

攻防世界weak_auth

原创

LEO-max 于 2020-01-22 10:08:31 发布 2157 收藏 2

分类专栏: [CTF学习](#)

生活会辜负努力的人, 但不会辜负一直努力的人——Leo的个人博客。

本文链接: <https://blog.csdn.net/zouchengzhi1021/article/details/104067829>

版权



[CTF学习 专栏收录该内容](#)

32 篇文章 3 订阅

订阅专栏

此题的登入界面不知道为何做完之后就打不开了, 所以我不在这黏贴界面。

首先要我们随便输入username和password, 跳出的check.php界面要求username为admin, 所以我们只要知道密码就OK了。
用burpsuite破解

The screenshot shows the Burp Suite Professional v1.6 interface. The main window displays a list of HTTP requests. The first request is highlighted, and a context menu is open over it. The context menu options include: Add to scope, Spider from here, Do an active scan, Send to Intruder (Ctrl+I), Send to Repeater (Ctrl+R), Send to Sequencer, Send to Comparer, Request in browser, Engagement tools, Show new history window, Add comment, Highlight, Delete item, Clear history, Copy URL, Copy as curl command, Save item, and Proxy history help.

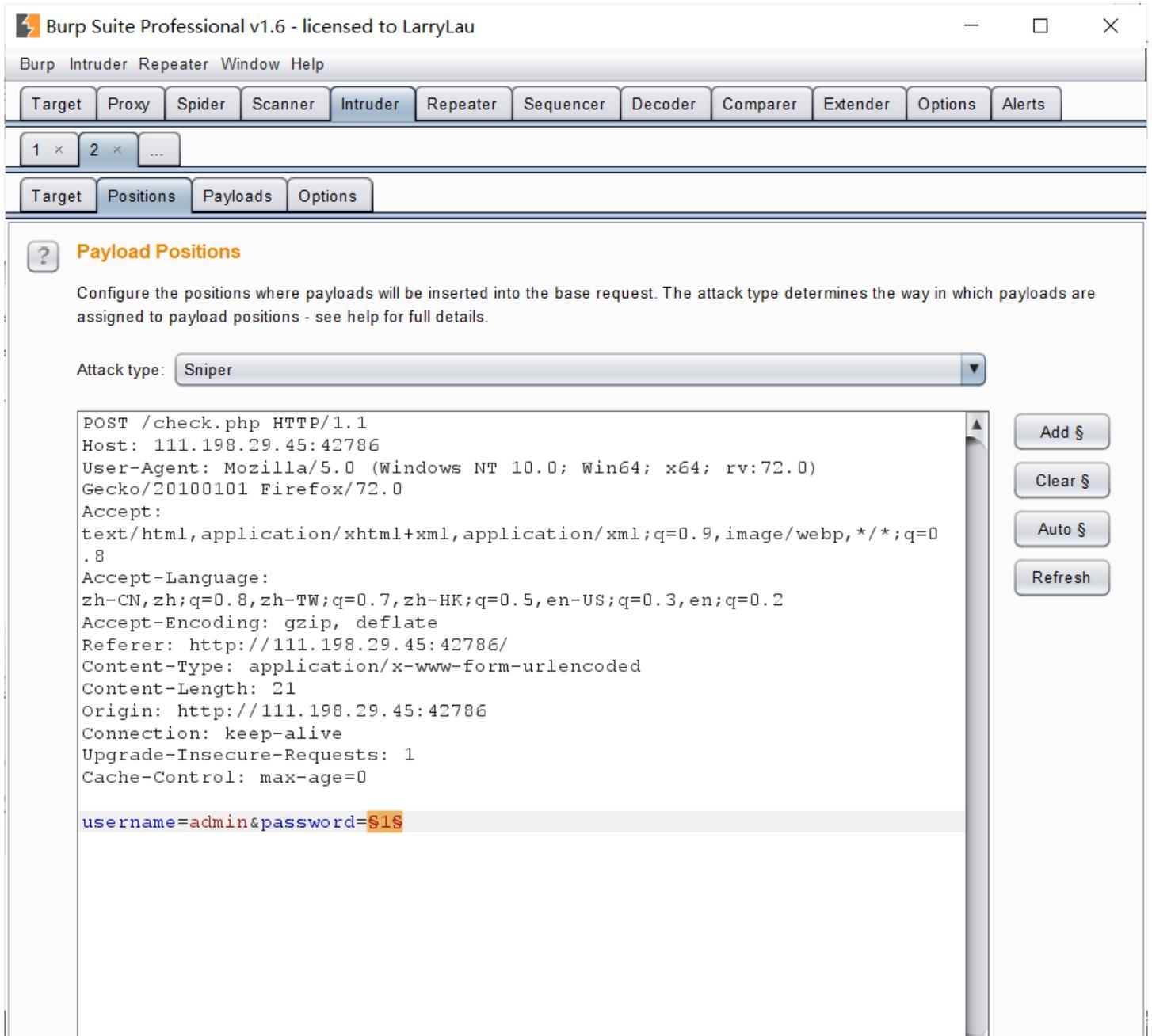
#	Host	Method	URL	Params	Edited	Status	Length	MIME 1
1	http://111.198.29.45:42786	POST	/check.php			200	384	text
2	http://detectportal.firefox.com	GET	/success	http://111.198.29.45:42786/check.php		200	384	text
3	http://detectportal.firefox.com	GET	/success			200	384	text
4	http://detectportal.firefox.com	GET	/success			200	384	text
5	http://detectportal.firefox.com	GET	/success			200	384	text
6	http://detectportal.firefox.com	GET	/success			200	384	text
7	http://detectportal.firefox.com	GET	/success			200	384	text
8	http://detectportal.firefox.com	GET	/success			200	384	text
9	http://detectportal.firefox.com	GET	/success			200	384	text
10	http://detectportal.firefox.com	GET	/success			200	384	text
11	http://detectportal.firefox.com	GET	/success			200	384	text

Request details:

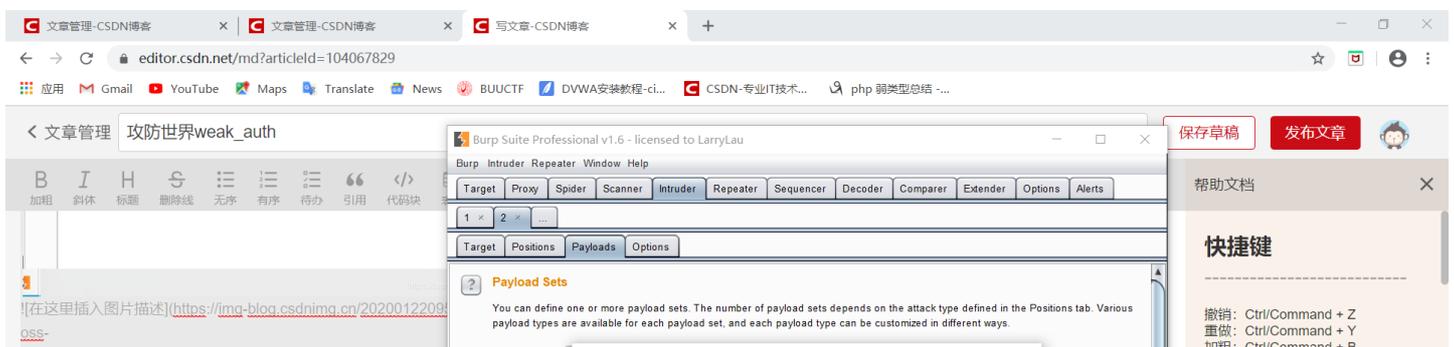
```
POST /check.php HTTP/1.1
Host: 111.198.29.45:42786
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.3,en-US;q=0.5,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://111.198.29.45:42786/
Content-Type: application/x-www-form-urlencoded
Content-Length: 21
Origin: http://111.198.29.45:42786
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

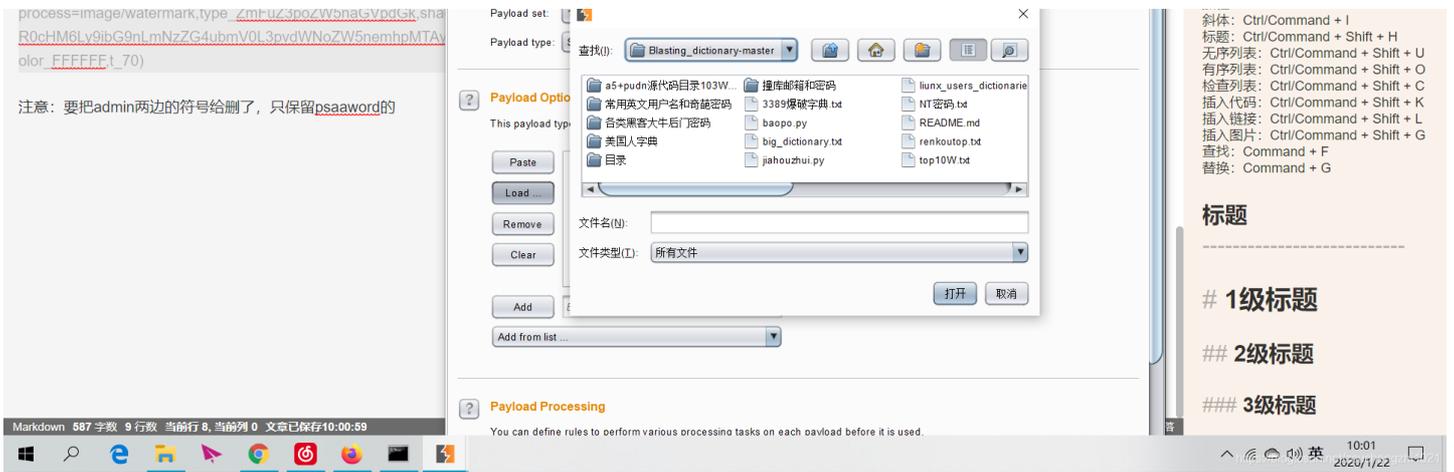
username=1&password=1
```

打开intruder选项卡

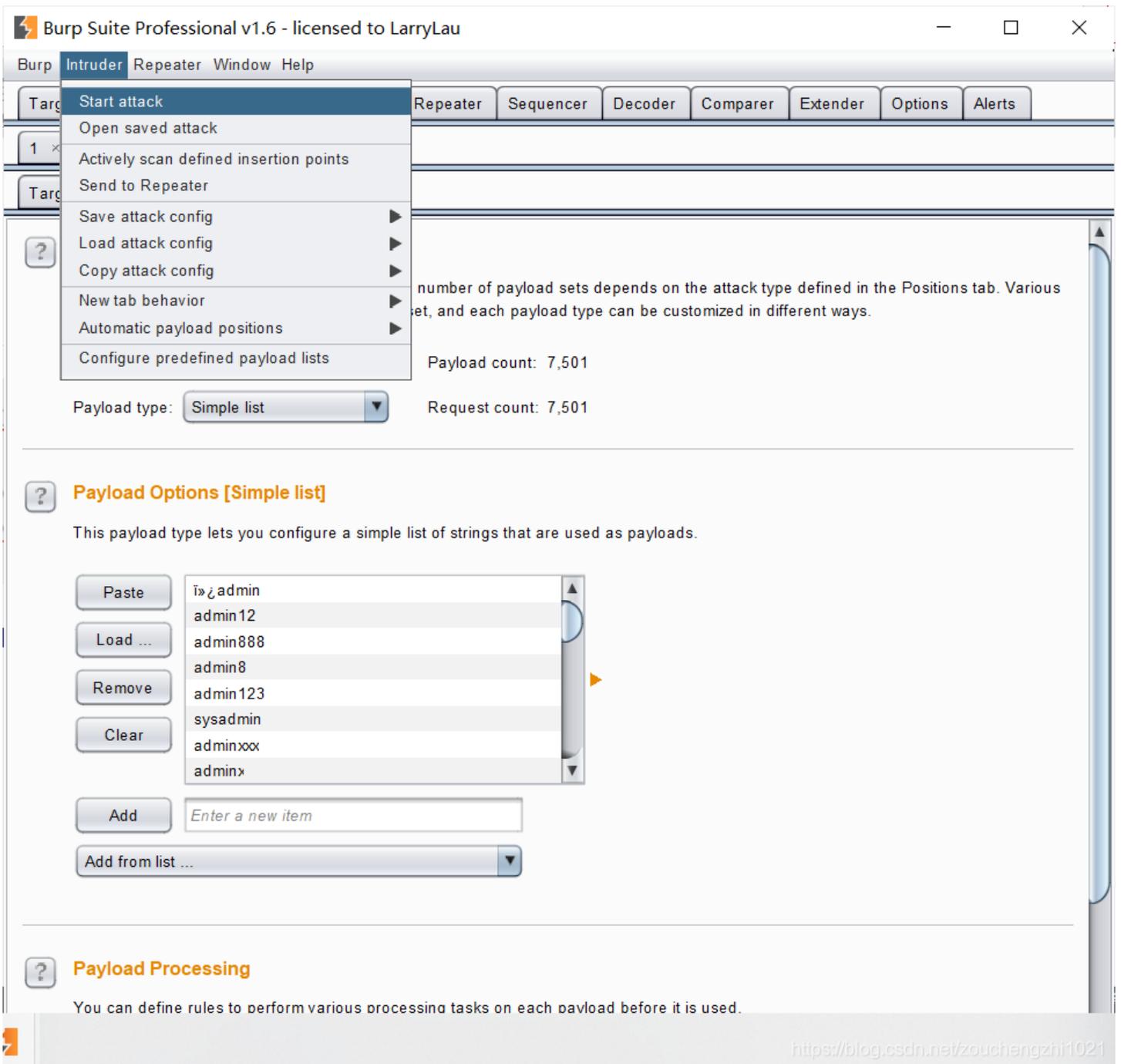


注意：要把admin两边的符号给删了，只保留psaaword的

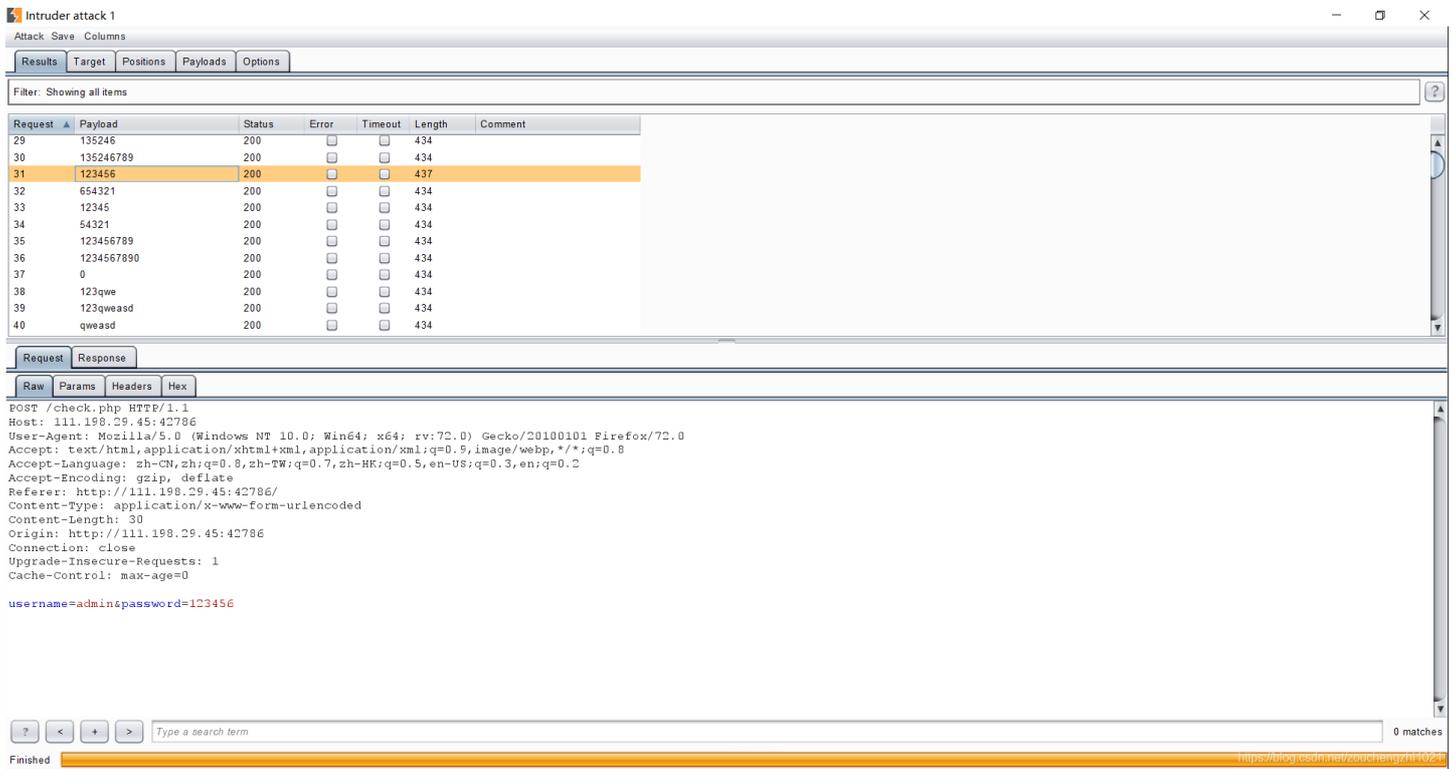




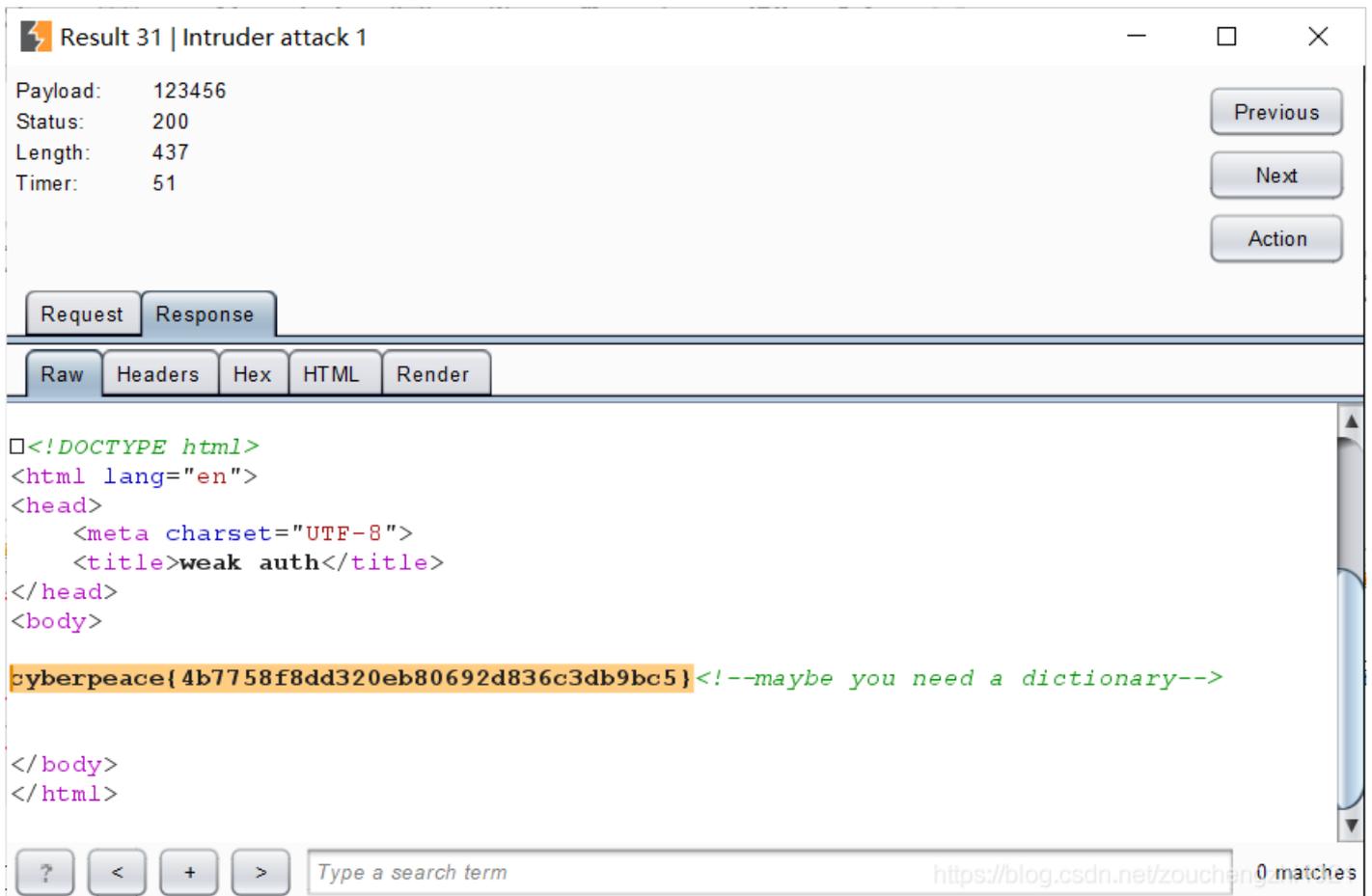
进入Payloads选项卡，在Payloads Option 中选中load，找到你下载的字典。



在上方的intruder中选中start attack进行爆破



在出现的result界面中进行一系列字典密码进行尝试，我们需要找到Lenth不同的密码，这个密码就是正确密码。



打开正确密码的界面就可拿到flag.

我写博客习惯先黏贴图片再进行解释，嘻嘻嘻嘻。