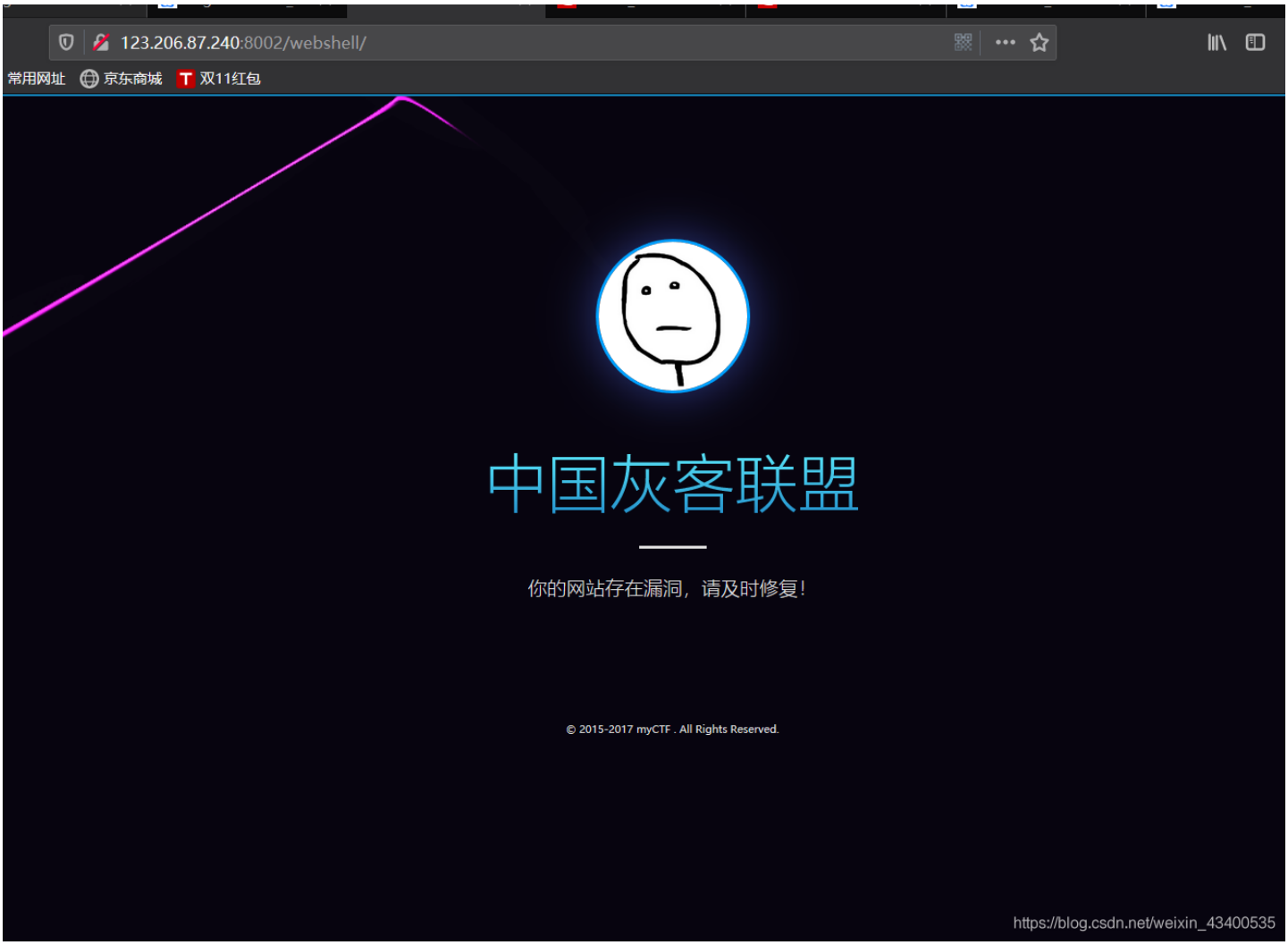
网站被黑 writeup

原创

ctf小菜鸡 于 2020-02-12 21:01:03 发布 174 收藏

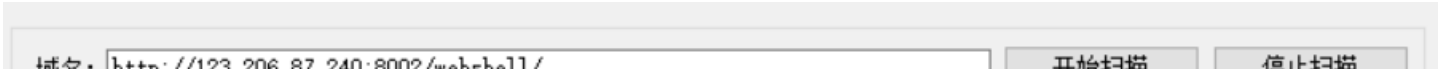
13.网站被黑 writeup

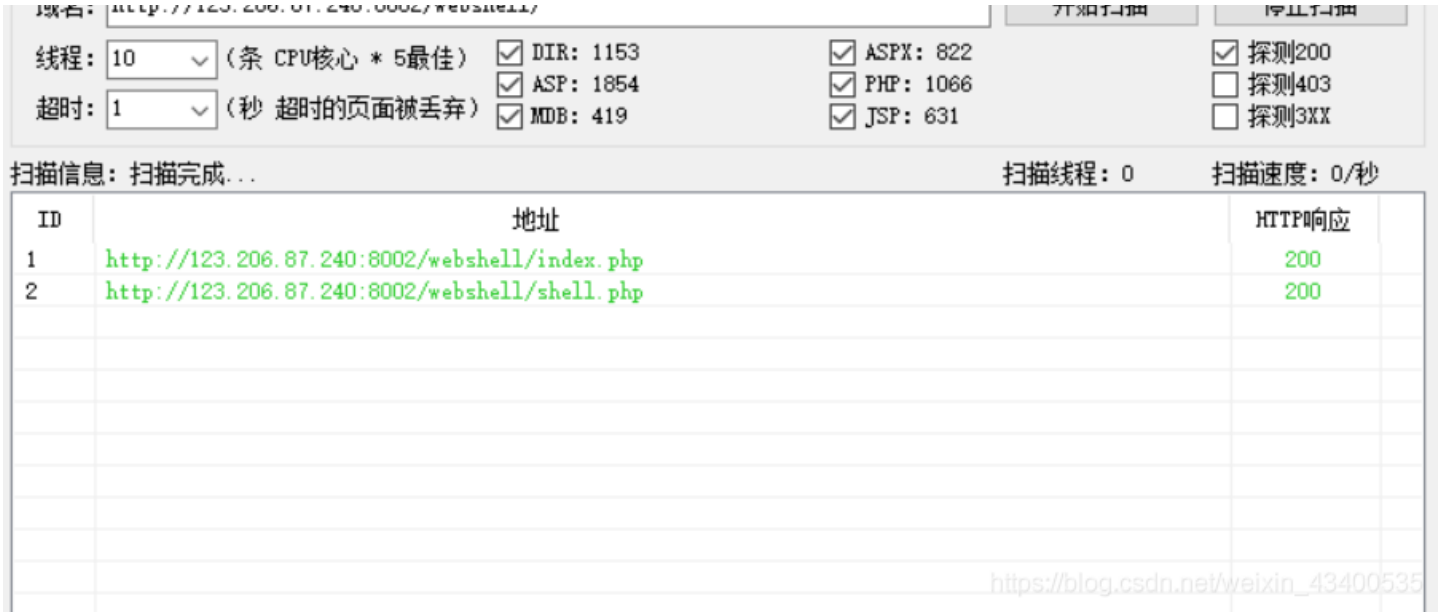


打开网址发现 网址上有个webshell 题目的名字也叫网页被黑。在这里就要提到一个知识，webshell

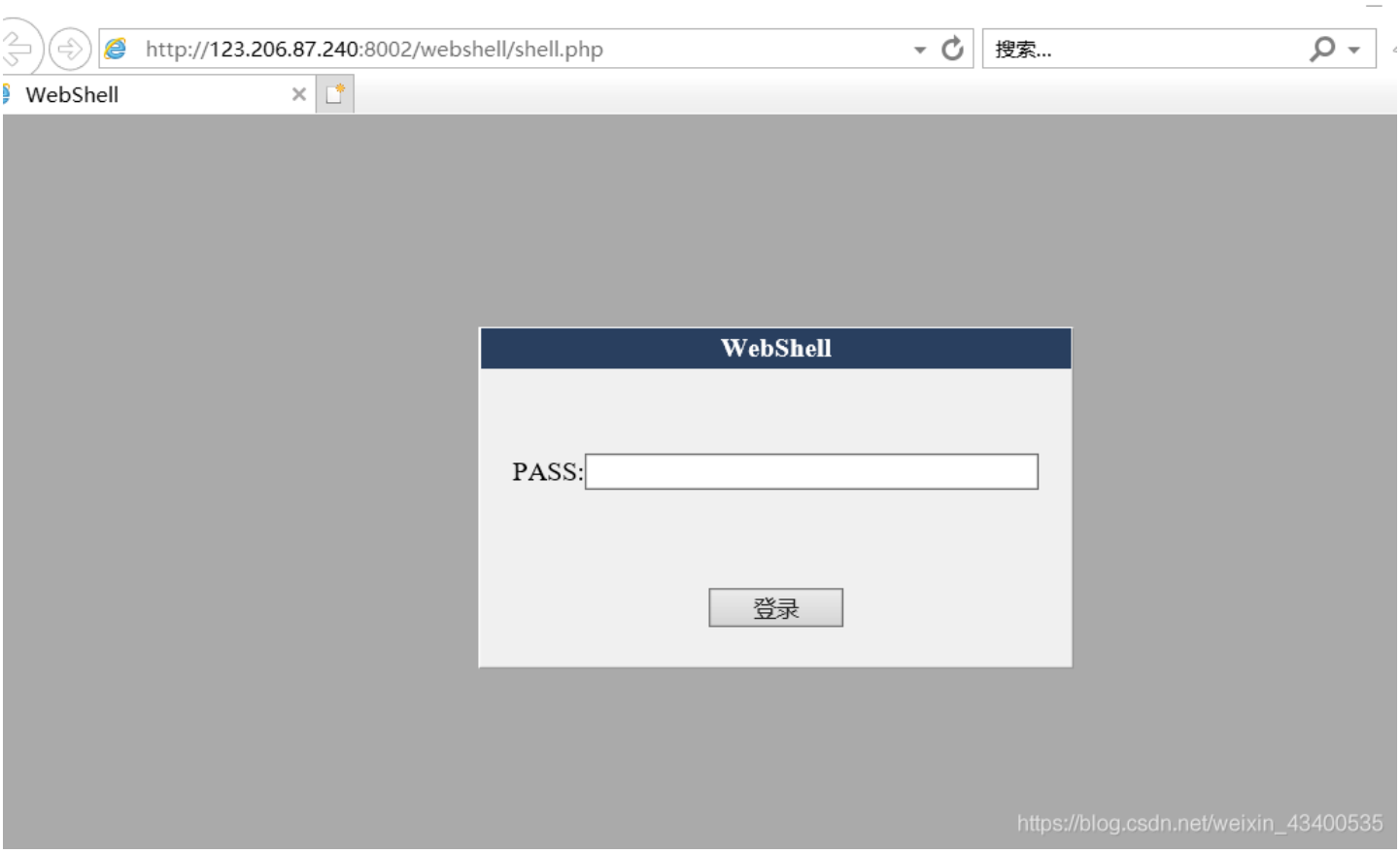
webshell就是以asp、php、jsp或者cgi等网页文件形式存在的一种命令执行环境，也可以将其称做为一种网页后门。黑客在入侵了一个网站后，通常会将asp或php后门文件与网站服务器WEB目录下正常的网页文件混在一起，然后就可以使用浏览器来访问asp或者php后门，得到一个命令执行环境，以达到控制网站服务器的目的。
顾名思义，“web”的含义是显然需要服务器开放web服务，“shell”的含义是取得对服务器某种程度上操作权限。
webshell常常被称为入侵者通过网站端口对网站服务器的某种程度上操作的权限。由于webshell其大多是以动态脚本的形式出现，也有人称之为网站的后门工具。

所以先用御剑扫描一下

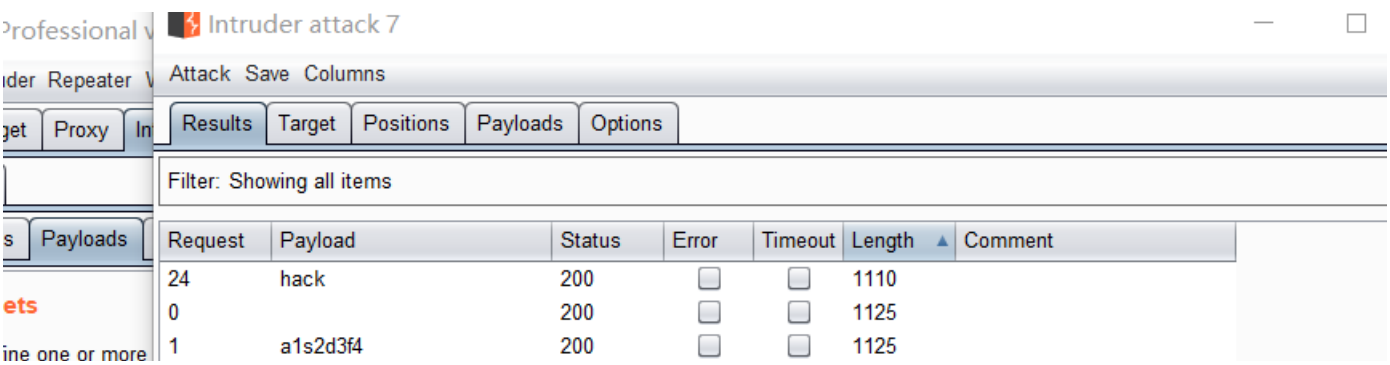


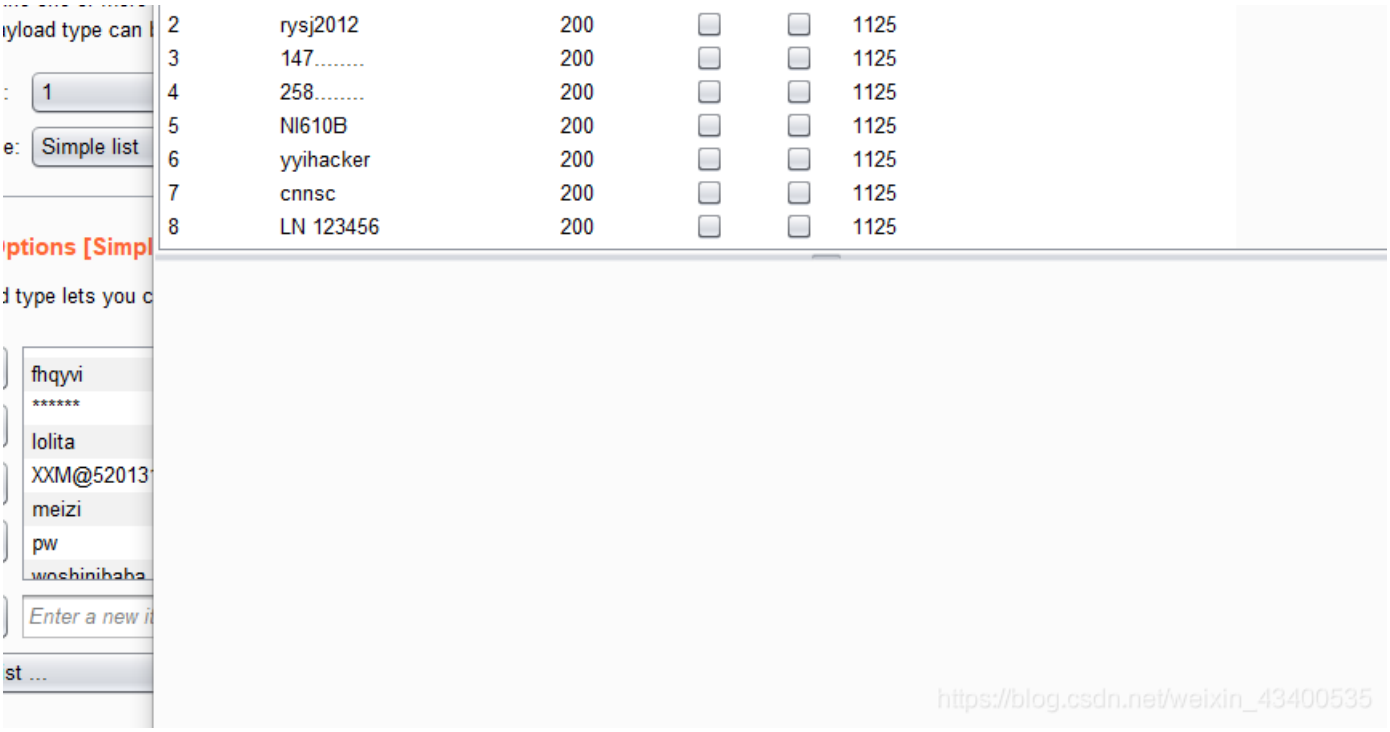


这里扫描到了一个shell.php 我们打开看看

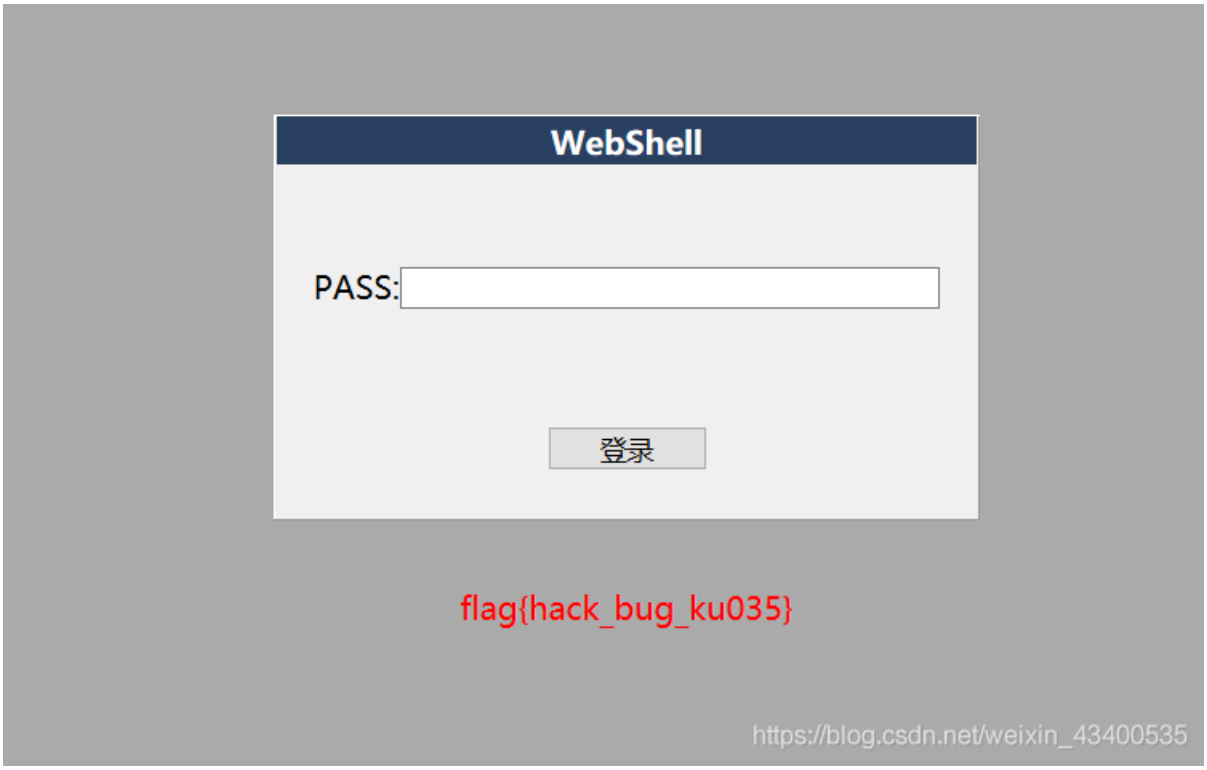


貌似是一个登录交界面，用burpsuite看看，爆破一下：





得到了hack 尝试一下



ok了

flag{hack_bug_ku035}