

攻防世界（WEB）weak_auth

原创

[-枢蓝-](#) 于 2021-08-24 11:12:33 发布 128 收藏

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/qq_54929891/article/details/119885447

版权

进入网页，出来一个登录注册页面

Login

https://blog.csdn.net/qq_54929891

接着自己用自己的账号密码去注册试一下

111.200.241.244:59259 显示

please login as admin

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

```
<!doctype html>
<html lang="en">
  <head>...</head>
  <body> == $0
    <script>alert('please login as admin');</script>
    <!--maybe you need a dictionary-->
    <div class="xl-chrome-ext-ban" id="xl_chrome_ext_{4DB361DE-01F7-4376-B494-639E489D19ED}" style="display: none;">...</div>
  </body>
</html>
```

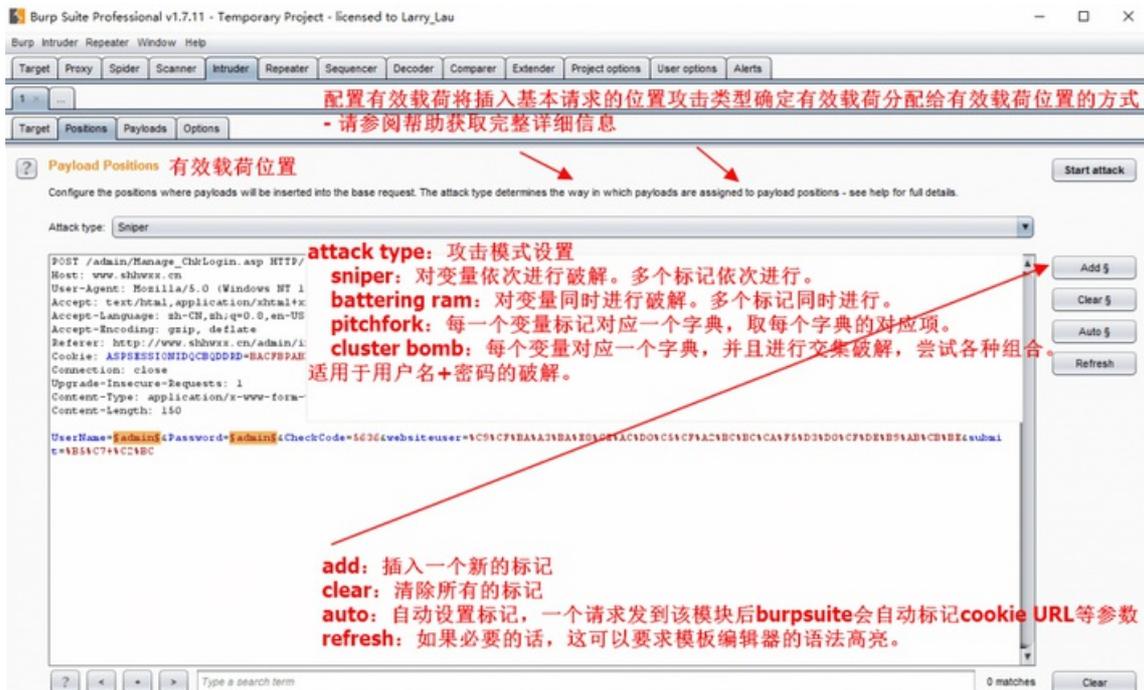
https://blog.csdn.net/qq_54929891

发现有个注释，可能你需要字典。

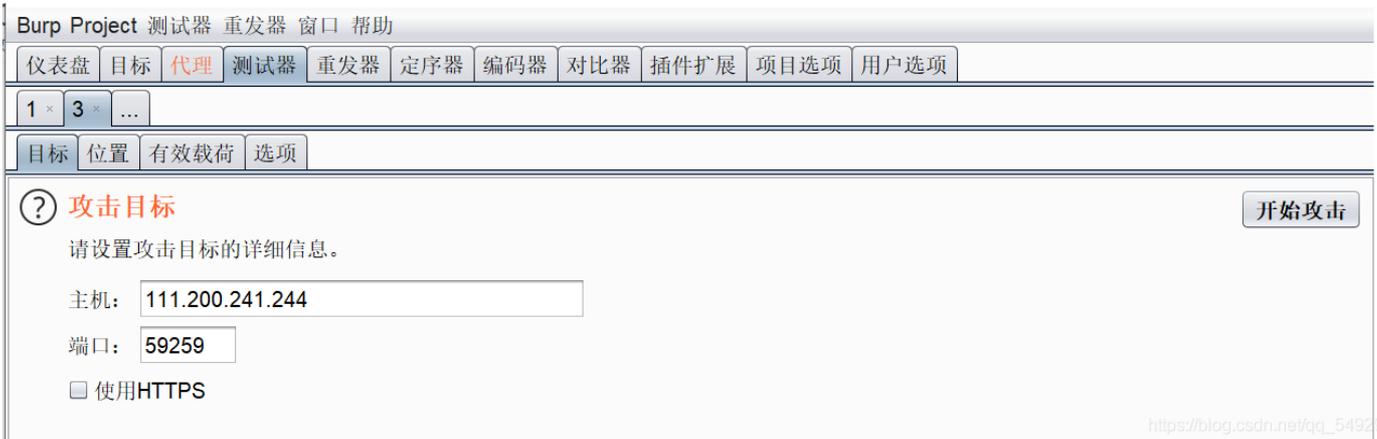
第一时间我以为密码是要像字典那样，但我心想那么多数字字母，我怎么知道，然后上网查询了一下，原来这里提示我们要字典是要进行密码爆破（第一次接触这玩意儿）

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）



https://blog.csdn.net/qq_54929891

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

? 有效载荷选项[简单列表]

设置用于有效内容的简单字符串列表。

| | |
|-----------|----------------------|
| 粘贴 | 998877665544332211 |
| 载入中..... | 00998877665544332211 |
| 删除 | 887766554433221100 |
| 清屏 | 99887766554433221100 |
| 添加 | 00880088 |
| | 3132353933 |
| | 输入新项目 |
| 从列表中添加... | |

https://blog.csdn.net/qq_54929891

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

? 有效载荷选项[简单列表]

设置用于有效内容的简单字符串列表。

| | |
|-----------|----------|
| 粘贴 | 1234587 |
| 载入中..... | asd |
| 删除 | fgfdg |
| 清屏 | 12354653 |
| 添加 | 123456 |
| | 634645 |
| | |
| 从列表中添加... | |

https://blog.csdn.net/qq_54929891

切记一定要点击位置

目标 位置 有效载荷 选项

有效负载位置 开始攻击

设置在基本请求中插入有效负载的位置。攻击类型指定如何将有效负载分配给有效负载位置。 - 有关详细信息，请参阅帮助。

攻击类型: **狙击手 (Sniper)**

```
POST /check.php HTTP/1.1
Host: 111.200.241.244:59259
Content-Length: 27
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.0.8793 Safari/537.36
Origin: http://111.200.241.244:59259/
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://111.200.241.244:59259/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,fr;q=0.8
Connection: close

username=admin&password=§123§
```

添加 §
§清除
自动§
刷新

https://blog.csdn.net/qq_54929891

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

攻击 保存 列

结果 目标 位置 有效载荷 选项

过滤器: 显示所有项目

| 请求 | 有效载荷 | 状态 | 错误 | 超时 | 长 | 评论 |
|----|----------|-----|--------------------------|--------------------------|-----|----|
| 0 | | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 434 | |
| 1 | 1234587 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 434 | |
| 2 | asd | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 434 | |
| 3 | fgfdg | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 434 | |
| 4 | 12354653 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 434 | |
| 5 | 123456 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 437 | |
| 6 | 634645 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 434 | |
| 7 | sadasd | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 434 | |

https://blog.csdn.net/qq_54929891

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

← → ↻ 🏠 ⚠ 不安全 | 111.200.241.244:59259/check.php

应用 娱乐 学校 ctf 网址 比赛

cyberpeace{20b49d3704eddfa54590d0fca489eb01}

https://blog.csdn.net/qq_54929891

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