BugKu Web题《网站被黑》writeUp

原创

Kuuny 于 2021-08-10 13:32:31 发布 18693 收藏 8
文章标签： web service 网络安全

本文链接：https://blog.csdn.net/CSDN_suuny/article/details/119567492

通过题目tips我们可以得知网站被黑之后，黑客留下了后门，我们在网站的url地址栏中添加/index.php发现也可以成功访问主页面(http://xxx.xxx.xxx.xxx:8080/index.php)，因此我们可以推断出档当前使用的后端语言为PHP，所以我们需要使用御剑、dirsearch和dirBuster或者dirb等后台扫描工具 扫描到黑客留下的后门地址，这里我们使用的字典需要为php类型的文件字典，

比如web.php,123.php,hacker/456.php等。

本次演示 我们这里使用dirsearch这个后台路径扫描工具。其他工具自行测试。

我们使用dirsearch -u http://xxx.xxx.xx.xx:8080/ 开启扫描

常用的参数有

- -u 指定网址
- -e 指定网站语言
- -w 指定字典
- -r 递归目录（跑出目录后，继续跑目录下面的目录）
- --random-agents 使用随机UA

这里的-u参数表示 指定url地址 我们这里的地址为网站的根目录。 我们这里不再指定字典。使用dirsearch自带的字典。

```
sunny@bogon ~ % dirsearch -u http://114.67.246.176:16774/
```

通过扫描结果我们发现shell.php文件非常可疑

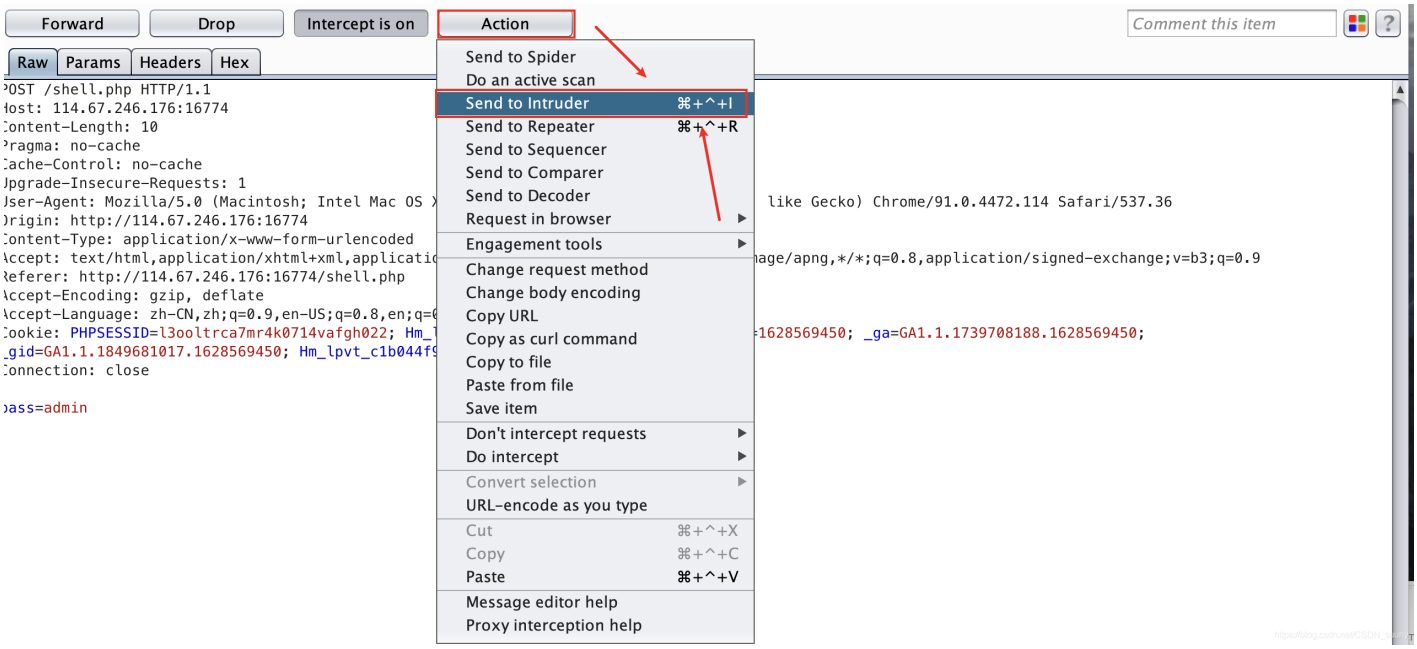
```
[13:06:35] Starting:
[13:06:37] 403 -  295B  - /.ht_wsr.txt
[13:06:37] 403 -  298B  - /.htaccess.bak1
[13:06:37] 403 -  298B  - /.htaccess.orig
[13:06:37] 403 -  300B  - /.htaccess.sample
[13:06:37] 403 -  296B  - /.htaccessBAK
[13:06:37] 403 -  299B  - /.htaccess_extra
[13:06:37] 403 -  298B  - /.htaccess_orig
[13:06:37] 403 -  296B  - /.htaccessOLD
[13:06:37] 403 -  289B  - /.html
[13:06:37] 403 -  297B  - /.htaccessOLD2
[13:06:37] 403 -  296B  - /.htaccess_sc
[13:06:37] 403 -  298B  - /.htaccess.save
[13:06:37] 403 -  288B  - /.htm
[13:06:37] 403 -  298B  - /.htpasswd_test
[13:06:37] 403 -  295B  - /.httr-oauth
[13:06:37] 403 -  294B  - /.htpasswds
[13:06:53] 403 -  288B  - /.php
[13:06:53] 403 -  289B  - /.php3
[13:08:40] 200 -   19KB - /index.php
[13:08:40] 200 -   19KB - /index.php/login/
[13:10:08] 403 -  298B  - /server-status/
[13:10:08] 403 -  297B  - /server-status
[13:10:09] 200 -  954B  - /shell.php
```


于是我们尝试访问。发现了一个需要密码的登录框

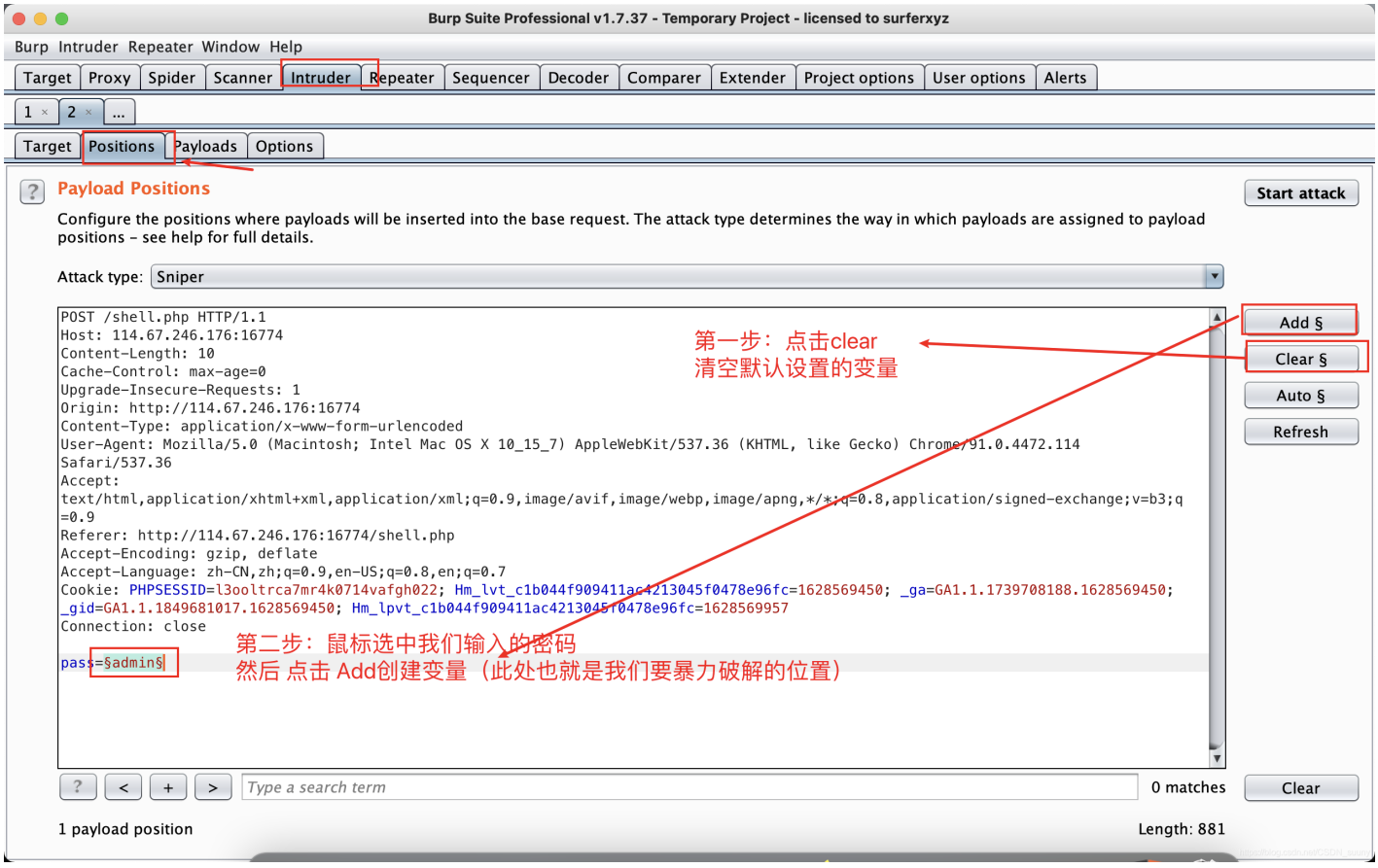
此处我们使用暴力破解的方式（因为webshell存在sql注入的方式不太可能）我们使用Burpsuite开启代理进行抓包。

这里不再演示如何使用Burpsuite抓包，不清楚的可以自行百度。

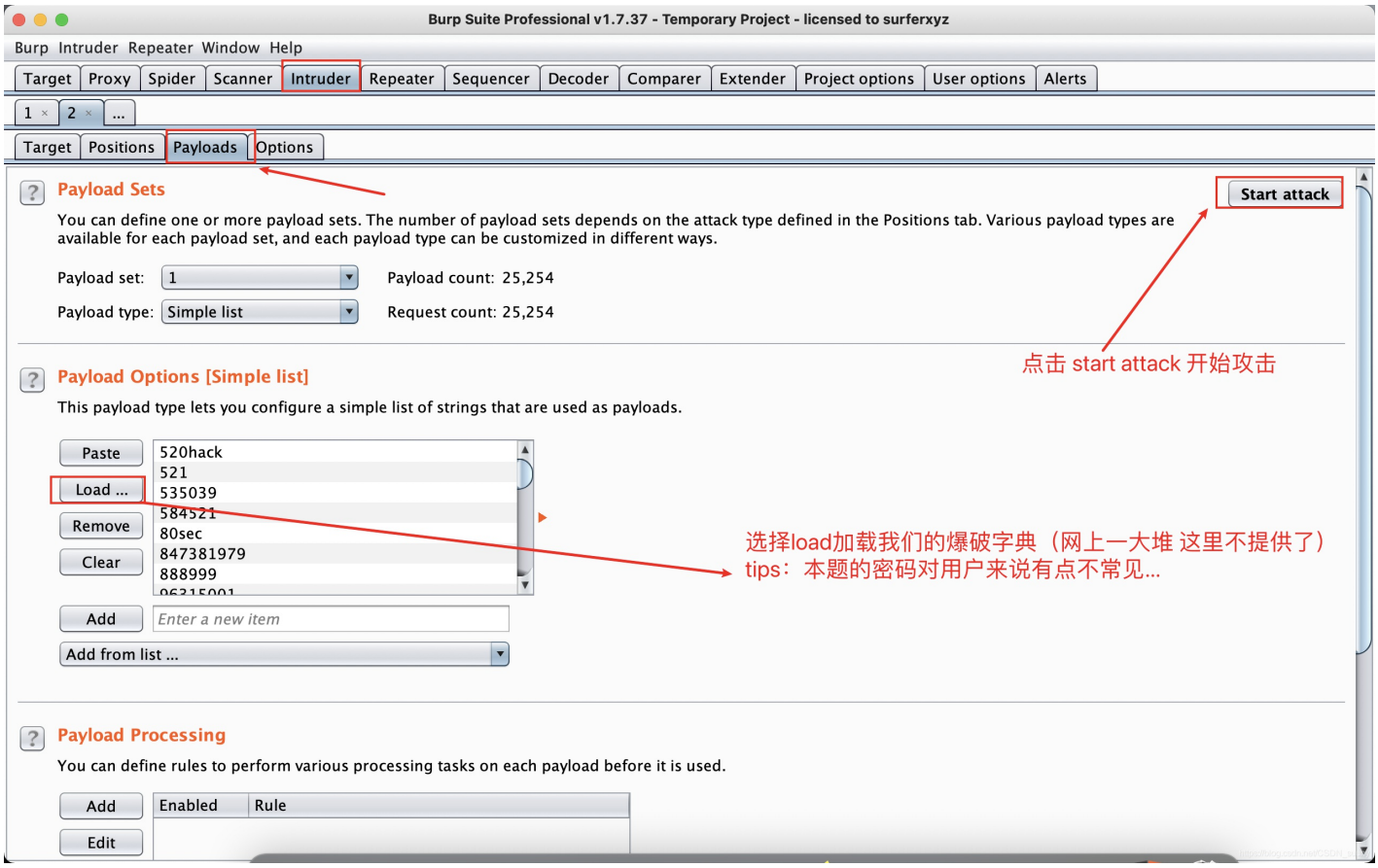
抓取到数据包之后 我们可以点击Action中的Send to Intruder(发送到暴力破解模块)



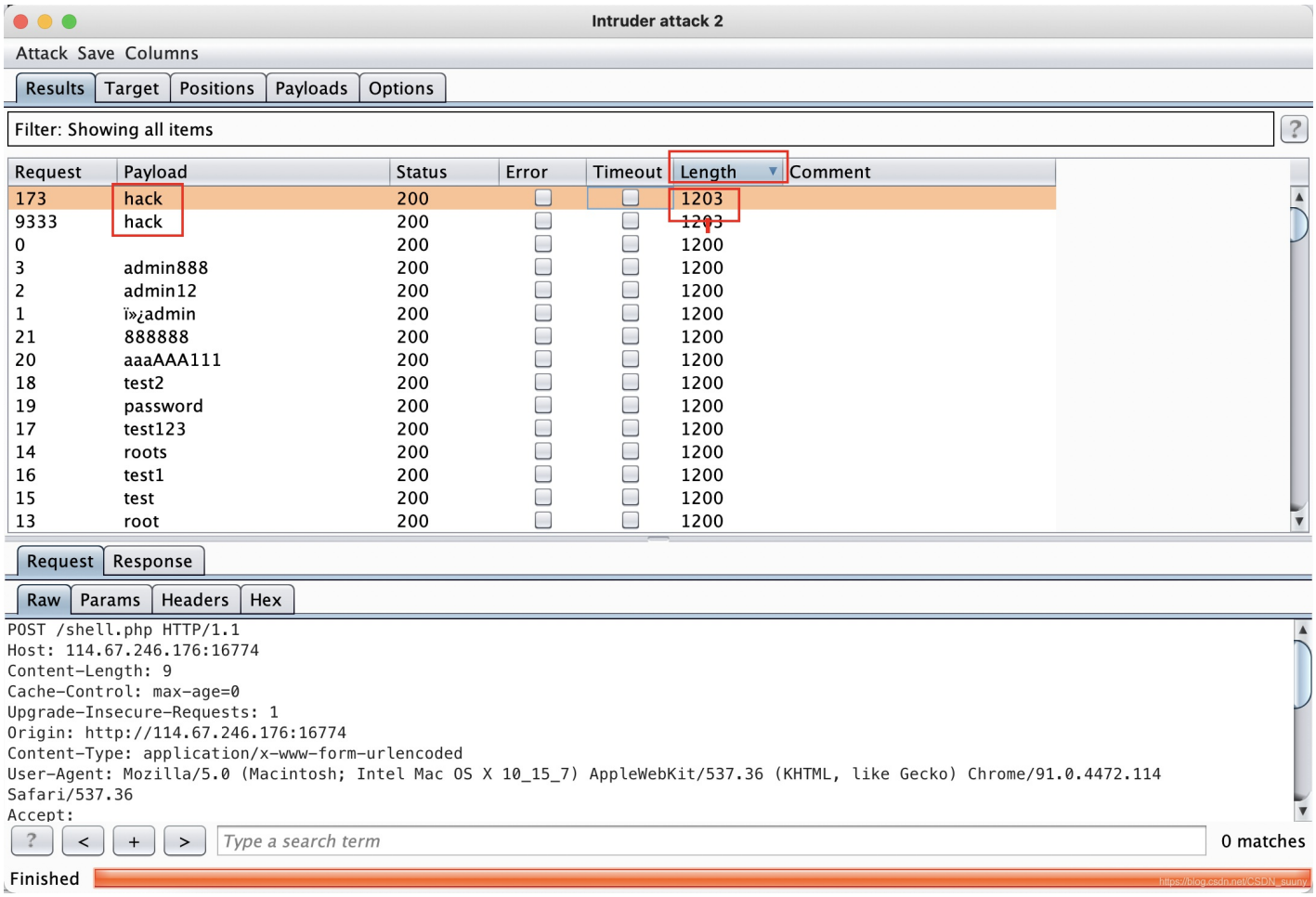
添加变量 （具体看图）



设置爆破字典



通过爆破返回的长度不同，我们可以判断出密码为hack 因为失败的话返回的长度（我这里的为1200） 失败的有很多次所以有很多长度为1200的数据包，而成功就那么一个，所以我们可以判断出长度为1203是我们本次爆破的密码。



返回网页尝试登录：

登录成功。