i春秋123



weixin_30652271 U 于 2019-08-05 18:51:00 发布 O 137 论 收藏 原文链接: <u>http://www.cnblogs.com/wosun/p/11304876.html</u> 版权

打开是个普普通通的登录窗口,下尝试根据提示12341234进行输入,发现不正确。。。可能1234是指步骤,然 后查看源码

```
<!DOCTYPE html>
<html>
<head>
   <meta charset="utf-8" />
   <title>会员登录</title>
</head>
<body>
<center>
   <h4>请输入帐号密码进行登录</h4>
   <form action="" method="POST">
       <input type="text" name="username" placeholder='用户名' />
       <br /><br />
       <input type="password" name="password" placeholder='密码' />
       \langle \rm br / \rangle < \rm br / \rangle
       <input type="submit" name="submit" value="登录" />
       <!-- 用户信息都在user.php里 -->
       <!-- 用户默认默认密码为用户名+出生日期 例如:zhangwei1999 -->
   </form>
</center>
</body>
</html>
```

发现了绿色的提示信息,我们就根据提示试试打开user.php 打开是白板网页,源码也是白板,那就抓包试试 抓包也没找到什么关键信息。。。。那就试试注入吧 没反应。。。。 去看了看wp,发现这是个**文件读取漏洞、备份文件**的题

根据步骤,直接访问user.php.bak,提示我们下载备份文件





下载后直接将bak格式改为txt格式,然后就可以看见一堆所谓的用户名了

🥘 user.php.txt - 记事本	-		\times
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)			
zhangweiwangweiwangfangliweilinazhangminlijingwangjingliuweiwangxiuyingzhanglilixiuy nzhangpingwangtingchentaowangyumeiwangnazhangbinchenlonglilinwangyuzhenzhangf nghuanlidongmeizhanglongchenbochenleiwangyunwangfengwangxiurongwangruiliqinligu nanliuguizhenliuyuliujianjunzhangshuyinglihongxiazhaoxiuyinglibowanglizhangrong	ingwa engyin uizhen	nglizha Igwang chenpe	ang ghc eng
٢			>

然后使用爆破,先进行login.php界面的抓包

然后去掉不需要改变的变量,切换成攻城锤模式

Burp Suite Professional v1.7.36 - Temporary Project - licensed to surferxyz	-		×
urp Intruder Repeater Window Help			
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts			
1 × 2 × 3 ×			
Target Positions Payloads Options			
a Pavload Positions			
Configure the restrictions where psycholic will be inserted into the base request. The attack type determines the way in which psycholic are assigned to psychol costions - see help for	r full	Start a	lack
details.			
Attack type: Bittering ram	*		
POST / JOYIN , BAD710*1 HTTP/1.1 Host: 500cD03941c41edb183d791cb9aaf8c6121822c3d5434f.changame.ichunqiu.com	ŕ.	Add	ş
Content-Length: c5 Cache-Control: max-age=0		Clear	6
Ocigini http://JOb20b3941c141edb18a36791cb8aaf8e6121822c3d5434f.changame.ichunqiu.com Upgrade-Insecure-Requestsi		Auto	5
Content-Type: application/x-www-form-urlencoded Uwer-Agent: Norlia/S.0 (Windows NT 10.0 WOWE(4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.26 Safari/537.36		Data	ch .
Core/1.63.6736.400 COBcovere/10.3.3565.400 Accept: text/html.application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8		Poelle	11
Peferer: http://3Db2Db39icl4iedb19a3679icb9aaf8c6121822c3d5434f.changame.ichunqiu.com/login.php?id=1 Accept=Encoding: grip, deflate			
Accept-Language: th-CN, th:q=0.9 Cookie: UM_distintid=fc65756274445-0df0d031400707-335a4b7d-144000-16c5375f27eba3; chkphone=acWxMpxhQpD1AchbMuSnEqy1QuD100000;			
Hm_lvr_2d0601bd38de704980183490135485943=1563950551,1563956464,15647760335,15648381955) cl_meesione=83750485b0935b575b91700441903507613802;Hm_lvvr_2d0601bd38de7449818249c153695943=1564978122;			
P#9925310=inmul0rgolD05ps3jmOct14v71;3=luid_b=73ble6fla168bde3e60aa61f77912c6c Connection: close			
username=\$zhangwei\$&password=\$zhangwei\$1990&submit=\E2\99\88\Z5\8D\95	-11		
	*		
? < + > Type a search term 0 a	natches	Clea	r -
2 payload positions Leng	h: 1242		

然后导入刚刚的user.php.txt

Burp Innote: Repeater Window Help Taget Proof Second Interview Repeater Sequencer Decoder Comparer Extender Project options Alerts T 2 3 Taget Presents Provided Sectors Taget Presents Provided Sectors Taget Proof Presents Provided Sectors Provided Sectors Payload Contr. 367 Payload type: Simple Set Payload Contr. 367 Payload type Simple Set Payload type Simple Simple Simple Set Payload type Simple Simple Simple Set Payload type Simple Simp	🚯 Bu	urp Suite P	rofessio	mal v1.7	7.36 - Te	mporary	Project - lic	ensed to	surferxyz								-		×
Type Procy Spider Sequencer Decoder Comparer Extender Project options User options Alerts 1 2 5	Burp I	ntruder Rep	ater Wir	ndow Hel	P														
Image: Payload Sets Start attack You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set. Start attack Payload Sets: Image: Payload Sets: Start attack Payload set: Image: Payload count: 357 Payload Type: Simple list Request count: 357 Payload Options (Simple list) This payload type: at a count: 357 This payload type its you configure a simple list of strings that are used as payloads. Image: Payload type: Payload type: Image: Payload type: Image: Payload type: Image: Payload type: Image: Payload type: Payload type: Image: Payload type: Image: Payload type:	Targe	t Praxy	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	Alerts						
Taget Poston Payload Set: Sant attack You can define one or more poyload sets. The number of payload sets depends on the attack type defined in the Postions tab. Various payload types are available for each payload set. Payload set: Payload set: Payload count: 357 Payload set: Image: Payload count: Store Request count: 357 Payload type: Simple list) Request count: Store This payload type (and payload is a simple list of strings that are used as payloads. Image: Payload type is the spuic configure a simple list of strings that are used as payloads. Image: Payload Set: Image: Payload type is the spuic configure a simple list of strings that are used as payloads. Image: Payload Set: Image: Payload type is the spuic configure a simple list of strings that are used as payloads. Image: Payload Set: Image: Payload type is the spuic configure a simple list of strings that are used as payloads. Image: Payload Processing You can define dues to perform various processing tasks on each payload before it is used. Image: Payload Reverse Image: Payload Reverse Image: Payload Reverse Image: Payload Rever	1 ×	2 × 3 ×																	
Payload Sets Start attack You can define one or more payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type: an be customized in different ways. Payload type: are be customized in different ways. Payload set: Payload court: 357 Payload type: Request court: 357 <t< td=""><td>Targe</td><td>t Positions</td><td>Paylo</td><td>ads Opt</td><td>tions</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></t<>	Targe	t Positions	Paylo	ads Opt	tions														
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways. Payload etti: Payload count: 357 Payload Options [Simple list] This payload Options [Simple list] This payload type is you configure a simple list of strings that are used as payloads. Patter sharagenin Remove Los terms from file Difference string Payload Processing You can define nules to perform various processing tasks on each payload before it is used. Add Edde Remove Upp Down	?	Payload S	ets															Start atta	ck 1
Payload Set: 1 Payload Court: 357 Payload Coptions [Simple list] The payload Options [Simple list] The payload Options [Simple list] The payload Options [Simple list of strings that are used as payloads. Paste theorem of the payload Options for the strings that are used as payloads. Paste theorem of the strings that are used as payloads. Paste theorem of the strings that are used as payloads. Paste theorem of the strings that are used as payloads. Paste theorem of the strings that are used as payloads. Paste theorem of the strings that are used as payloads. Paste theorem of the strings that are used as payloads. Paste theorem of the strings that are used as payloads. Paste theorem of the strings that are used as payloads. Paste theorem of the strings that are used as payloads. Paste theorem of the strings that are used as payloads. Paste theorem of the strings that are used as payloads. Paste theorem of the strings that are used as payloads. Paste theorem of the strings that are used as payloads before it is used. Add them list to perform various processing tasks on each payload before it is used. Add make the list to perform various processing tasks on each payload before it is used. Add make the list to perform usious processing tasks on each payload before it is used. Add make the list to perform usious processing tasks on each payload before it is used. Add make the list to perform usious processing tasks on each payload before it is used.		You can del and each pe	ine one o Iyload typ	r more pay	yload sets customize	. The num d in differe	ber of payload s nt ways.	ets depend	is on the atta	ack type def	ined in the Positio	is tab. Various	s payload t	ypes are avai	able for eacl	h payload s	et,		
Payload type: Single list Payload Cytions [Simple list] This payload type lets you configure a simple list of strings that are used as payloads. Passes thangves wangees wangees among Lood dens from file Clear thangvinin Add torm list		Payload set	1			Payl	load count: 357												
Payload Options [Simple list] This payload type lets you configure a simple list of strings that are used as payloads. Paste changer imaging Remove Loss tenss from lie changer imagin Add Enter a new item Add mon lat		Payload typ	e: Simp	le list		Req	uest count: 357												
This payload type lets you configure a simple list of strings that are used as payloads. Paste changwei vangwei vangw	2	Payload O	ptions (Simple I	list]														
Paste thangvei Vargaei inglarg Remove Load tents from file inglarg Add Enter a new Idem Add Enter a new Idem Add tent list • • • • • • • • • • • • • • • • • • •	•	This payloar	i type lets	s you con	figure a sir	nple list of	strings that are	used as p	ayloads.										
Uargree Image: Imag		Paste	zhang	wei			*												
Remove Loss terms from file 2 hangmin ining Add Enter a new Item Add from ist Add from ist You can define rules to perform various processing tasks on each payload before it is used. Add Enabled Remove Up Down		Load	vangt	iei ing			1 .												
Clear thangmin Iging Image: Clear a new item Add Enter a new item Add thom list Image: Clear and the new item You can define rules to perform various processing tasks on each payload before it is used. Add Enabled Remove Image: Clear and the new item Up Image: Clear and the new item		Remove	.oad item	s from file															
Add Enter a new ikem Add from list Payload Processing You can define rules to perform various processing tasks on each payload before it is used. Add Enabled Rule Edit Remove Up Down		Clear	zhang lijing	min			÷												
Add from list Payload Processing You can define rules to perform various processing tasks on each payload before it is used. Add Enabled Rule Edit Remove Up Down		Add	Enter a	a new iten	0														
Payload Processing You can define rules to perform various processing tasks on each payload before it is used. Add Enabled Rule Edt Remove Up Down		Add from I	st				•												
Payload Processing You can define rules to perform various processing tasks on each payload before it is used. Add Enabled Rule EdR Remove Up Down											-								
You can define rules to perform various processing tasks on each payload before it is used. Add Enabled Rule Edit Remove Up Down Down Enabled	?	Payload P	rocessi	ng															
Add Enabled Rule Edit Remove Up Down		You can del	ine rules I	to perform	various p	ocessing t	tasks on each p	payload befo	ore it is used	i.									
Edit Remove Up Down		Add	Enable	ed Rule	8														
Remove V Up Down		Edit																	
Dewn		Remove						•											Ĩ
		Down																	
		Com																	_ [

然后开始attack,每次attack结束后根据提示更改密码后面的年份

🚯 Intrue	der attack 6						-		×
Attack Sa	ave Columns	Y	_						
Results	Target Positions Pa	ayloads Option	S						
Filter: Sho	wing all items								?
Request	Payload	Status	Error	Timeout	Length 🔻	Comment			
311	lixiuyun	200			1044				
1	zhangwei	200			1009				
2	wangwei	200			1009				
3	wangfang	200			1009				- 1
5	lina	200			1009				- 1
7	lijing	200			1009				
6	zhangmin	200			1009				
4	liwei	200			1009				- 1
8	wangiing	200			1009				- 1
11	zhanoli	200			1009				
	2.10.19.1	200							
Request	Response								
Raw Pa	arams Headers Hex								
Origin: 1	http://30b20b3941c	141edb19a3679	1cb9aaf	8c612182	22c3d5434	f.changame.ichungiu.c	om		
Upgrade-1	Insecure-Requests:	1	2002000						- E
Content-7	Type: application/	x-www-form-ur	lencode	d					
User-Ager Chrome/63	nt: Mozilla/5.0 (W 3.0.3239.26 Safari	1ndows NT 10. /537.36 Core/	1.63.67	(4) Apple (26.400.0)	OBrowser	37.36 (KHTML, like Ge /10.2.2265.400	cko)		
Accept: t	text/html,applicat	ion/xhtml+xml	,applic	ation/x	ml;q=0.9,	image/webp,image/apng	,*/*;q=0.8	8	
Referer:				0-04540					
Accept-Er	ncoding: gzip, def	ase/sicosaare late	0612182	20303434	.cnanga	me.ichunqiu.com/10gin	. hub %rd=1		
Accept-La	anguage: zh-CN, zh;	q=0.9							
Cookie: 1	JM_distinctid=16c5	375f27d4f5-0d	l£0d0314	00707-33	35a4b7d-1	44000-16c5375f27eba3;			
Hm lvt 20	d0601bd28de7d49818	249cf35d95943	156395	0551.15	63966464.	1564768335,1564838395	:		
ci_sessio	n=e357cd685b0935b	f57b917e0c441	9039b76	13882;		,	-		
Hm_1pvt_2	d0601bd28de7d4981	8249cf35d9594	3=15649	78122;	PHPSESSID	=1nmulOrqo2hOkps3jmOc	ti4v71;		
Connectio	n=/spiesizais8bde	3e60aa6117/91	2080						
username	lixiuyun&password	lixiuyun1990	€submit	-\E7\99	BBNE5NBD	\$95			
_									
? <	+ > Type a	search term						0 r	natches
Finished									

🚯 Intruc	ler attack 11							-		×
Attack Save Columns										
Results	Target Positions	Payload	s Options							
Filter: Show	ving all items									?
Request	Payload		Status	Error	Timeout	Length V	Comment			
195	zhangyuzhen		200			1044				
0			200			1009				
1	zhangwei		200			1009				
2	wangwei		200			1009				- 1
3	wangfang		200			1009				- 1
4	liwei		200			1009				- 1
5	lina		200			1009				
6	zhangmin		200			1009				- 1
7	lijing		200			1009				
8	wangjing		200			1009				
Request	Response									
Raw Pa	rams Headers H	lex								
Cache-Con	trol: max-age=0]								
Upgrade-I	nsecure-Request	ic:41ed:s: 1	b19a36791	.cb9aai	8C61218	220305434	ir.changame.ichunqiu.	com		
Content-T	ype: applicatio	on/x-www	-form-url	encode	d					_
User-Agen Chrome/63	t: Mozilla/5.0	(Window	s NT 10.0	; WOW6	4) Apple 26 400 0	eWebKit/5	37.36 (KHTML, like G	ecko)		
Accept: t	ext/html, applic	ation/x	html+xml,	applic	ation/x	ml;q=0.9,	image/webp,image/apn	ug,*/*;q=O	.8	
Referer:			1 - h C 4 C -							
Accept-En	coding: gzip, d	ieflate	ICD944100	014104	2030343.	4r.changa	me.ichunqiu.com/iogi	n.pnp/id-	1	
Accept-La	nguage: zh-CN, z	zh;q=0.9								
Cookie: U	M_distinctid=18	bNuSpEc	7d4f5-0df	0d0314	00707-3	35a4b7d-1	.44000-16c5375f27eba3	;		
Hm_1vt_2d	0601bd28de7d498	318249cf	35d95943=	156395	0551,15	63966464,	1564768335, 156483839	5;		
ci_sessio	n=e357cd685b093	5bf57b9	17e0c4419	039b76	13882:	DUDOPOOT	a langu l On an 2 h Olen - 2 h	on i dav711 -		
jsluid	h=73b1e6f2a168k	de3e60a	a61f77912	-15649 C6C	/0155; 1	rnrataa 11	-Imparordornowbarlmo	GC14V/1;		
Connectio	n: close									
username=	zhangyuzhen&pas	sword=z	hangyuzhe	n19956	submit=	¥E7%99%BI	%E5%BD%95			
? <) + > Type	e a search	term						0	matches
Finished										

随机安排一个就可以登录进去了

⊕ ↑A⊕6 ×	+					T	-	σ	×
く)で合田(☆日	0b20b3941c141edb19a36791cb9aaf8c6121822c3d5434f.changame.ichunqiu.com	₹ = ~	◎・ 在山援索	۹ 🛤	\pm %	· D·	6		=
🔺 非然 📄 無用限社 🛈 京东南端	■ 中国大学MODC() \ominus C 原育开設研究 😳 ZOJ = Horne 🐧 SICNU GJ Corri 🔮 展PHP制作発展2) 👼 総な板型 - 学校行	O ROME	通量尔利 CISON性能解析及	😫 squ	AP第单位	9,2	SPEwel		Ð

0

13kg 64s

进去也是白板,右键源码

看到提示,然后这里我们可以按F12去修改网页源码



然后删除掉注释



弹出文件上传框,但是这里上传木马是被屏蔽了的

文件名不合法

再直接上传jpg试试

。。。。。有点鸹貔了,又去看了看wp才知道这里是修改pht后缀,原因是Apache 配置文件中会有.+.ph(p[345]? |t|tml)此类的正则表达式,文件名满足即可被当做php解析

直接上传任意文件,其后缀满足是.pht就行了,如我随意将123.jpg重命名为123.jpg.pht



然后这里就直接访问view.php试试

	eb3e9o	:48bf6	e48bfb	e7523	7e5842 ×	◎ 高级设置		+			
<	>	C	\triangle	Φ	☆ (b3e9c48bf6e48bfb	e75237e5842a583	a9ff6bedb96e4l	b50.changame.ichu	nqiu.com/view.php	1
*	书签		常用网址	0	京东商城	▶ 中国大学MOOC(① C 语言开发环境	DZOJ :: Home	SICNU OJ Cont	📸 用PHP制作简单的	(
file	?										

file? 应该是文件读取类型,问我们file的量是什么,查看源码没什么信息就直接在url中试试?file=1

● eb3e9c48bf6e48bfbe75237e584:×
 ◇ 高級設置
 +
 ◇ ○ ○ □ ○ ☆ □ ☆ eb3e9c48bf6e48bfbe75237e5842a583a9ff6bedb96e4b50.changame.ichunqiu.com/view.php?file=1
 ★ 书签 ○ 常用网址 ◎ 京东商城
 ● 中国大学MOOC(◎ C 语言开发环境 ◎ ZOJ :: Home ⑤ SICNU OJ | Conti ⑧ 用PHP制作简单的 ◎ 菜鸟数 filter "flag"

既然有过滤我们就绕过试试

最开始我用大小写混写的方法结果绕过不了,再尝试双写就可以了

?file=flflagag



提交flag{巴拉巴拉}就行了

转载于:https://www.cnblogs.com/wosun/p/11304876.html