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

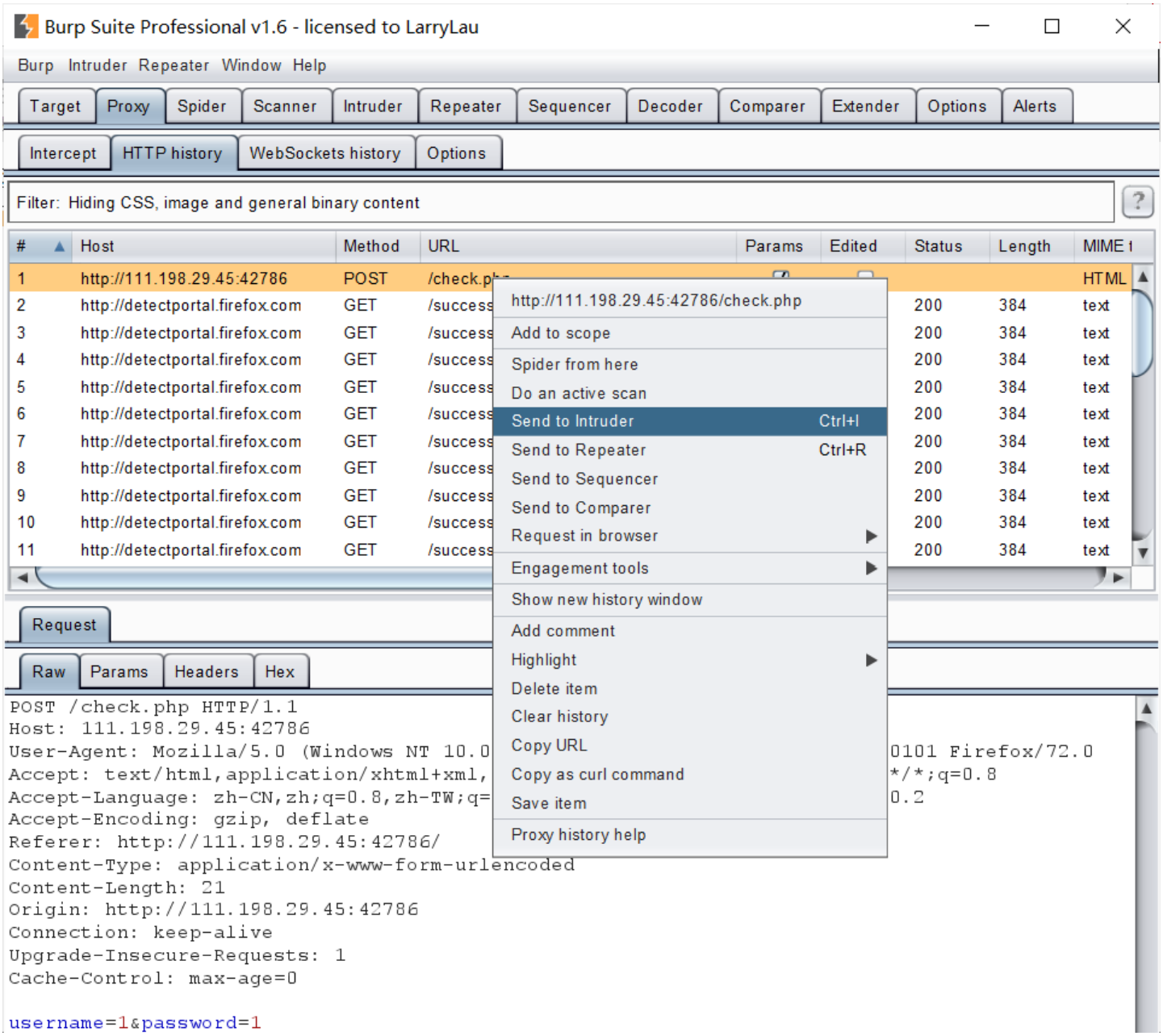
生活会辜负努力的人，但不会辜负一直努力的人——Leo的个人博客。

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

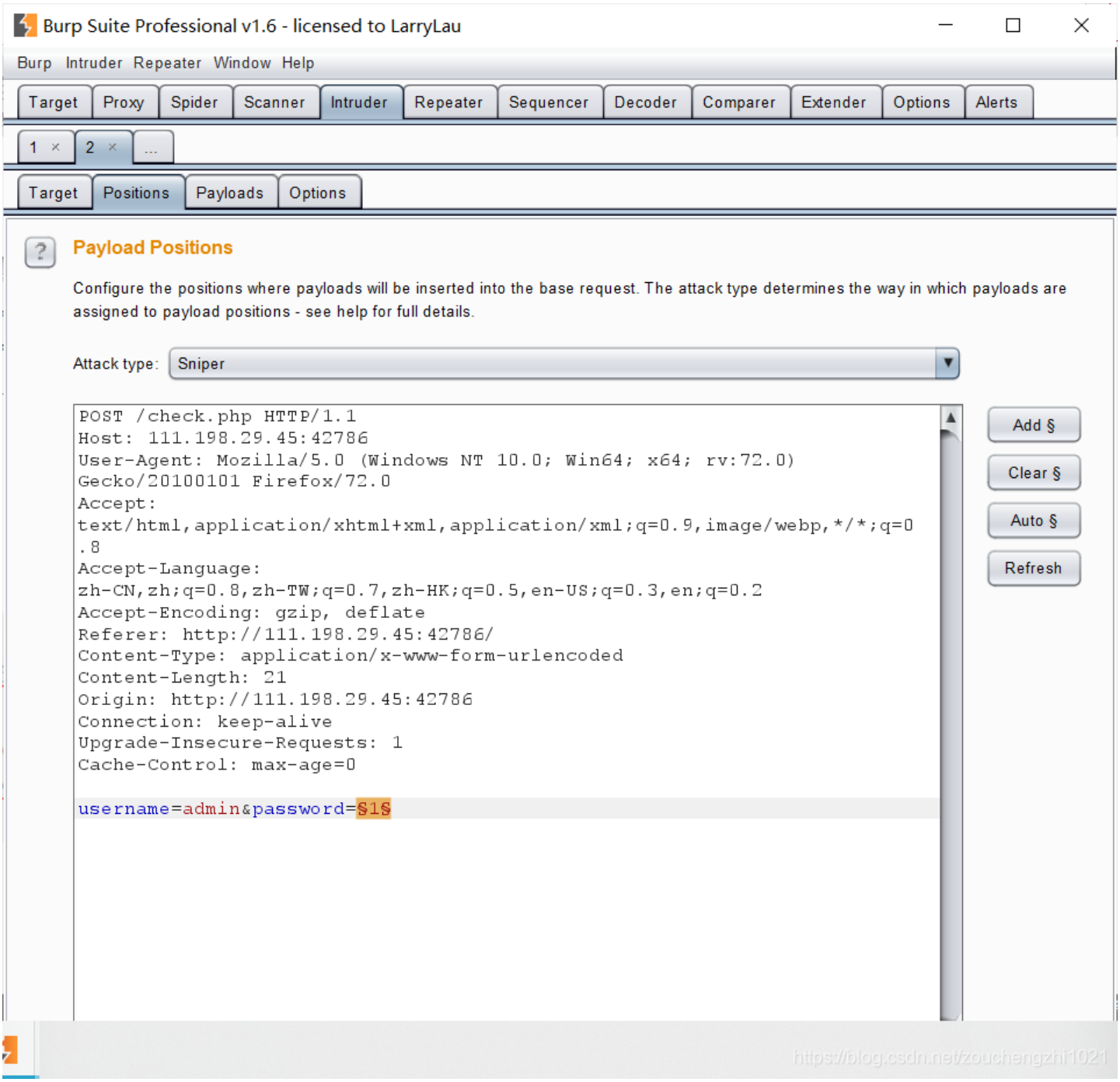
此题的登入界面不知道为何做完之后就打不开了，所以我就不在这黏贴界面。

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

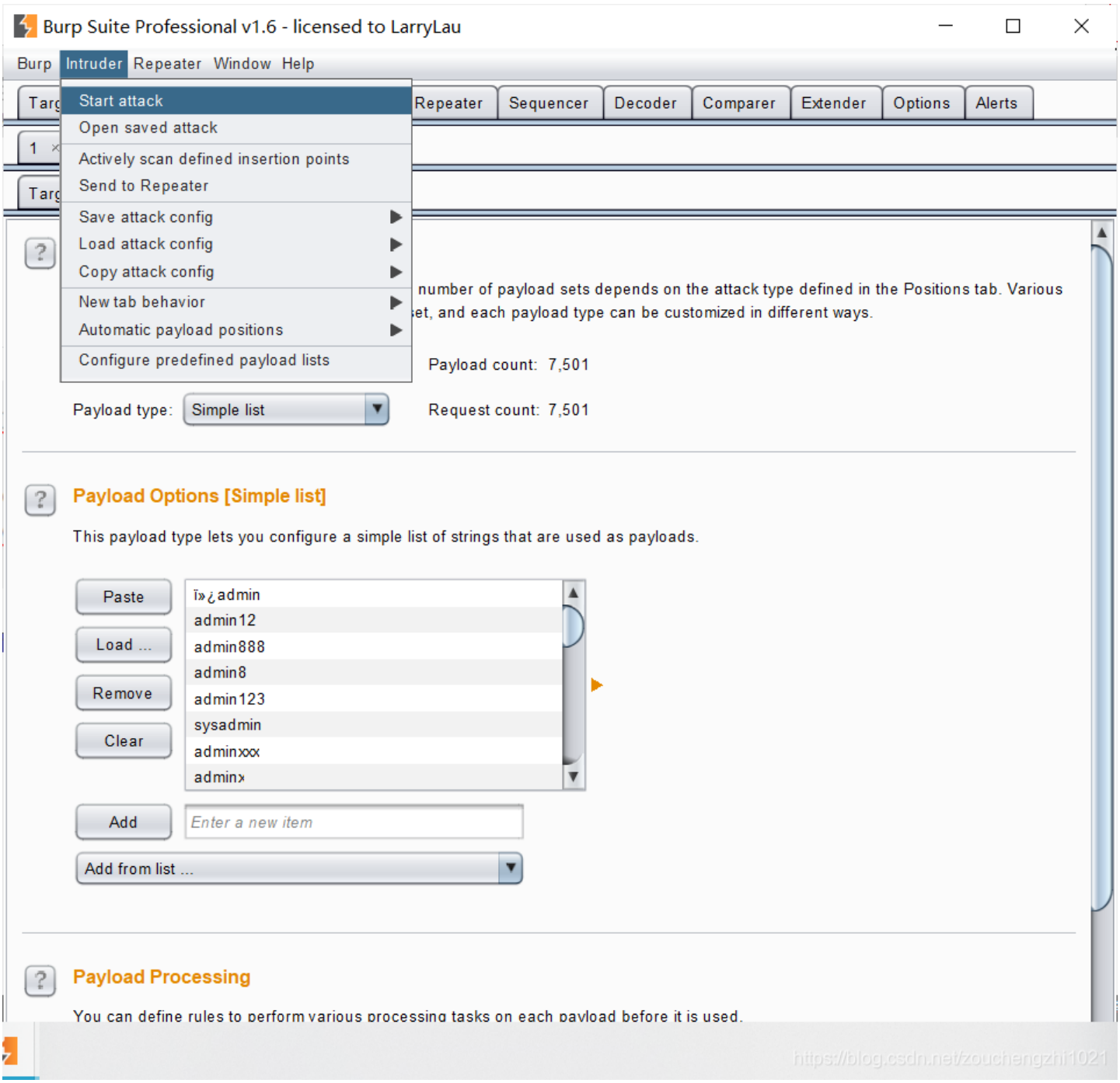


打开intruder选项卡

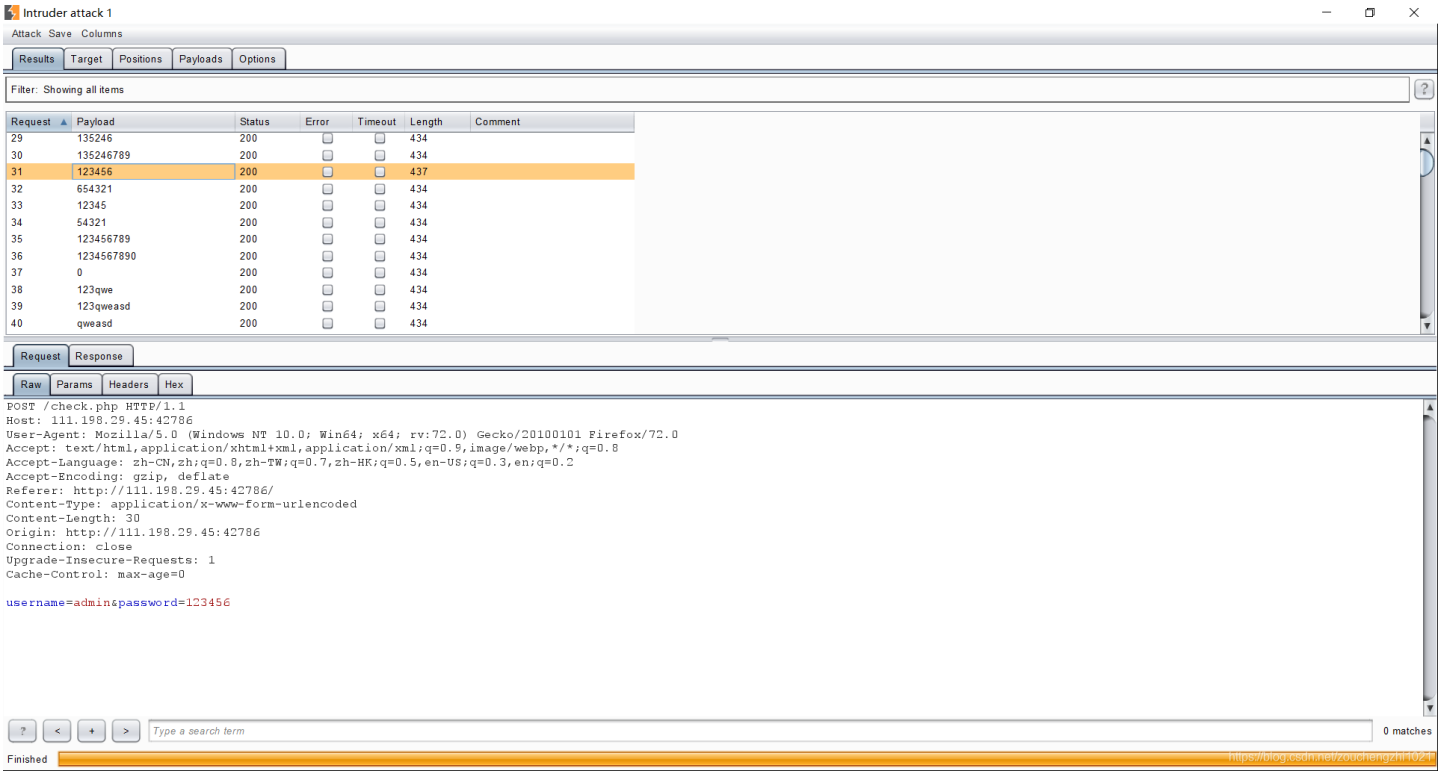


注意：要把admin两边的符号给删了，只保留psaaword的

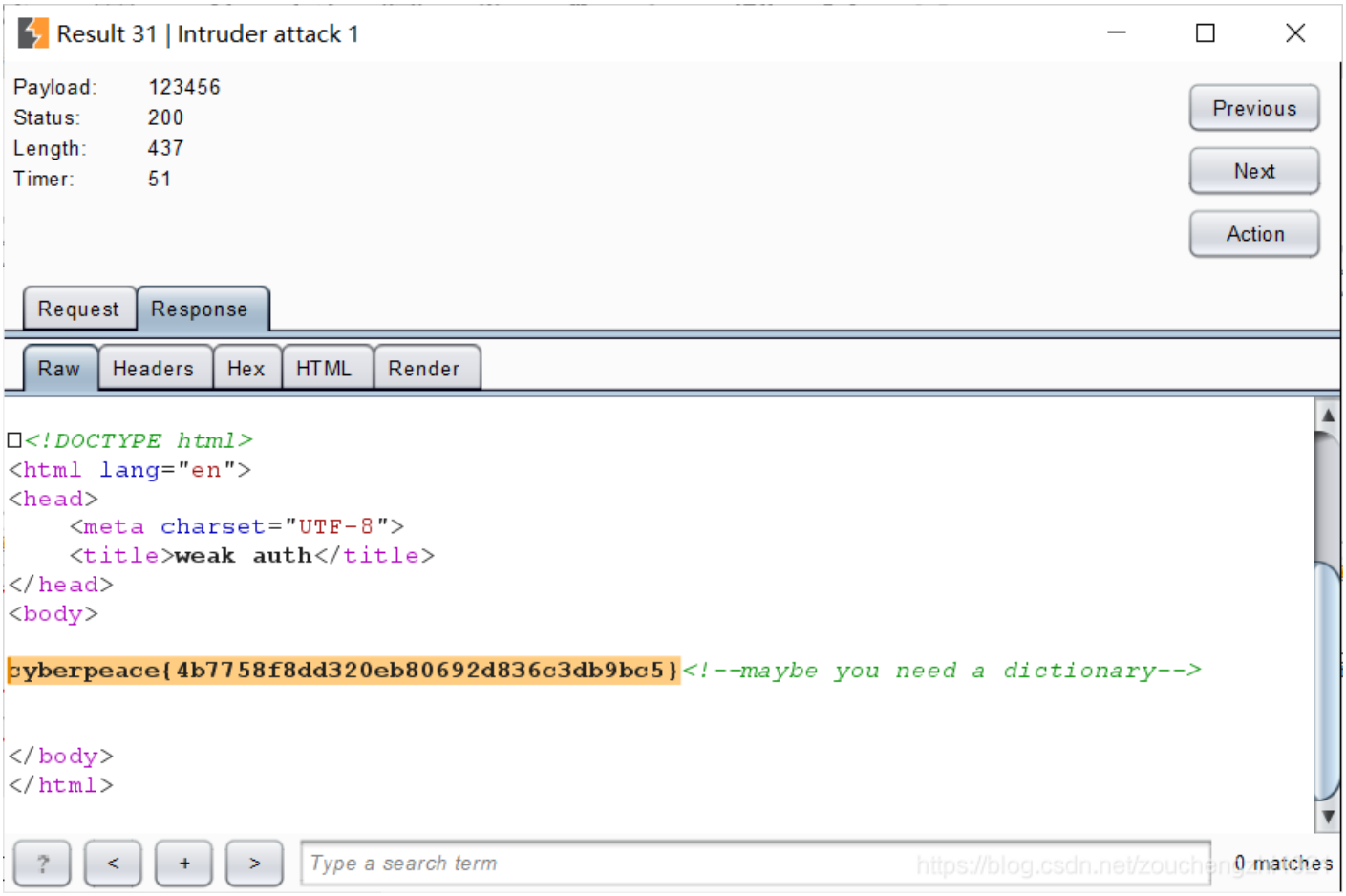
进入Payloads选项卡，在Payloads Option 中选中load，找到你下载的字典。



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。