BugkuCTF web11_网站被黑 writeup

原创

Mitch311 于 2020-12-21 17:48:20 发布 910 收藏 2
分类专栏： CTF 文章标签： unctf

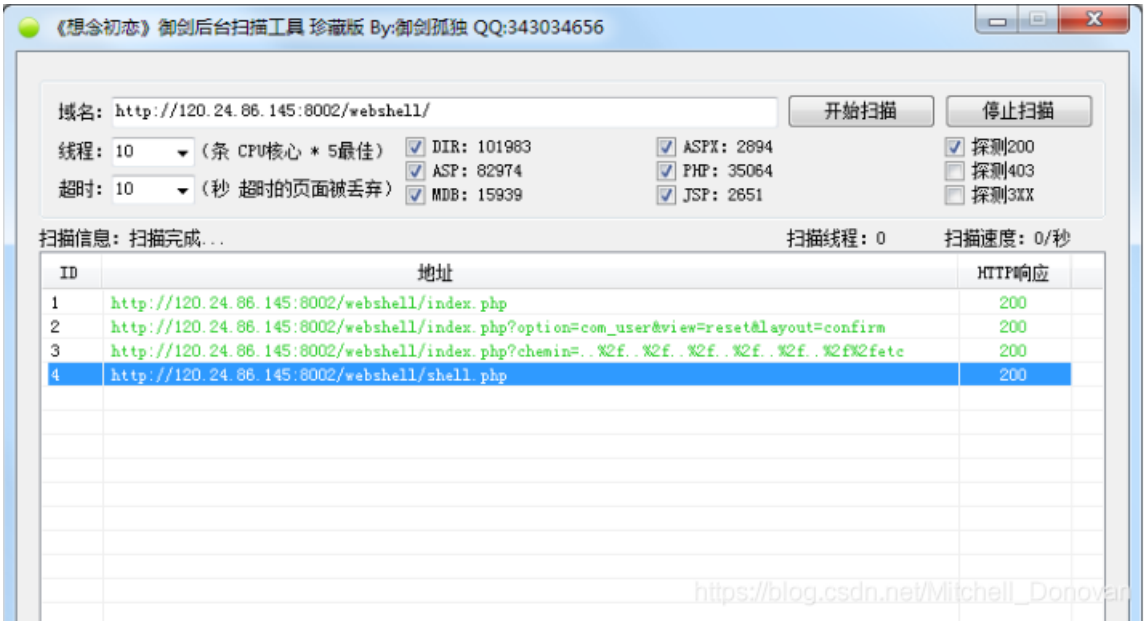
web11_网站被黑

原题链接

key:御剑后台扫描+burpsuite密码爆破

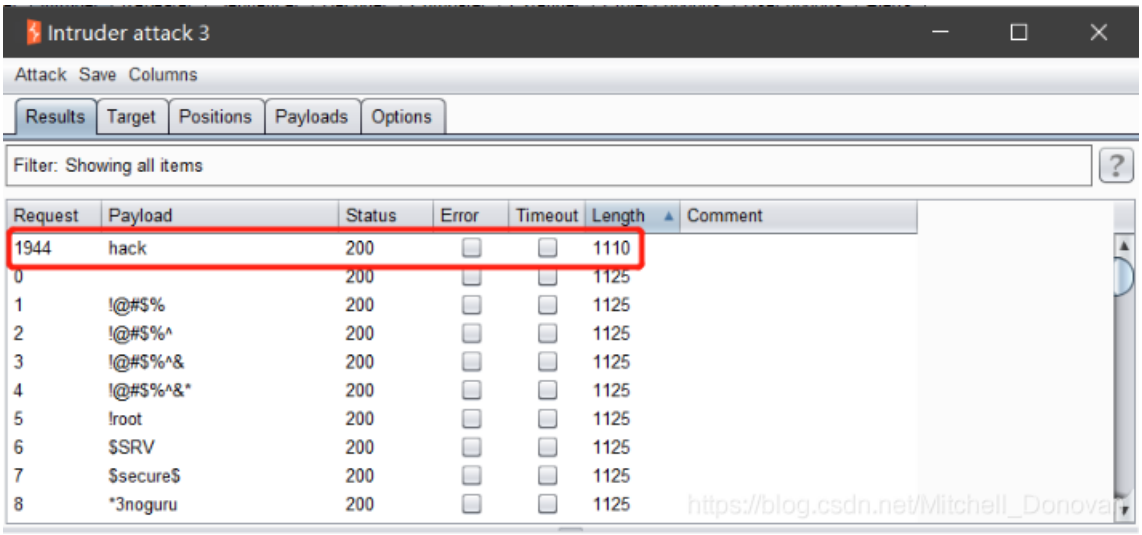
> 知识补充：
>
> webshell就是以asp、php、jsp或者cgi等网页文件形式存在的一种命令执行环境，也可以将其称做为一种网页后门。黑客在入侵了一个网站后，通常会将asp或php后门文
>
> 与网站服务器WEB目录下正常的网页文件混在一起，然后就可以使用浏览器来访问asp或者php后门，得到一个命令执行环境，以达到控制网站服务器的目的。
>
> 顾名思义，"web"的含义是显然需要服务器开放web服务，"shell"的含义是取得对服务器某种程度上操作权限。webshell常常被称为入侵者通过网站端口对网站服务器的某
>
> 程度上操作的权限。由于webshell其大多是以动态脚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

①用御剑后台扫描工具扫描一下该网页，果然发现了shell.php



②在网页中打开shell.php，发现是一个密码爆破题

③burpsuite抓包爆破（使用burpsuite自带字典就行，在playloads里面的playload type选 simple list）



④输入密码获得flag