初试ctf wp



2 篇文章 0 订阅 订阅专栏

初试ctf wp

X-forwarded -for和reffer

□ 答题	× 🗅 index	×	C 写文章-CSDN博客	× +		-	-	ð	\times
$\leftarrow \ \rightarrow \ G$	③ 不安全 111.198.29.45:30156				☆	ABP	有	Θ	:

ip地址必须为123.123.123.123

根据提示,想到要请求真是的ip,于是我用burpsuite,拦截后到repeater,添加xff,这里遇到些问题,到r后,必须先go,再去添加xff才能有正确的提示,经验吧积累。后面又试了又不是这样,纳闷。

Workstation 🔻 📔 🖌 🛱 📮 🚇	9 🗆 🗆 🖸	2 - 5 -	☆ 主页 × Гр	Kali-Linux-2018.4-vm-amd >	<		. 0 .
	Burp Suite Community Edition v1.7.36 - Temporary Project						
Burp Intruder Repeater Window H	elp						
Target	Ргоху	Spider	· · · · · ·	Scanner	Intruder		
Repeater Sequencer	Decoder	Comparer	Extender	Project options	User options	Alerts	
3 ×							
Go Cancel <	> *	ł	Kali Docs	Target: http:	://111.198.29.45:301	56 🖉 ?	



看到"必须来自www.google.com"所以想到还要加referer

🕽 Workstation 🔻 📙 🗲 🛱 💬) 🚑 🕰 🗌 🗆 🔁	2 2 5 -	습 主页 × □ 🕞 🖡	Kali-Linux-2018.4-vm-amd 🤇	×	1	
	Burp Suite C	ommunity Edit	ion v1.7.36 - T	emporary Project	¢		
Burp Intruder Repeater Wind	dow Help						
Target	Proxy	Spider		Scanner	Intruder	-	
Repeater Sequen	cer Decoder	Comparer	Extender	Project options	User options	Alerts	
3 × 4 ×							
Go Cancel <	< v > v			Target: http	»://111.198.29.45:30	156 🖉 🤶	1
Request			Respon	se			
Raw Headers Hex			Raw H	eaders Hex HTML	Render		
Host: 111.198.29.45:30156 User-Agent: Mozilla/5.0 (X11 Gecko/20100101 Firefox/60.0 Accept: text/html,application/xhtml =0.8 Accept-Language: en-US,en;q Accept-Encoding: gzip, defla Connection: close Upgrade-Insecure-Requests: x-forwarded-for:123.123.123 referer:https://www.google.	l; Linux x86_64; rv:60. =0.5 ate 1 3.123 .com)) q=0.9,*/*;q	<pre>min.css re</pre>	///ibs.baidu.com/bdot il="stylesheet" /> in-left:auto; in-right:auto; in-TOP:200PX; h:20em; h:20em; o">ip地址必须为123.123.1 cument.getElementById(.google.com"; o").innerHTML="xctf{be cript>	23.123 "demo").innerHTML=" <script></script>		

flag就出现了 实验证明,xff可以不用大写,小写也行

密码破解题

首先随便输入,它会提示要我们用admin作为用户名登陆,照做。之后显示密码错误,然后打开这时的源代码,看见注 释"dictionary",所以需要用字典爆破。在github上下载好字典到文档中(其实就是密码集合),用burpsuite拦截,到intruder,即使 再做一遍,依然出现很多问题,郁闷。拦截后要在proxy界面就把username和password写上,不能到intruder写,我也不知道 why。到intruder后,设置爆破点,load字典,开始attack。发现123456那一行的后面数字与其他不同,点出来,在点到 response,就发现flag了。



🔁 Workstation	n 🕶 🛛 🚺 🕶	· 🕂	p 斗 🖇			🗐 🔻 🏠 主页 🗡 🕞 Kali-Linux-20)18.4-vm-amd $ imes$			
						Intruder attack 2	$\overline{}$		×	
Burp At	Attack Sav	e Colum	105							
		1								
	Results	Target	Positions	Payloads	Options					
Fi	ilter: Sho				Resu	ılt 31 Intruder attack 2		?		
1	_	Pavload:	1234	56						
R	Regu 🔺	Status:	200				Previous			
Tar 20	20 1	Length:	431							
21	21 .	Timer:	42				Next			
22	22									
- 23	23						Action			
24	24		~							
2	25	Reques	t Respor	ise						
27	27	(Barry)	Hander		Bandar]		1		
28	28		Headers							
29	29 0	onnectio	on: close	4.1			A	-		
30	30 ^C	ontent-I	ype: text	/html				~		
31	31	DOCTYP</td <td>₽E html></td> <td></td> <td></td> <td></td> <td></td> <td>v</td> <td></td> <td></td>	₽E html>					v		
20	C Reserved	html lan	g="en">							
	Request <	head>								
	Raw	<meta c<="" td=""/> <td>harset="U</td> <td>[F-8"></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	harset="U	[F-8">						
POS	ST /chec	/head>	weak au th	y citter						
Hos	st: 111. <	body>						-		
Use	ser-Agen									
Aco	cept: te X	ctf{64a]	.86efe8be7	1f11949db2a	370ed407}<	!maybe you need a dictionary>				
Aco	ccept-Lar						V			
Cor	onnection	2	< L	L C	ine a rearch i	terro	0 partshar			
Upg	grade-In			ا ت ا	rpe a seart///	Merriri	omatches			
Cor	ontent-Typ	pe:appli	cation/x-	www-form-ur	lencoded			T		
	?) (+		Type a searcf	term			0 matches		
38	8 of 7501								tps://blog.csdn.net/c10	042503039

在拦截的时候最好是跳回登陆界面,在输入用户名和密码的时候在拦截,这时候很多格式上的东西就会自动帮你写好,避免出现问题。

webshell

□ 答题 ×	🗅 webshell	× G 写文章-CSDN博客	× 📔 🔄 安全测试——利用Burpsuit × 📔 用户登录 - PHPSHE B2C商 × 📔 🕇	-	Ø	\times
← → C ③ 不安全 1	11.198.29.45:30190		☆	ABP 有	θ	:

你会使用webshell吗? <?php @eval(\$_POST['shell']);?>

burpsuite commexe	https://biog	全部显示	×
已下载 56.4/90.2 MB, 还需		csdn.net/c10425	3039

这题用的蚁剑,还有另一个方法,是用hackbar post一些命令,但好像是关于php的,我还不懂。

对于蚁剑,下载好加速器和代码后,添加数据,打开,就看到了flag.txt,但我不太明白为什么用dirsearch扫不出来flag.txt。而且 不明白密码为啥是shell,是因为题目提示中的post shell呢?还是啥?

@ 中国蚁剑			_		×
AntSword 编辑 窗口 调试					
 ▲ ■ □ 111.198.29.45 ⑧ 					•
日录列表 (0) <	① 文件列表 (2)				^
	●新建 ▼ ↑上层	/var/www/html/		→ 读耳	Z
• var	名称	日期	大小	属性	
btml	🖹 flag.txt	2019-02-21 10:27:59	38 b	0664	
	动 index.php	2018-09-27 04:02:04	539 b	0664	
	雪 任务列表				5030 3 9