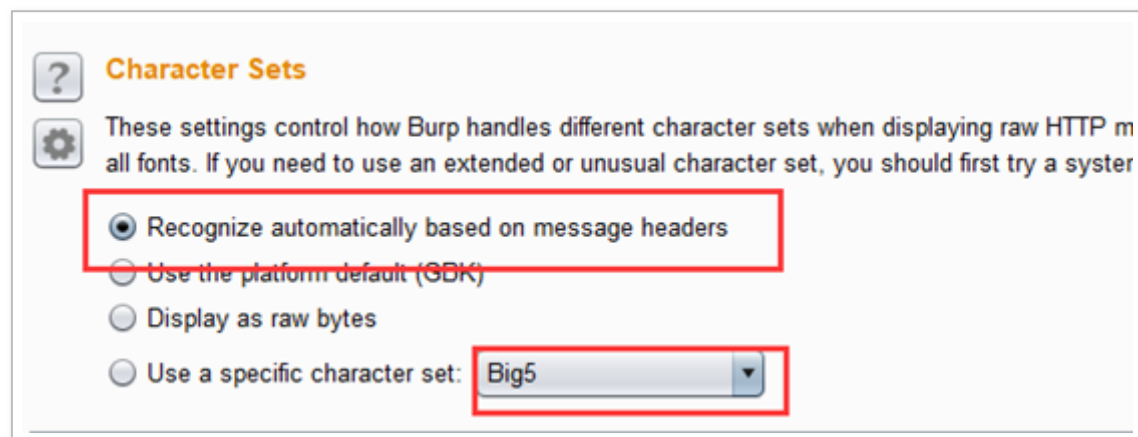
那么，第一个想到的应该是更改显示。

在 burp 的用户选项下，有一个 display 选项。

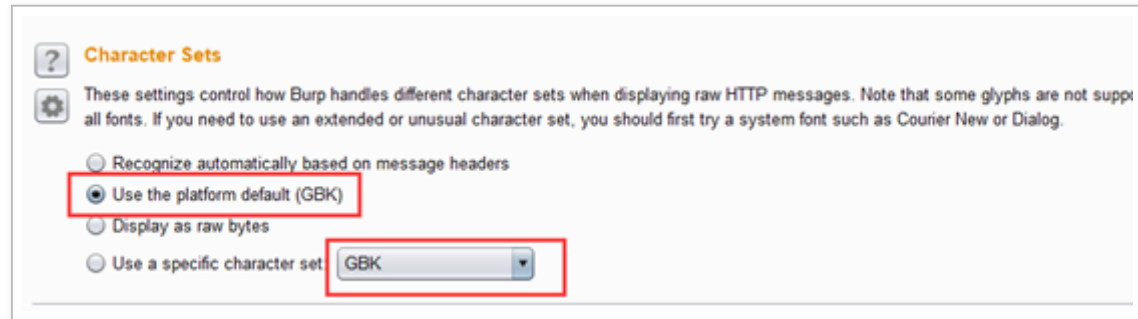


有的人可能会认为是 character set 的问题，我们来试一下。

默认的 character set 的选项是这样的。

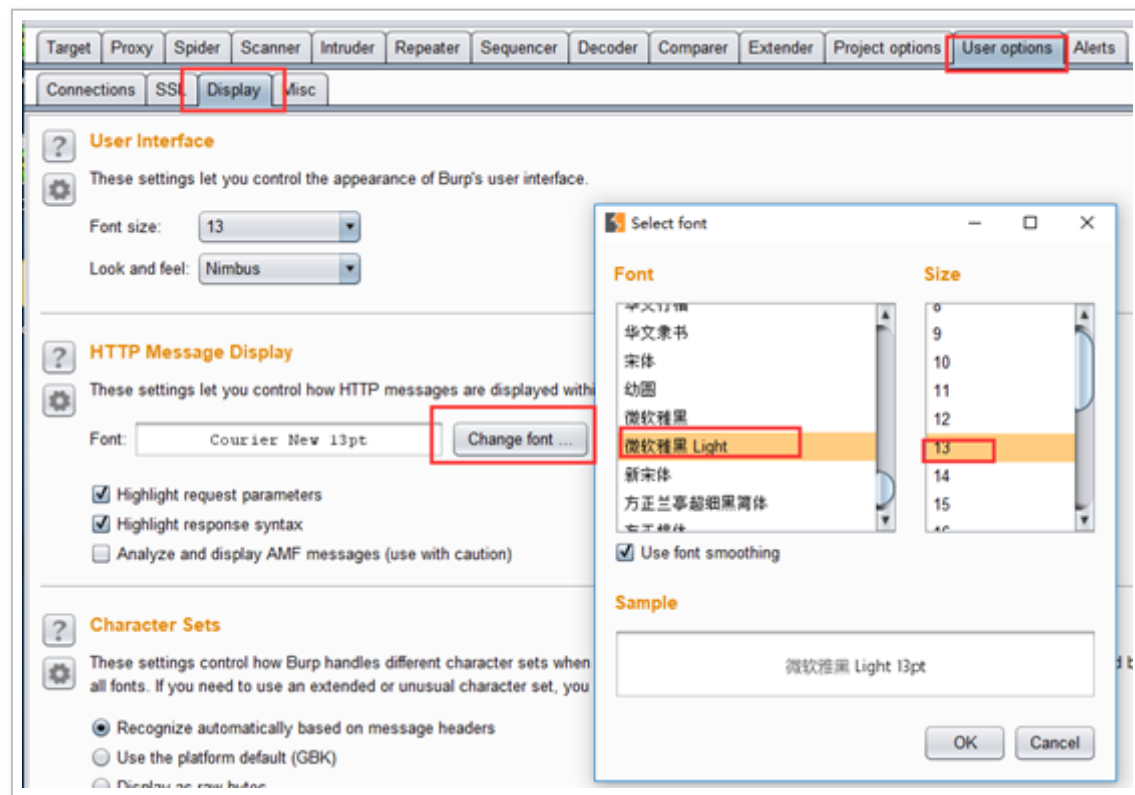


我们试着修改一下为 GBK 或者 UTF8，然而并没有什么卵用。

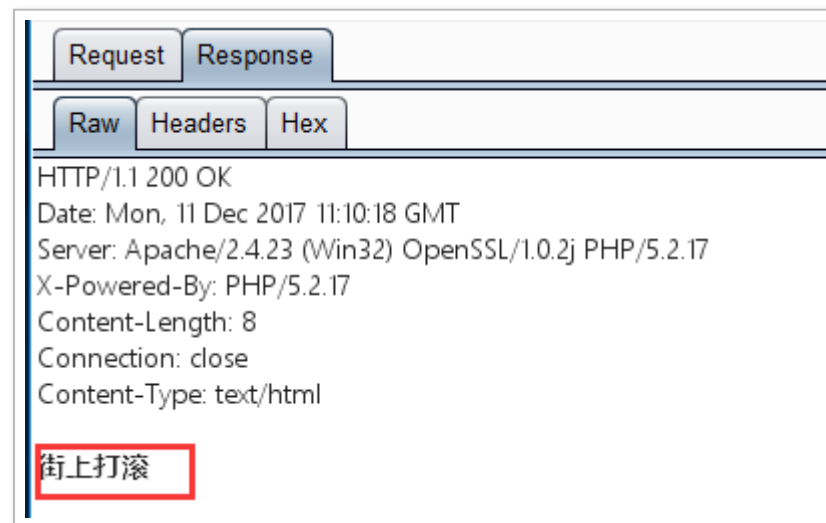


其实正确的做法是，更改显示的字体，这里我们修改为微软雅黑，当然你也可以选择宋体隶书啥的，只要支持中文的字体就 ok。





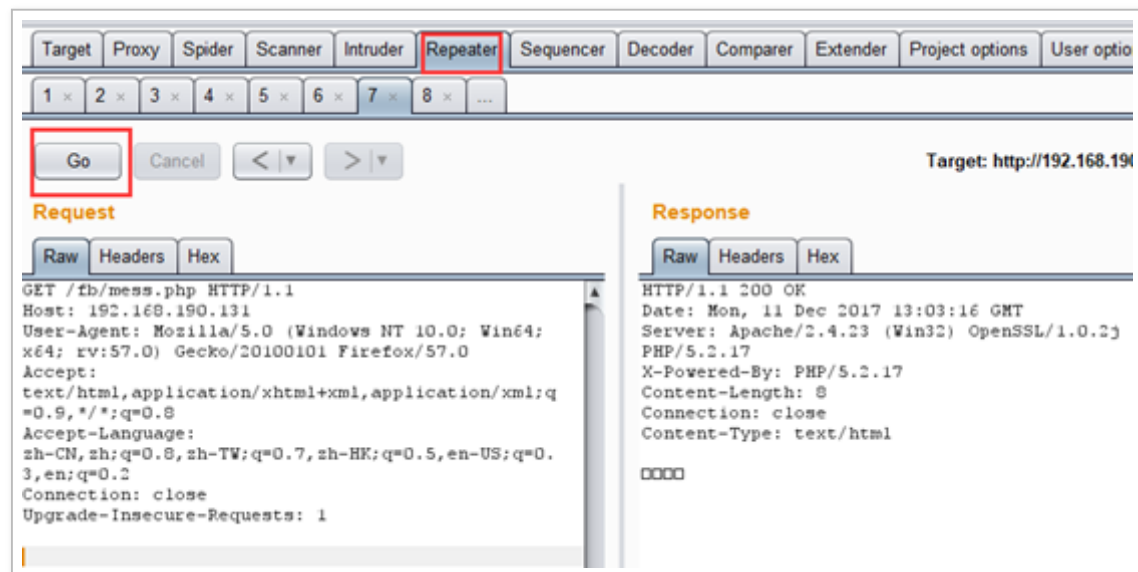
改完之后，是不是神清气爽，以后遇到各种 json 字符串的时候就不会看得蛋疼了。



0x02 burpsuite 持续重放报文

我们都知道 burpsuite 的 repeater 可以重放报文，但是有时候遇到需要持续发送某个报文问题的时候，比如时间竞争等，难道一直点 go 吗。





当然，我们可以写 python 脚本，很简单啊。

```
#!/usr/bin/python
import requests as req
url='http://192.168.190.131/fb/mess.php'
while True:
    resp=req.get(url)
```



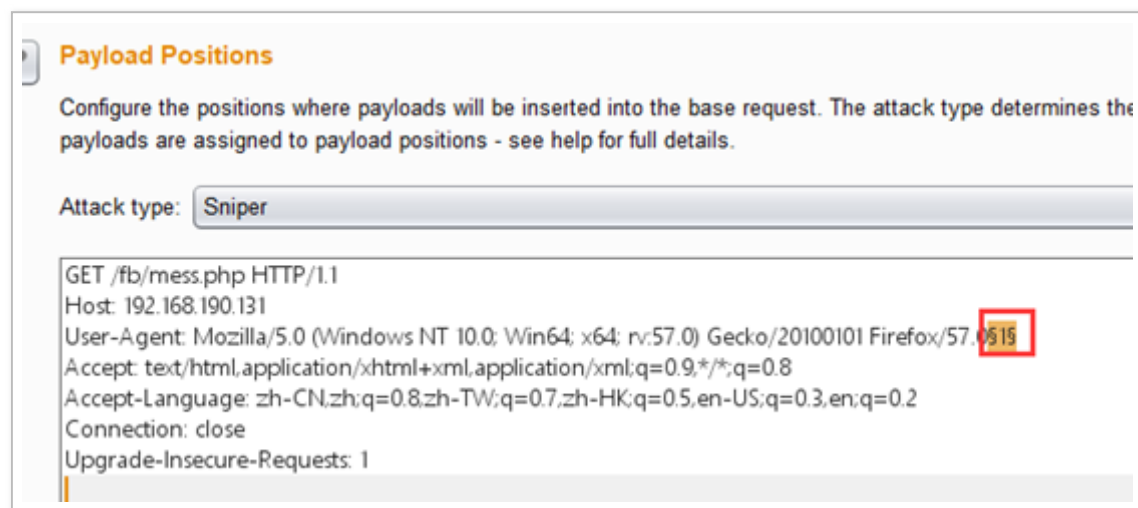
```
print resp.content
```

但是这样不够直观，输出满天飞。当然，大佬也完成增加脚本的功能来保存查看内容，进行对比，甚至写个界面来展示。自己动手丰衣足食，不过针对初学者，还是有一些技巧。其实，我们完全可以借助 burp 已有的模块完成这个功能，节省时间，输出的结果也直观具体，便于对比。

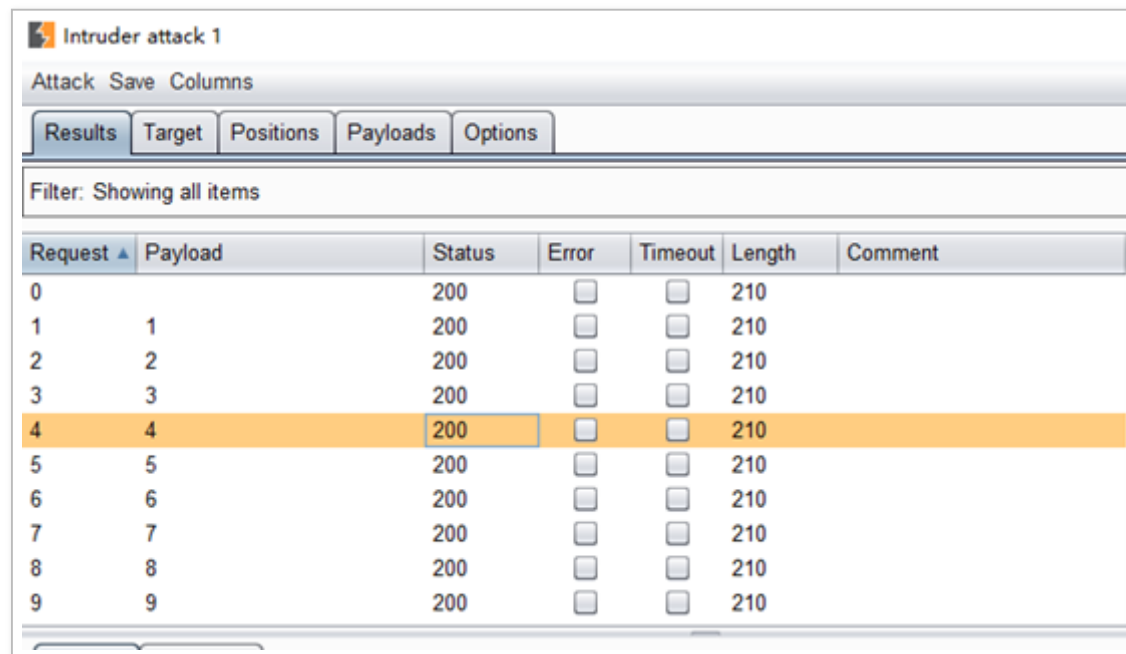
接下来是解决问题的原始版本和强迫症版本：

原始版本

我们知道 burp 有 intruder 功能，可以通过添加各种参数来重放报文，这样我们选择 intruder，在一个不会影响报文结果的位置随意添加一个参数 \$1\$。



这样就能满足我们持续重放报文的要求。



Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	210	
1	1	200	<input type="checkbox"/>	<input type="checkbox"/>	210	
2	2	200	<input type="checkbox"/>	<input type="checkbox"/>	210	
3	3	200	<input type="checkbox"/>	<input type="checkbox"/>	210	
4	4	200	<input type="checkbox"/>	<input type="checkbox"/>	210	
5	5	200	<input type="checkbox"/>	<input type="checkbox"/>	210	
6	6	200	<input type="checkbox"/>	<input type="checkbox"/>	210	
7	7	200	<input type="checkbox"/>	<input type="checkbox"/>	210	
8	8	200	<input type="checkbox"/>	<input type="checkbox"/>	210	
9	9	200	<input type="checkbox"/>	<input type="checkbox"/>	210	

强迫症版本

一般情况下这样就够了，但是强迫症患者可能不会满意，因为报文被插入了其他东西。比如 firefox 版本后面加入了 226，某些情况下可能造成 bug。

226	226	200	<input type="checkbox"/>	<input type="checkbox"/>	210
227	227	200	<input type="checkbox"/>	<input type="checkbox"/>	210
228	228	200	<input type="checkbox"/>	<input type="checkbox"/>	210
229	229	200	<input type="checkbox"/>	<input type="checkbox"/>	210

Request	Response
---------	----------

Raw	Headers	Hex
-----	---------	-----


```

GET /fb/mess.php HTTP/1.1
Host: 192.168.190.131
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
Upgrade-Insecure-Requests: 1

```

如果我们想完全不插入任何东西咋整。

这样，我们可以选择 NULL payload，然后选择 continue，这样 payload count 又是 unknow，即可以发送到天荒地老。

?

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the number of requests. Various payload types are available for each payload set, and each payload type has a specific request count.

Payload set: Payload count: unknown

Payload type: Request count: unknown

?

Payload Options [Null payloads]

This payload type generates payloads whose value is an empty string. With no payload, the base request is unmodified.

☐ Generate payloads

☒ Continue indefinitely

而且报文不会有任何形式的改变。

25	null	200	<input type="checkbox"/>	<input type="checkbox"/>	210
26	null	200	<input type="checkbox"/>	<input type="checkbox"/>	210
27	null	200	<input type="checkbox"/>	<input type="checkbox"/>	210

RequestResponse

RawHeadersHex

```

GET /fb/mess.php HTTP/1.1
Host: 192.168.190.131
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Connection: close
Upgrade-Insecure-Requests: 1

```

payload 还有更多的类型和技巧，大家可以自己挖掘。

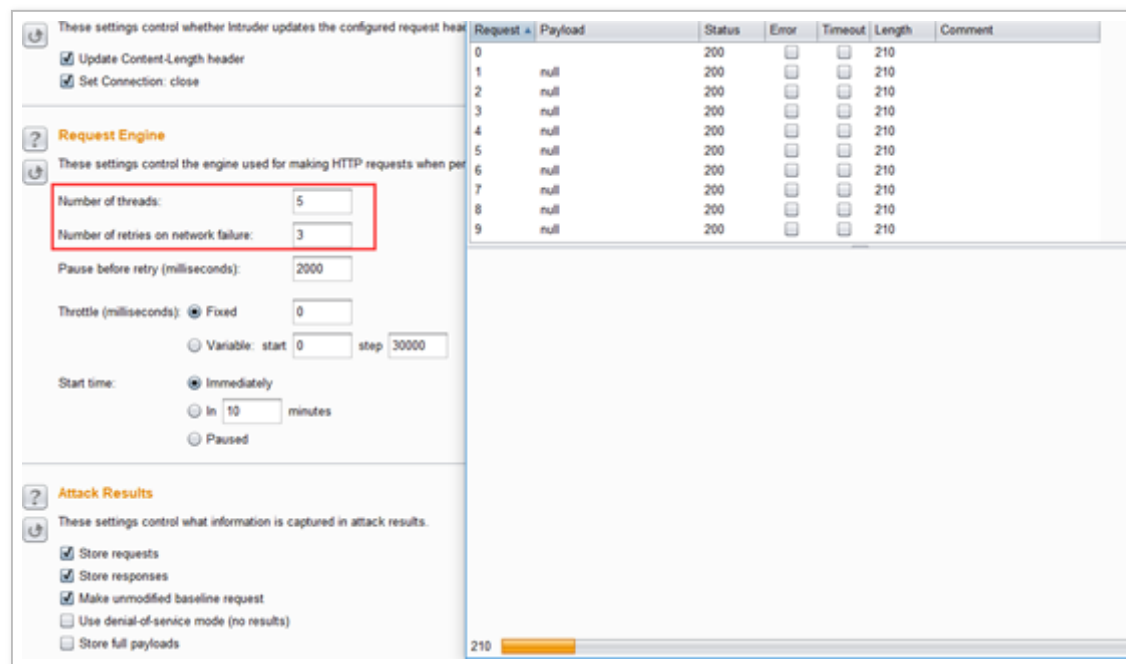
0×03 burpsuite 模拟 DOS 攻击

通过 burpsuite 也可能完成小规模 DOS 攻击，特别是在内部测试某些资源消耗型问题的时候，不需要下载各种其他工具，也不需要编写脚本。

同时使用 burpsuite intruder 攻击其他主机，也可以实现分布式攻击。

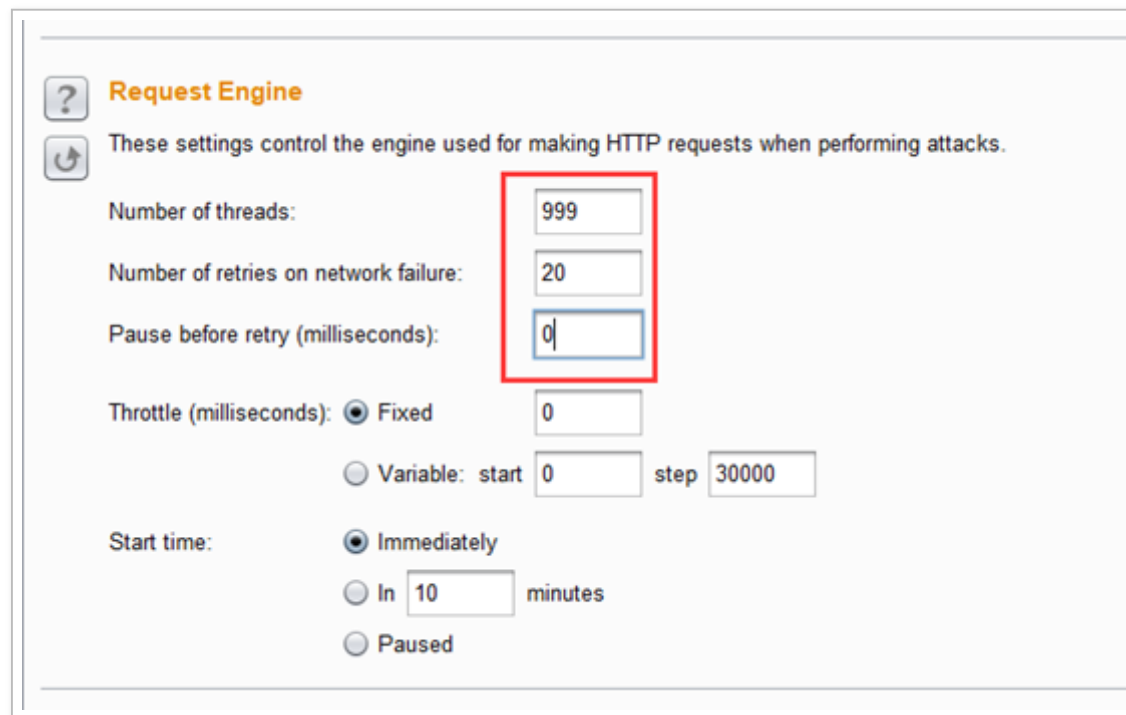
直接使用 burpsuite intruder，结合上述持续重放技巧，使用单台机器就可以造成 DOS 攻击。

普通的 instruder 配置，一般来说达不到 DOS 攻击的效果，因为默认是 5 个线程在发送报文。



实际上，我们完成修改到 100 倍以上，使得线程数量为 999，失败重试次数为 20，暂停

秒数为 0，可以完全达到小型 DOS 工具的效果，享受飞一般的感觉。



Request Engine

These settings control the engine used for making HTTP requests when performing attacks.

Number of threads: 999

Number of retries on network failure: 20

Pause before retry (milliseconds): 0

Throttle (milliseconds): ☒ Fixed 0 ☐ Variable: start 0 step 30000

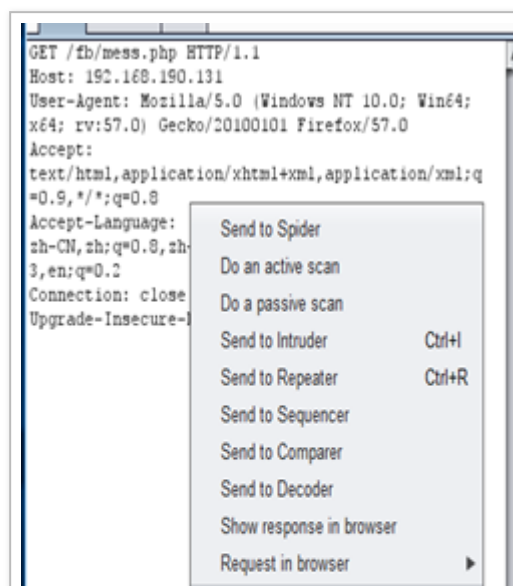
Start time: ☒ Immediately ☐ In 10 minutes ☐ Paused

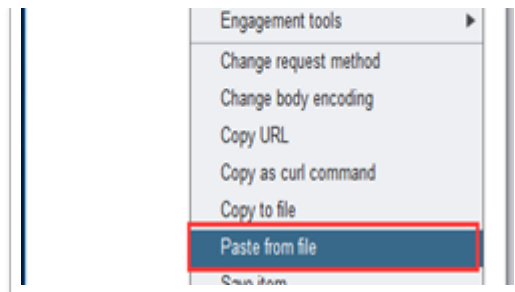
0x04 burpsuite 上传 / 直接 POST 文件

很多时候我们需要构造上传包，然后使用 burp 截获包内容改包，这样又要写一串 html。


```
</body>
<form action="http://192.168.190.137/xxx" method="post" enctype="multipart/form-data">
  <input type="file" name="uploadfile" />
  <input type="submit" value="upload" />
</form>
</body>
```

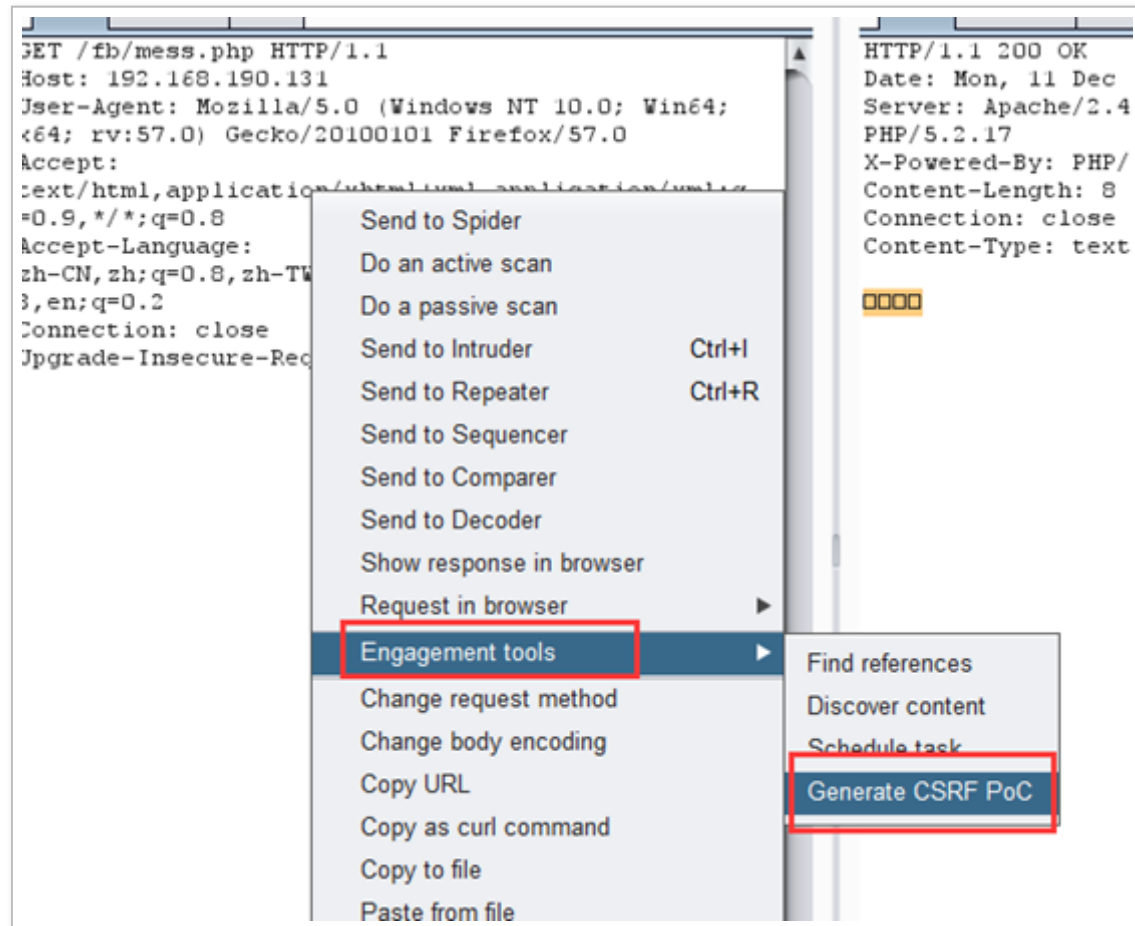
实际上，使用 burp 可以直接完成上传文件的功能，通过右键选择 paste from file 即可。



[illegible]

还有，CSRF 跨站请求伪造，又到了懒得写 html 的时候。

burpsuite 也可以帮我们完成比较简单的 form 类 csrf POC 构造。不过, 高级的 js 代码还得自己动手。



UX05 彩蛋

快过年了，burp 也过期了，咋整。动手党肯定没什么问题，搜索下 Burp 时间到期问题解决办法。

伸手党可以点击：【[传送门](#)】

感谢下大神的 release，仅供学习参考，你懂得。

如果还有更多更好的办法或者技巧，请在评论中分享，互相学习，感谢各位大佬！

* 本文作者：shadow4u，本文属 FreeBuf 原创奖励计划，未经许可禁止转载

