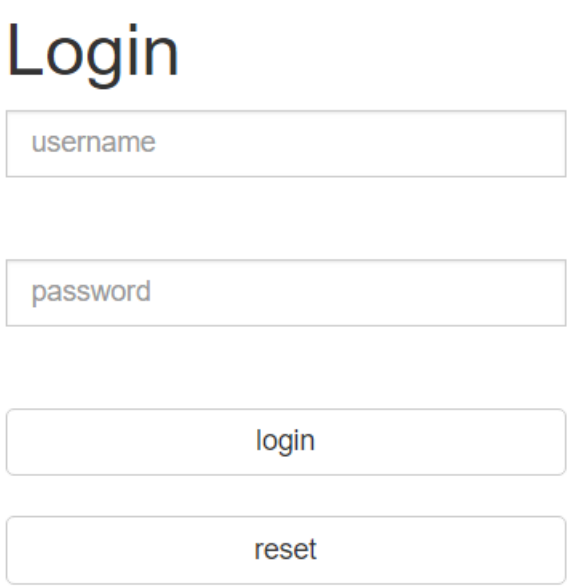
攻防世界（WEB）weak_auth

原创

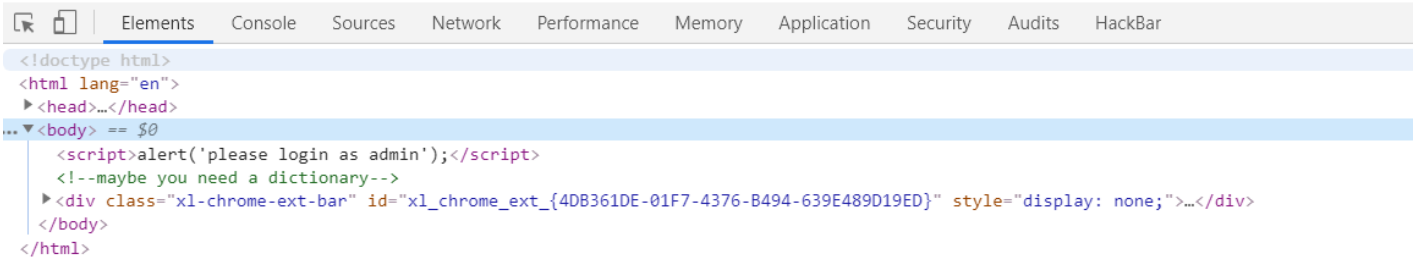
-栀蓝- 于 2021-08-24 11:12:33 发布 128 收藏

进入网页，出来一个登录注册页面



接着自己用自己的账号密码去注册试一下

结果点击login后出来一个提示弹窗：请用admin账号登录，但是我们不知道密码，我在这个时候也很莫名其妙的，没有碰过这种题目，便想着打开一下F12看看还有没有提示

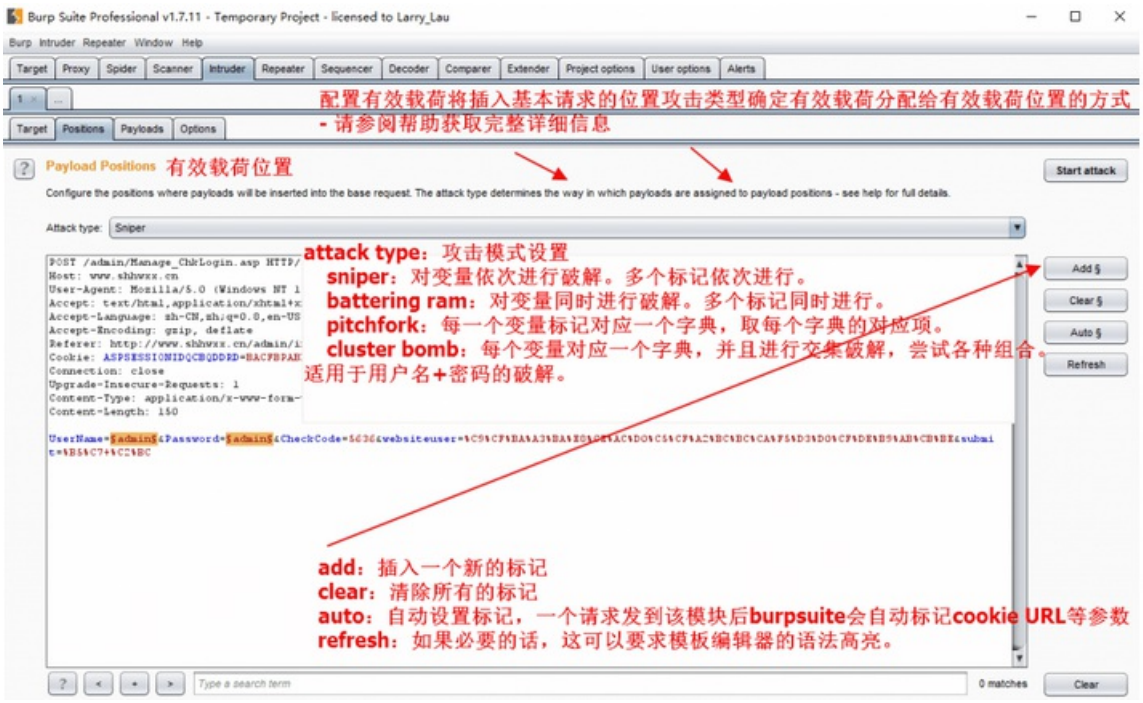


发现有个注释，可能你需要**字典**。

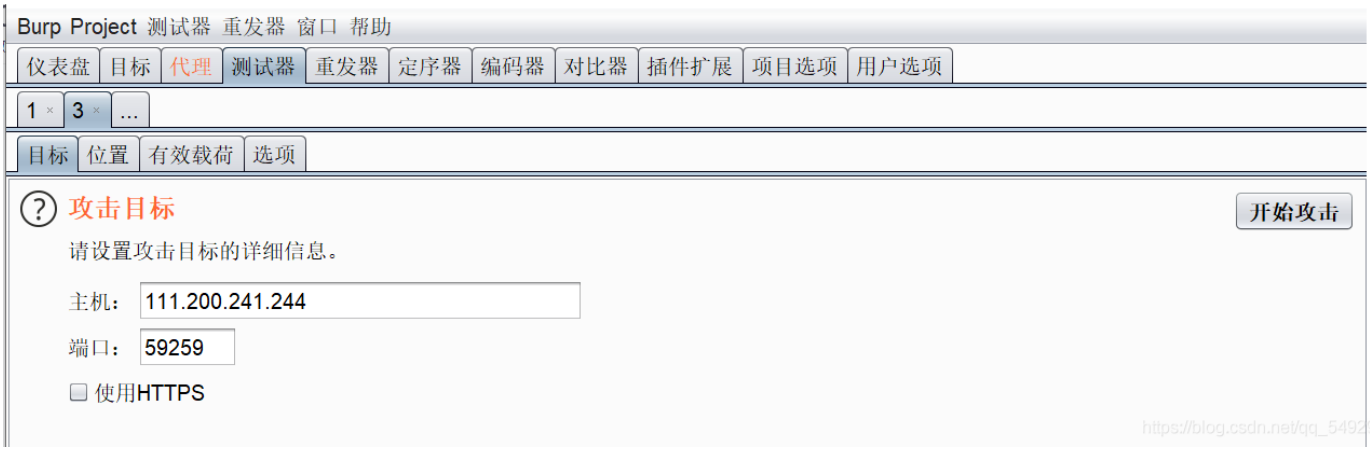
第一时间我以为密码是要像字典那样，但我心想那么多数字字母，我怎么知道，然后上网查询了一下，原来这里提示我们要字典是要进行**密码爆破（第一次接触这玩意儿）**

按照搜的教程学习怎么进行爆破https://jingyan.baidu.com/article/ca41422f054c881eae99eda0.html

转载网上一张功能介绍图片



在抓取的请求中，右键点击发送到intruder（侵入者）



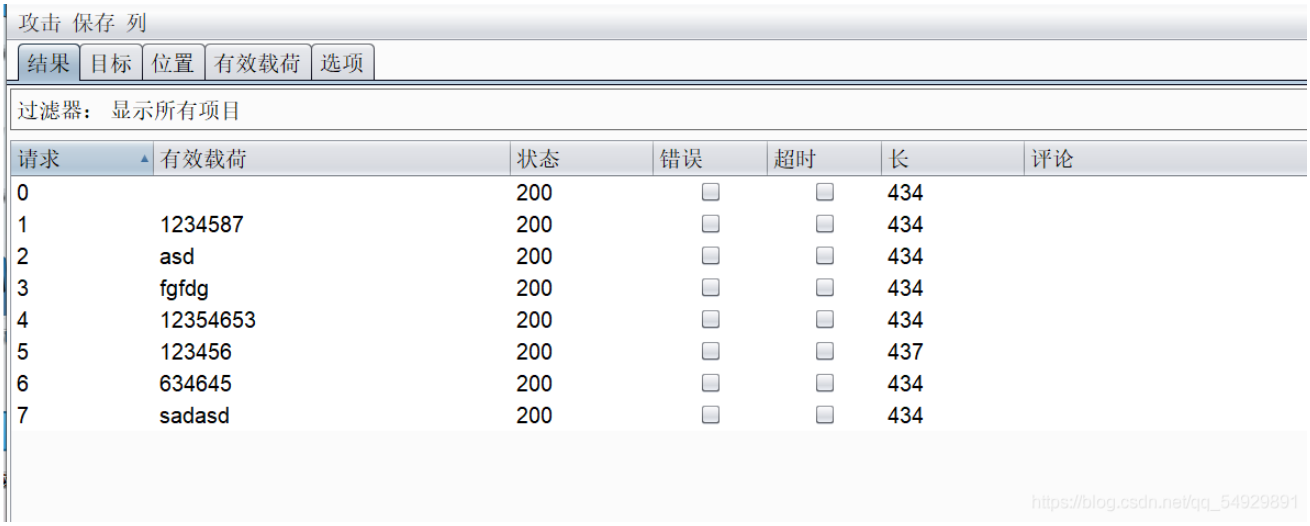
然后我直接点击开始攻击，显示字典是空的，然后点击有效载荷

点击载入中，可以在网上下载一些**密码字典**，因为数据很多，载入的时候会要一点时间，这里节约时间，我就随便自己添加几个和密码

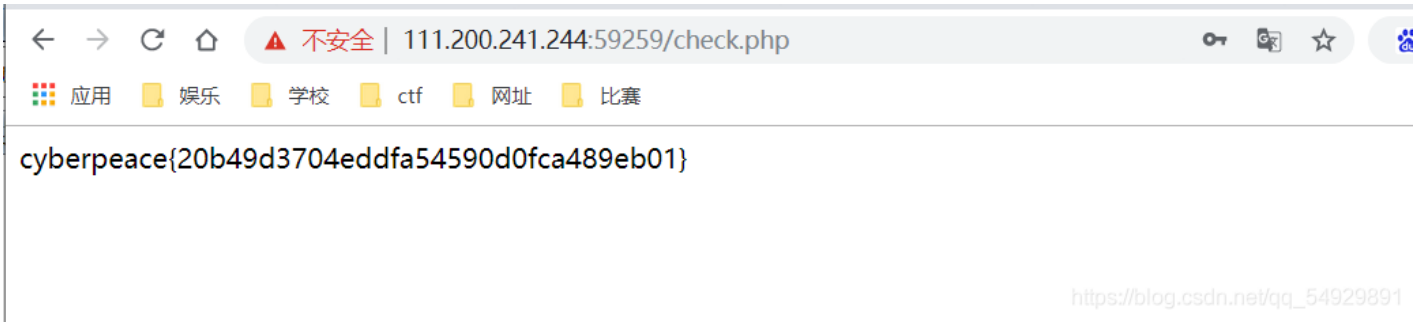
切记一定要**点击位置**

因为你username已经知道是admin，将他旁边的两个符号 §去掉，只留下password的，要爆破的地方会有一个绿色的框框（§符号之间代表要爆破的位置§）

点击开始攻击



发现自己输入的密码只有一个那个长与其他密码是不一样的，便可以猜想这个123456就是密码，尝试输入一下



flag就出来了，因为是新手题目，也没有设很多关卡，不然不随随便便就把别人的账号密码盗了哈哈哈哈哈，可以说这个题目让我长见识了，随着题目一点一点学习