CTF之扫描后台

原创

J0hnson666 于 2020-11-15 13:45:04 发布 1154 收藏 1

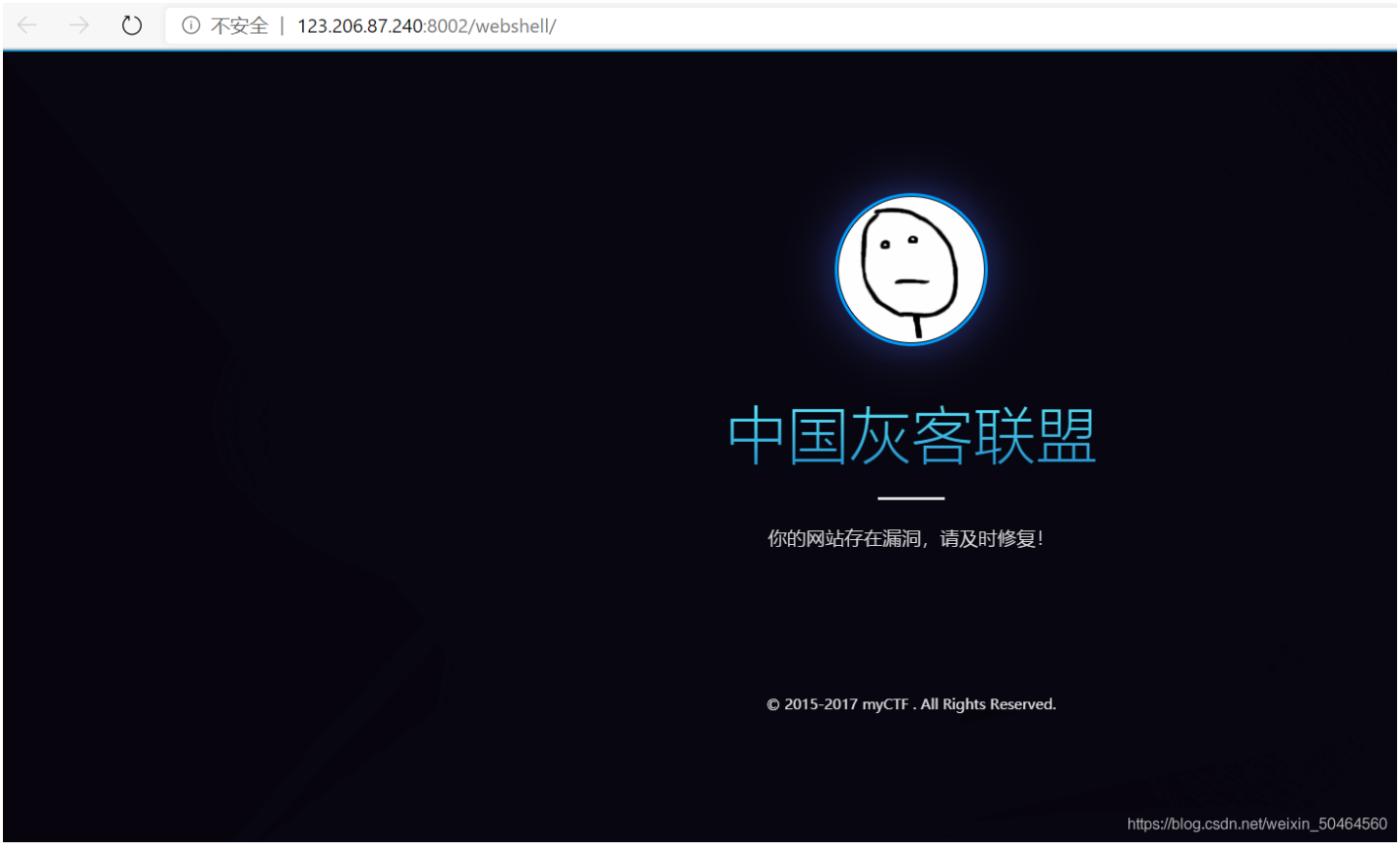
分类专栏： # CTF

本文链接：https://blog.csdn.net/weixin_50464560/article/details/109380778

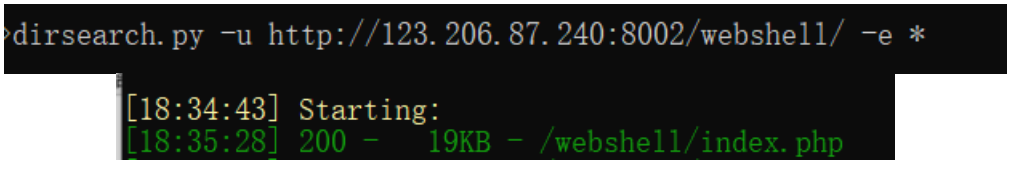
本人在freebuf的文章:https://www.freebuf.com/sectool/253708.html

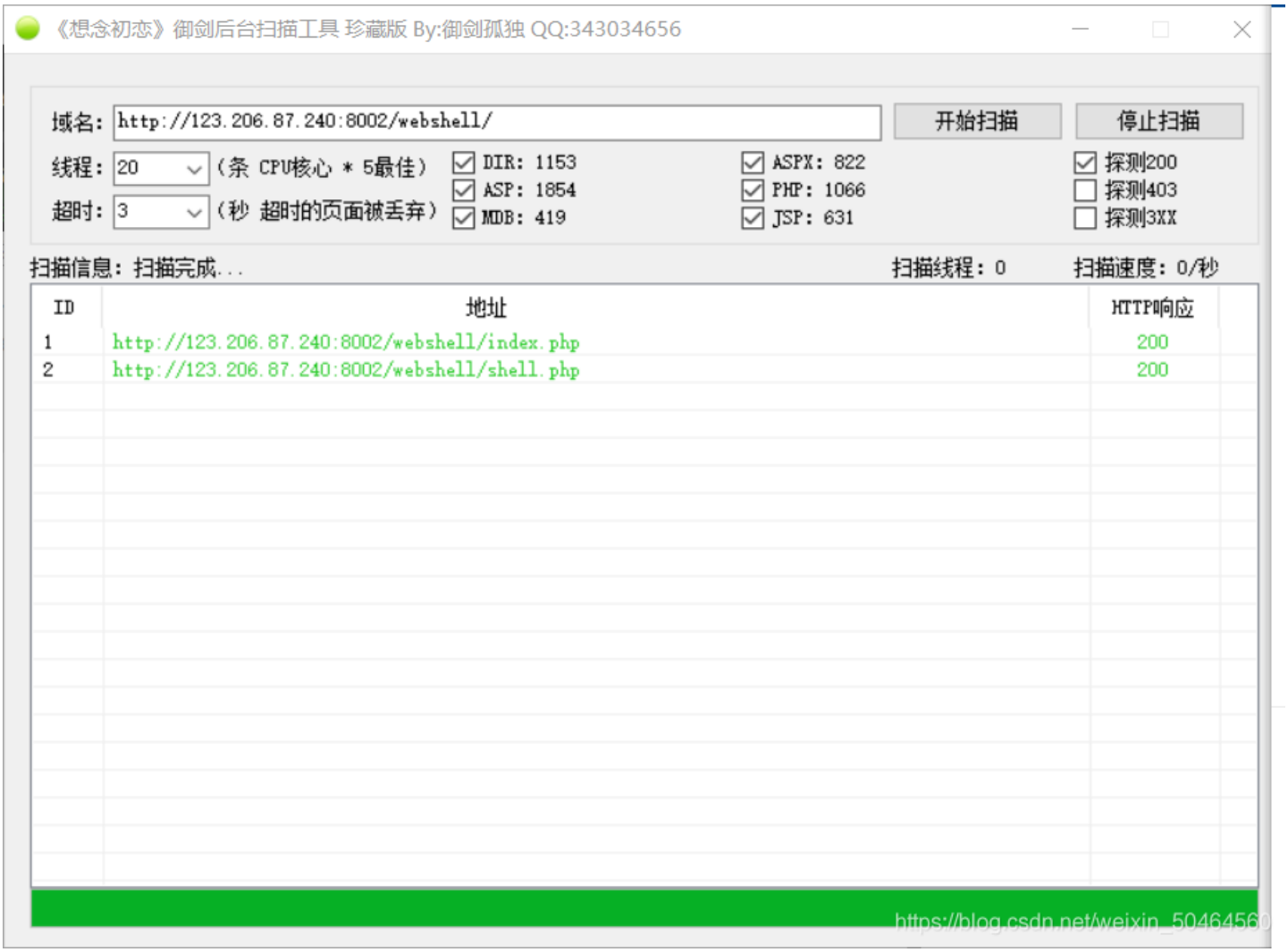
CTF之扫描后台

去底部



1、首先进入题目，题目直接提示“你的网站存在漏洞，请及时修复！”这几个字，那必须要进行后台扫描了。这里我用到了dirsearch和御剑。



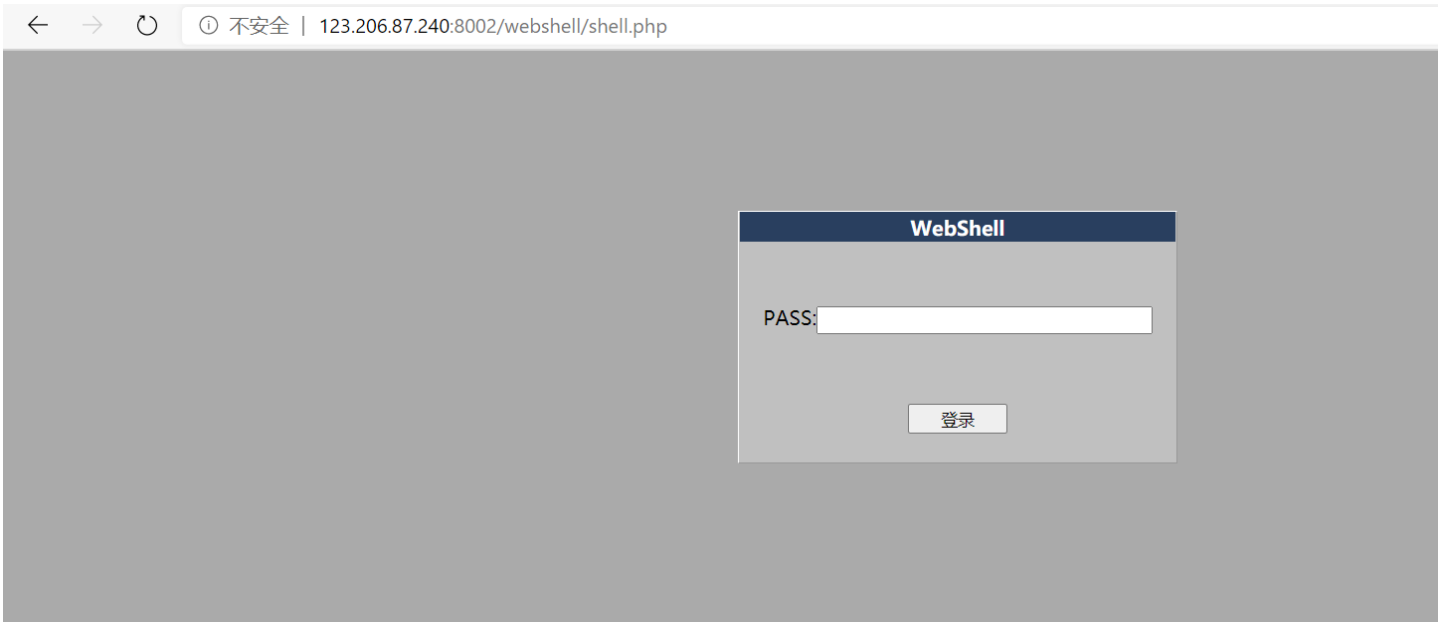


2、这里可以看到用dirsearch和御剑扫描出来的地址不一样。御剑还多了一个shell.php，这个是解题的关键。从这里可以推断出我的dirsearch里跑的字典没有御剑里的字典全面。后来我把shell.php补充到了dirsearch里的字典后，这两个就都有了。但是不得不说，这两个工具都贼好用呀

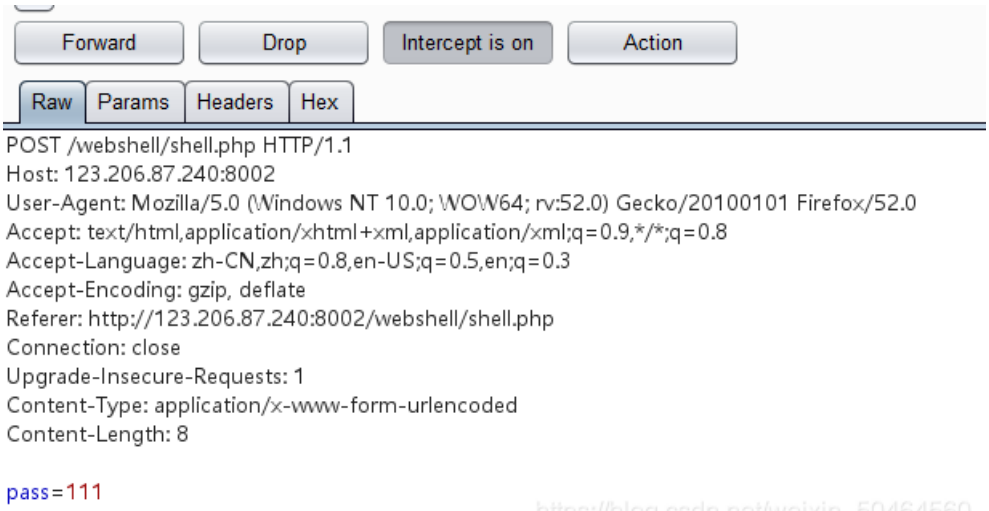
```
>dirsearch.py -u http://123.206.87.240:8002/webshell/ -e *

[18:34:43] Starting:
[18:35:28] 200 -   19KB - /webshell/index.php
[18:35:29] 200 -  954B  - /webshell/shell.php
```

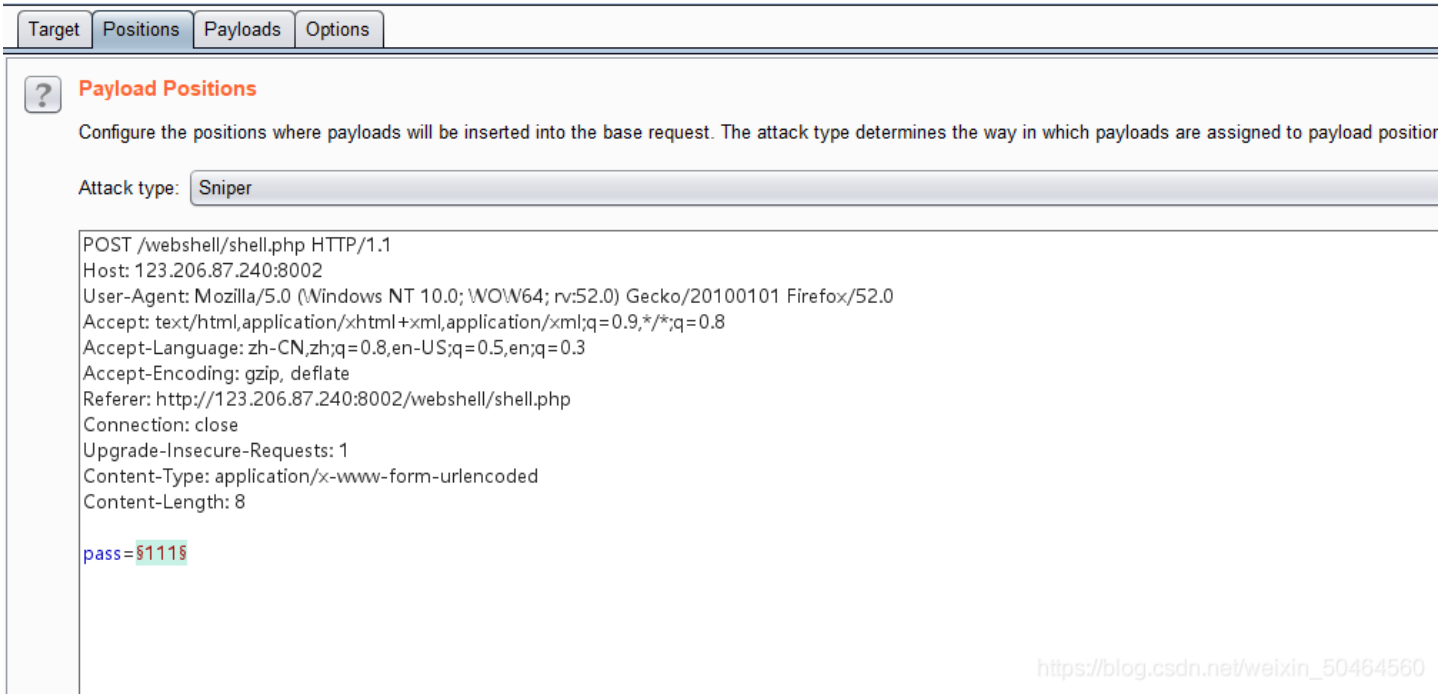
3、接下来在URL里输入shell.php，便返回了该后门



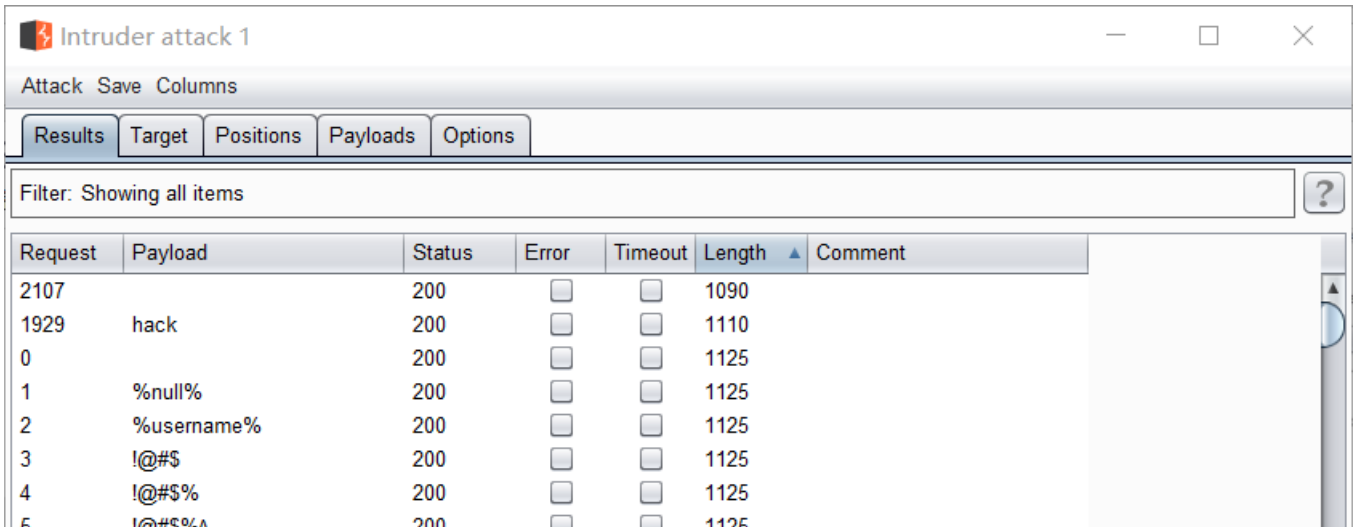
4、这里直接用burp suite进行爆破

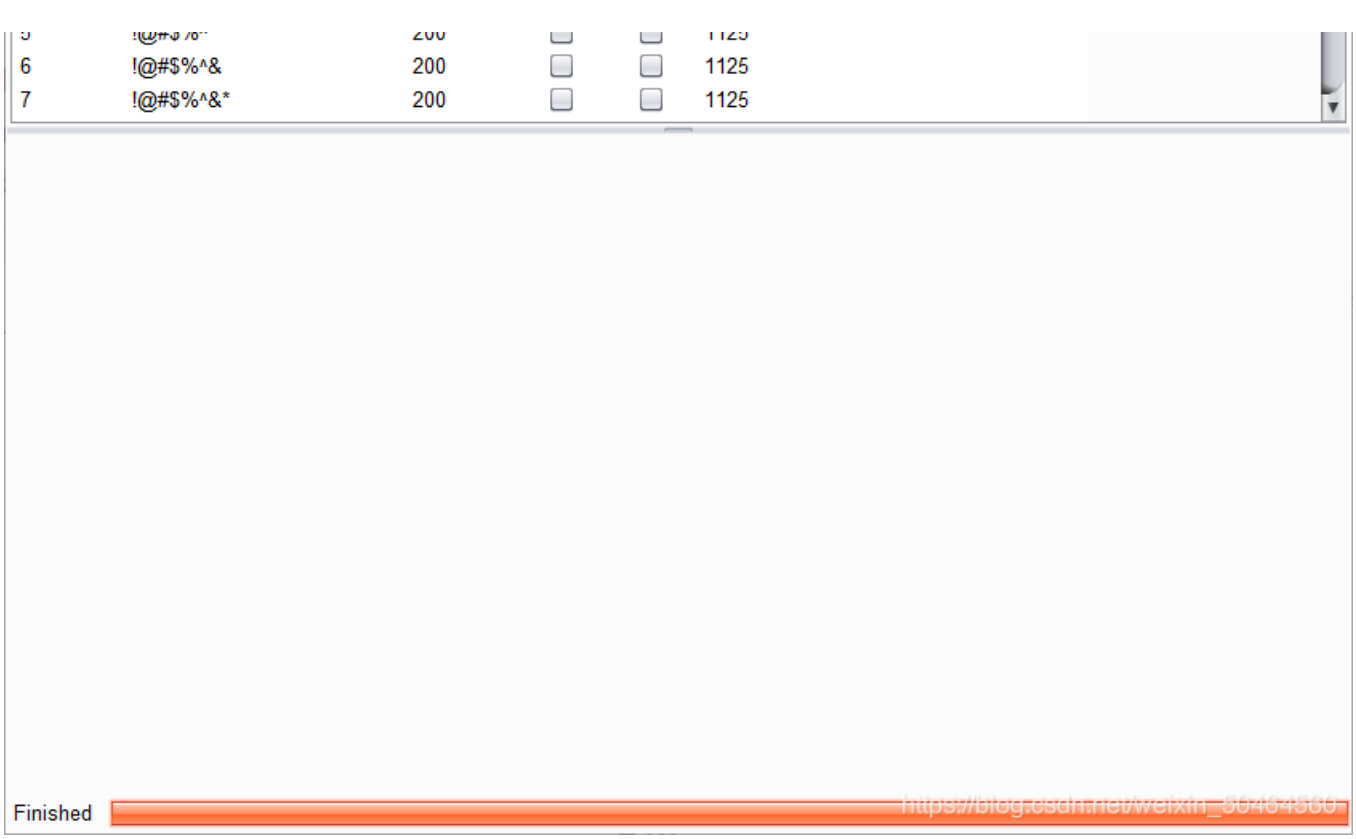


5、通过点击Action或者直接右键发送到burp里的intruder模块里，Attack type选择Sniper

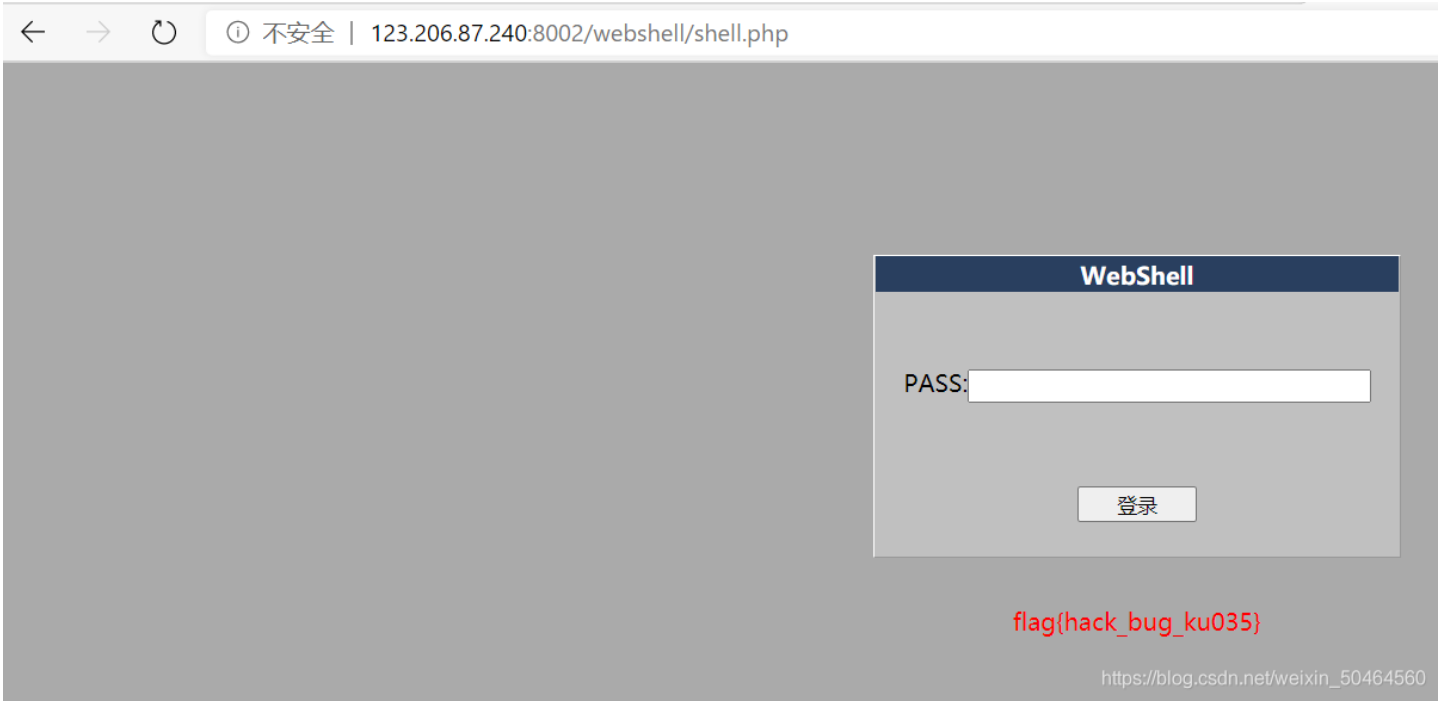


6、用上我的弱口令字典，开始攻击，接下来就是等待了





7、最后得到结果是hack，那咱就在PASS：里输入,最后得到flag，顺利完结



总结：多刷题，一定要完善自己的字典！

回到顶部