Web密码爆破实验



<u>烟雨天青色</u> 于 2019-07-19 20:30:55 发布 5331 少 收藏 45 分类专栏: <u>CTF</u> 文章标签: <u>密码爆破 CTF</u> 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u> 版权协议,转载请附上原文出处链接和本声明。 本文链接: <u>https://blog.csdn.net/qq_38603541/article/details/96494194</u> 版权

CTF 专栏收录该内容

29 篇文章 1 订阅 订阅专栏

前言:由于爆破其他正常网站密码属于违法行为,因此本次实验是使用自行搭建web环境进行密码爆破实验。

这个实验是今天老师给留的附加作业,虽然心很累,但这种实验确实挺好玩。

咱们看一下实验环境吧......

实验环境是老师自己搭建的,只给了我们一个IP地址和端口号,不过这就够用了,哈哈哈哈

120.78.92.198:8009/	×	+					
← → ⊂ ଢ		i 120.7	3.92.198 :8009	9	实验环	境	
📄 火狐官方站点 🍨 新	新手上路 📄 常	常用网址 🖨 微博	🖨 携程旅行	🖨 百度	🖨 网始大全	🖨 京东商城	JD
Pelease find the l	ogin page	^_^					

https://blog.csdn.net/qq_38603541

可是这个地址访问出来,提示: "Pelease find the login page ^_^"。嗯???什么鬼,登录页面还要自己找?? 行吧行吧,这种网络后台找登录界面就单纯靠经验了……要找到登录页面就需要知道网站后台是使用什么语言 写的,这个很重要,因为涉及到后缀名的,现在管它呢,随便输一个字符串看看,到底是个什么情况……

404 Not Found X	+		
(←) → ℃ @	(120.78.92.198:8	009/login	
🔄 火狐官方站点 🍯 新手上路 📋	常用网址 💮 微博 💮 携程前	統 🖨 🖬 🖨 🖓 网址	大全 🛈 京东商
Not Found			
The requested URL /login was n	ot found on this server.		
Apache/2.2.15 (CentOS) Server	nt 120.78.92.198 Port 800	9	
1			

我先构造了一个login的字符串,回车之后,页面提示: Apache......巴拉巴拉的,看到Apache我们就知道,网站 后台肯定是使用php写的,知道这个就好办了,我们在IP地址后面加上一个/login.php试试......不行!! 昂??想 想网站后台还有啥常用的登录名: admin、manage......经过尝试,/manage.php可以访问到我们需要的登录页面。

Admin Panel	× +	+	
(←) → C' @		 ④ 120.78.92.198:8009/manager.php 	
📄 火狐官方站点 🍥 新手上路	📄 常用网	网址 🕀 微博 🕀 携程旅行 🖨 百度 🖨 网址大全 🖨 京东商城 🎵 京东商城 🖨 爱海宝	
		Admin_Login	

UserName:	admin	
PassWord:		
	Login	

一般遇到这样的情况,我下意识的回去查看一下网页源代码,可是......这个网页穷的什么都没有......那能咋办?上工具抓包呗......接下来,小杨开始了漫长的抓包过程......

第一步,设置代理,这里推荐使用火狐浏览器,功能很强大滴。

		- 0 ×
☆	III\ 🗊 🔹 🖪	🗭 🦘 🔘 📃
	3 登录同步服务	
	☑ 内容拦截	标准
	🗗 新建窗口	Ctrl+N
	🗢 新建隐私窗口	Ctrl+Shift+P
	中 恢复先前的浏览状态	5
	缩放 一	100% + 2
	编辑	ኤ 🖒 🖨
	Ⅲ 我的足迹	>
	静 附加组件	Ctrl+Shift+A
	✿ 选项	
	✓ 定制	
	打开文件	Ctrl+O
	另存页面为	Ctrl+S
	🖶 打印	
	Q、在此页面中查找	Ctrl+F
	更多	>
	Web 开发者	>
	⑦ 帮助	>
/	Ů 退出	Ctrl+Shift+Q
/		

https://blog.csdn.net/qq_38603541



设置好代理之后,我们打开著名的爆破工具: burpsuite,设置一下,进行抓包实验。

第二步,配置burpsuite。

🛃 Bur	p Suite P	ofessional	v1.6beta -	icensed to	LarryLau								_		×
Burp I	ntruder l	Repeater V	Vindow Hel	р											
Targe	t Prox	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Options	Alerts				
Interc	ept HT	TP history	WebSock	ets history	Options]									
? &	Proxy Burp Pro proxy se	.isteners xy uses lis rver.	steners to re	ceive inco	ming HTTP r	equests from	your brows	er. You will n	need to confi	gure your b	prowser to	o use one of th	ie listenei	rs as its	
	Add Edi Remo	/e	ning Inter ✓ 127	face 0.0.1:8080	Invisible	Redirect		Certificat Per-host	te			Q			
	Each in: certifica	tallation of e for use ir	Burp generation other tools	ates its ow or another	n CA certific installation	ate that Prox of Burp.	y listeners	can use whe	n negotiating	g SSL conr	ections.	You can impo	rt or expo	ort this	
	CA co	rtificate													_
?	Interce	pt Client	Requests	•											¥
1					1161-116		1 197				hii	<u>os://blog.cs</u>	<u>p/terrint</u>	<u>q 389</u>	164

这里使用本地默认的IP和端口就行,127.0.0.1端口号8080,然后点击Intercept,进行下一步实验操作。

点击Intercept is off。点击之后这个按钮它会变成Intercept is on,然后回到我们的浏览器下,关掉刚刚我们配置的代理服务器,在密码输入框内输入任意字符串,回车。这个时候你会发现,浏览器的该页面有一个圈圈会不停的转呀转,没事啊,这说明正在抓包。现在,我们回到BurpSuite下,已经可以发现到我们已经将信息抓到了。

Burp Suite Professional v1.6beta - licensed to LarryLau	– 🗆 X
Burp Intruder Repeater Window Help	
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts	
Intercept HTTP history WebSockets history Options	
Forwal Drop Intercept is off Action	Comment this item
Raw Parans Headers Hex	
	A
$ \cup\rangle$	
	ttps://blog.csdn.net/gg
Admin Panel X +	
(←) → × ŵ ① 120.78.92.198:8009/manager.php	
📄 火狐官方站点 🍨 新手上路 📄 常用网性 🗇 微博 🗇 携程旅行 🚭 百度 🔂 网址大全 🖽 京东商城 🔟 京东商城 💭 豪东商城	
	Admin Login
Us to traceru Pa	erName: admin
Us 输入任意密码 Pa	erName: admin ssWord: ••••• 《此连接不安全。在此页面输入的
Us 输入任意密码 Pa	erName: admin ssWord: ••••• 此连接不安全。在此页面输入的 登录信息可以被窃取。详细了解 https://blog.csdn.net/qq_38603541
Us 输入任意密码 Pa	erName: admin ssWord: ••••• 此连接不安全。在此页面输入的 登录信息可以被窃取。详细了解 https://blog.csdn.nel/qq_38603544
Us 输入任意密码 Pa Burp Suite Professional v1.6beta - licensed to LarryLau	erName: admin ssWord: ••••• 此连接不安全,在此页面输入的 登录信息可以被窃取。详细了解 https://blog.csdn.net/qq_38603541
Use 输入任意密码 Pa Surp Suite Professional v1.6beta - licensed to LarryLau Burp Intruder Repeater Window Help	erName: admin ssWord: ••••• 此连接不安全。在此页面输入的 登录信息可以被窃取。详细了解 https://blog.csdn.net/qq_38603541
Us: 输入任意密码 Pa Burp Suite Professional v1.6beta - licensed to LarryLau Burp Intruder Repeater Window Help Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts	erName: admin ssWord: ••••• 此连接不安全。在此页面输入的 登录信息可以被窃取,详细了解 https://blog.csdn.nel/qq_38603541
Us 输入任意密码 Pa Burp Suite Professional v1.6beta - licensed to LarryLau Burp Intruder Repeater Window Help Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts Intercept HTTP history WebSockets history Options	erName: admin ssWord: ••••• 此连接不安全。在此页面输入的 登录信息可以被窃取。详细了解 https://blog.csdn.net/qq_38603541
Us: 输入任意密码 Pa Burp Suite Professional v1.6beta - licensed to LarryLau Burp Intruder Repeater Window Help Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts Intercept HTTP history WebSockets history Options Request to http://120.78.92.198:8009	erName: admin ssWord: ••••• 此连接不安全。在此页面输入的 登录信息可以被窃取。详细了解 https://blog.csdn.net/qq_38603541
Us 输入任意密码 Pa Burp Suite Professional v1.6beta - licensed to LarryLau Burp Intruder Repeater Window Help Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts Intercept HTTP history WebSockets history Options Request to http://120.78.92.198:8009 Forward Drop Intercept is on Action	erName: admin ssWord: ••••• 此连接不安全。在此页面输入的 登录信息可以被窃取,详细了解 https://blog.csdn.net/qq_38603541 — □ X Comment this item
Us 输入任意密码 Pa	erName: admin ssWord: ••••• 此连接不安全。在此页面输入的 登录信息可以被窃取。详细了解 https://blog.csdn.net/qq_38603541 X
Us 输入任意密码 Pa Burp Suite Professional v1.6beta - licensed to LarryLau Burp Intruder Repeater Window Help Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts Intercept HTTP history WebSockets history Options Request to http://120.78.92.198:8009 Forward Drop Intercept is on Action Raw Params Headers Hex POST / manager.php HTTP/1.1 POST / manager.php HTTP/1.1	erName: admin ssWord: ••••• 此连接不安全。在此页面输入的 登录信息可以被窃取。详细了解 https://blog.csdn.net/qq_338603541 — — — — — — — — — — — — — — — — — — —
Second State Sta	erName: admin ssWord: ••••• 此连接不安全。在此页面输入的 登录信息可以被窃取。详细了解 https://blog.csdn.net/qq_38603541 × Comment this item ?
With Professional v1.6beta - licensed to LarryLau Burp Suite Professional v1.6beta - licensed to LarryLau Burp Intruder Repeater Window Help Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts Intercept HTTP history WebSockets history Options Poward Drop Intercept is on Action Raw Params Headers Hex POST / manager.php HTTP/1.1 Host: 120.78.92.198:8009 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 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	erName: admin ssWord: ••••• 此连接不安全。在此页面输入的 登录信息可以被窃取。详细了解 https://blog.csdn.net/qq_38603541 X
Us 输入任意密码 White Professional v1.6beta - licensed to LarryLau Burp Nuture Repeater Window Help Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts Intercept HTTP history WebSockets history Options Request to http://120.78.92.198:8009 Forward Drop Intercept is on Action Raw Params Headers Hex POST //manager.php HTTP/1.1 Host: 120.78.92.198:8009 User-Agent: Mostila/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0 Accept: Lext/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept: Language: sh-CN,sh;q=0.8, sh-TW;q=0.7, sh-HK;q=0.5, en-US;q=0.3, en;q=0.2 Accept-Encoding: gsip, deflate Content-Type: application/x-www-form-urlencoded Content-Type: application/x-www-form-urlencoded	erName: admin ssWord: ••••• 此连接不安全。在此页面输入的 登录信息可以被窃取。详细了解 https://blog.csdn.net/qq_38603541
小人任意密码 Wa Wa Max Burp Suite Professional v1.6beta - licensed to LarryLau Burp Intruder Repeater Window Help Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts Intercept HTTP history WebSockets history Options Post / manager.php HTTP/1.1 Host: 10.78,92,198:8009 Forward Drop Intercept is on Action Request to http://120.78.92.198:8009 User-Agent: Mozilla/5.0 West Content in the second in the seco	erName: admin ssWord: ••••• 此连接不安全。在此页面输入的 登录信息可以被窃取。详细了解 https://blog.csdn.net/qq_38603541 X
小社意密码 第A入任意密码 Walk Burp Suite Professional v1.6beta - licensed to LarryLau Burp Intruder Repeater Window Help Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts Intercept HTTP history WebSockets history Options Post /manager.php HTTP/1.1 Host: Action Post /manager.php HTTP/1.1 Host: 10.78.92.198:8009 Ser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0 Accept-Language: accept-Language: Sectort: text/thtml,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Content-Length: 21 Content-Length: 21 Content-Length: 21 Opgrade-Insecure-Requests: 11	erName: admin ssWord: ••••• 此连接不安全。在此页面输入的 登录信息可以被窃取。详细了解 https://blog.csdn.net/qq_38603541 X
小人任意密码 ● Burp Suite Professional v1.6beta - licensed to LarryLau Burp Intruder Repeater Window Help Target Proxy Spider Scanner Intruder Repeater Decoder Comparer Extender Options Alerts Intercept HTTP history WebSockets history Options Proward Drop Intercept is on Action Post / manager.php HTTP/1.1 Host: 120.78.92.198:8009 Ever-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0 Accept-Language: sh-CN, sh;q=0.8, sh-TW;q=0.7, sh-HK;q=0.5, en-US;q=0.3, en;q=0.2 Accept-Lencoding: gzip, deflate Content-Length: 21 Content-Length: 21 Content-Length: 21 Content-Length: 21 Content-Length: 21 Content-Parealive	erName: admin ssWord: ••••• 此连接不安全。在此页面输入的 登录信息可以被窃取。详细了解 https://blog.csdn.net/qq_38603541 X
Separation of the second sec	erName: admin ssWord: ••••• 此连接不安全。在此页面输入的 登录信息可以被窃取。详细了解 https://blog.csdn.net/qq_38603541
See Section 2015	erName: admin ssWord: ••••• 此连接不安全。在此页面输入的 登录信息可以被窃取。详细了解 https://blog.csdn.net/qq_38603541
Surp Suite Professional v1.6beta - licensed to LaryLau Burp Intruder Repeater Window Help Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts Intercept HTTP history WebSockets history Options @ Request to http://120.78.92.198.8009 Forward Drop Intercept is on Action Reser Learning Headers Hex POST / manager.php HTTP/1.1 Host: 120.78.92.198.8009 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0 Accept-Language: sh-CN, zh:q=0.8, sh-TW; q=0.7, zh-HK; q=0.5, en-US; q=0.3, en; q=0.2 Accept-Language: sh-CN, zh:q=0.8; ab:q=0.7, zh-HK; q=0.5, en-US; q=0.3, en; q=0.2 Accept-Language: sh-CN, zh:q=0.8; ab:q=0.9*/*; q=0.7, zh-HK; q=0.5, en-US; q=0.3, en; q=0.2 Accept-Language: sh-CN, zh:q=0.9; sh:g=009/manager.php Ugrade-Insecure-Requests: 1 JN取到的信息 user=adminispass=12345	erName: admin ssWord: ••••• 此连接不安全。在此页面输入的 登录信息可以被窃取。详细了解 https://blog.csdn.net/qq_38603541 X
White Professional v1.6beta - licensed to LarryLau Burp Suite Professional v1.6beta - licensed to LarryLau Burp Intruder Repeater Window Help Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts Intercept HTTP history WebSockets history Options Pervard Drop Intercept is on Action Porward Drop Intercept is on Action POST / manager.php HTTP/1.1 Host: 120.705.92.196:8009 Start. Hostilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0 Accept: text/html.application/xhtml+xml,application/xml;q=0.3, r/*;q=0.3 Accept-Encoding: gzip, deflate Content-Length: 31 Content-Length: 31 Content-Pequests: 1 MRX 9010fe8 User=admindpass=12345	erName: admin ssWord: ••••• 此连接不安全。在此页面输入的 登录信息可以被窃取。详细了解 https://blog.csdn.net/qq_33603541

Burp Suite Professional v1.6be	ta - licensed to	LarryLau								_	-		×
Burp Intruder Repeater Window	Help												
Target Proxy Spider Scar	ner Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Options	Alerts					
Intercept HTTP history Web	Sockets httory	Options											
Request to http://120.78.92.1 Forward Drop Raw Params Headers He	98:8009 Inte cep	ot is on	Action						Comment t	this item			?
POST /manager.php HTTP/1. Host: 120.78.92.198:8009 User-Agent: Mozilla/5.0 (Accept: text/html,applica Accept-Language: zh-CN,zh Accept-Encoding: gzip, de Content-Type: application Content-Length: 21 Connection: keep-alive Referer: http://120.78.92 Upgrade-Insecure-Requests user=admin&pass=12345	l Vindows NT :o=0.8,zh-T flate flate (x-www-form .198:8009/no : 1	10.0; Win xml,appli W;q=0.7,z -urlencod anager.ph	ı64; x64; r cation/xm] h-HK;q=0.5 led	cv:68.0) 1;q=0.9,* 5,en=US;c	Gecko/201 :/*;q=0.8 =0.3,en;q	00101	Send to S Do an act Send to Ir Send to S Send to C Send to C Send to C Request i Engagem Change b Copy URI Copy as o	Spider tive scan ntruder Repeater Sequence Comparer Decoder in browse ient tools equest m ody enco L curl com	er er sethod oding mand	Ctrl+I Ctrl+R			4
? < + > Type a	search term						Copy as to	ile niir	ps://blog.c		t/qq_	30 ma	tches

切换到burpsuite中的Intruder下的Position,这个时候我们可以看到一个重要的信息被标注了起来,我们现在爆破的是密码,并不需要爆破用户名,因此我们只选择密码就可以,把标注的用户名的参数取消掉就行,怎么取消?选中点击右边的Clear。

rp Intruder Repeater V	Vindow Hel	р											
arget Proxy Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Options	Alerts				
× 3 × 4 ×													
arget Positions Pay	loads Opt	ions											
Payload Position Configure the positi positions - see help	ns ons where p o for full deta	ayloads wi ils.	ill be inserte	d into the bas	se request.	The attack ty	vpe determin	es the way	/ in which	payload	s are assig	ied to pay	/load
Attack type: Snip	er						\rightarrow				•		
Attack type: Snip Accept: text/H Accept-Languag Accept-Encodir Content-Type: Content-LengtH Connection: ke Referer: http: Upgrade-Insecu user=SadminSkp	er html,appl ge: zh-CN hg: gzip, applicat h: 21 eep-alive ://120.78 ure-Reque pass=§123	ication/ ,zh;q=0. deflate ion/x-ww .92.198: sts: 1 45§	/xhtml+xm 8,zh-TW; ww-form-u :8009/man	il, applicat q=0.7, zh-H rlencoded accphp	ion/xml; K;q=0.5,	q=0.9,*/* en-US+q=0	;q=0.8 .3,en;q=0	.2				Add Clea Auto Refre	§ r§ sh
Attack type: Snip Accept: text/h Accept-Languag Accept-Encodir Content-Type: Content-Length Connection: ke Referer: http: Upgrade-Insect user=SadminSkp ? < +	er html,appl ge: zh-CN ng: gzip, applicat i: 21 eep-alive ://120.78 ure-Reque pass=\$123) > Typ	ication/ ,zh;q=0. deflate ion/x-ww .92.198: sts: 1 455 pe a searc	/xhtml+xm 8,zh-TW; ww-form-u :8009/man	l,applicat q=0.7,zh-H rlencoded accphp	ion/xml; K;q=0.5,	q=0.9,*/* en-U3+q=0	rq=0.8 .3,en;q=0	.2			0 matches	Add Clea Auto Refre	§ r§ § sh

之后,切换到Payloads下,并选择左侧的Load...添加密码字典,点击确定。

然后,选择最上方的Intruder下的Start attack开始进行密码破解。

🗧 Bu	rp Suite Professional v1.6bet	arryLau —		×
Burp	Intruder Repetiter window Heip			
Tarç	Start attack	peater Sequencer Decoder Comparer Extender Options Alerts		
	Open saved attack			
	Actively scan defined insertion points			
Targ	Send to Repeater			
	Save attack config			
?	Load attack config	•		
	Copy attack config	number of payload sets depends on the attack type defined in the Positions tab. Various payloa	d types are	e
	New tab behavior	, had type can be customized in different ways.		
	Automatic payload positions	Devland county 42		
	Configure predefined payload lists			
L	rayloau type. Simple list	Request count: 42		
?	Payload Options [Simple list] This payload type lets you configure a simple	le list of strings that are used as payloads.		
	Paste admin	A		
	admin12			
	Load admin888			
()	admin8			
\cup	admin123			
	Clear sysadmin			
	adminxxx			
	Add Enter a new item			
	Add from list	•		
		https://blog.csdn.net/)3541

由于密码字典是我自己现做的一个简单的密码字典,所以很快我们就可以破解完成。破解完成之后,我们点击 length进行排个序看看有没有不同的信息,排序之后,我们发现了长度为218的这一项比较特殊,点击之后跟其 他选项反馈的信息都不一样,这样基本上就能判定这个就是密码了.....

	5 Intrude	r attack (5								_		×
1	Attack Sa	ve Colu	mns										
2	Results	Target	Positions	Payloads	options								
2	Filter: Show	wing all it	tems							7			?
a	Request	Payload	ł		Status	Error	Timeout	Length 🔹	Comment				_
ay	40	0			200			582					
I	17	667788			200			218					
a 1	0				200			209	baseline request				
_	1	adm	in		200			209					
	2	admin1	2		200			209					
a	3	admin8	88		200			209					
ni	4	admin8			200			209					
	5	admin1	23		200			209					
	6	sysadm	nin 		200			209					
	1	adminx	xx		200			209					۳
-	Request	Respo	nse 🔶										
F		e adoro Ì	Hav										
		aders	пех										
	Date: Fri	200 OK 1, 19 J	ul 2019 1	2:15:09	GMT								^
	Server: A	pache/	2.2.15 (0	entOS)									
	x-Powered Content-L	i-By: Р Jength:	HP/5.2.17 25	ſ									
4	Connectio	on: clo	se										
	content-1	ype: t	ext/ntml;	crarse	t=01F-8								
ł													
	KEX{p08eq	ftulq4g	0a}										
a													
DI													v
	? <	+	> Туре	e a search	term							0 ma	atches
	Finished 📔								https://bl	og.csd	n.net/go	1 3860	03541
1	Edit					_							

其它选项爆出的信息,全都是Error这肯定不是啦!

5 Intrude	er attack 6						_		×
Attack Sa	ave Columns								
Results	Target Positions	Payloads Option	5						
Filter: Sho	wing all items								?
Request	Payload	Status	Error	Timeout	Length	Comment			
40	0	200			582				
17	667788	200			218				
0		200			209	baseline request			
1	admin	200			209				
2	admin12	200			209	1			
3	admin888	200			209				
4	admin8	200			209				
5	admin123	200			209				
6	sysadmin	200			209				
7	adminxxx	200			209				v
Request	Response								
Raw H	leaders Hex								
HTTP/1.1	200 OK								
Date: Fr. Server:	i, 19 Jul 2019 1 Apache/2.2.15 (0	L2:15:08 GMT CentOS)							
X-Powere	d-By: PHP/5.2.17	7							- 11
Content-1	Length: 16 op: close								
Content-	Type: text/html;	charset=UTF-8							
	_								
Error =D:	-								
2									-
									Ŧ
? <	+ > Type	e a search term						0 m	atches
Finished						https://bl	og esdn net/g	a 386	03541

好!现在我们将密码爆破出来以后就可以去网页上进行验证了!

现在我们回到浏览器里,关掉服务代理,输入刚刚爆破出来的密码,进行测试。

120.78.92.198:8009/manager.ph × +			
(←) → ♂ ŵ	(i) 120.78.92.198:8009/manager.php		
📄 火狐官方站点 🍯 新手上路 📄 常用网	网址 \ominus 微博 \ominus 携程旅行 \ominus 百度 \ominus 网址大全 🖨 京东商城 Đ 京东商城		
Error =。=			

测试结果......嗯????小老弟怎么回事???不对???破解出的密码不对???怀疑人生了,啊~

细心一点,看看网页还有什么猫腻......

哎~等等……破解出来的是6位数的密码,为什么密码输入框只能输入5位数,F12看看源代码吧……果然,给限制了,这就好办了,把maxlength的值改成6保存,然后输入密码,稳稳的OK。

Admin Panel	× +
(←) → C' û	(i) 💋 120.78.92.198:8009/manager.php
🔄 火狐官方站点 🧕 新手上路	🗎 常用网址 🕀 微博 💮 携程旅行 💮 百度 💮 网址大全 🗇 京东商城 🔟 京东商城 💭 京东商城
-	Admin Login
	UserName: admin PassWord: ••••• Login
	center 1904 × 105
	⊃ 调试器 {}样式编辑器 ⑦ 性能 ①:内存 1↓ 网络 😑 存储 🛉 无障碍环境
Q,搜索 HTML	
<pre>> <head> ··· </head></pre>	
★ <body></body>	
Admin_Login	
<pre> <form action="" method=" UserName: <input type=" nam<="" text"="" th=""><th>POST"> e="user" value="admin" maxlength="5"> name="pass" value="imaxlength="5"> 把这里maxlength的值改成6,然后保存执行</th></form></pre>	POST"> e="user" value="admin" maxlength="5"> name="pass" value="imaxlength="5"> 把这里maxlength的值改成6,然后保存执行

执行之后,再次输入破解出的6位数密码......哎~这返回的结果有点熟悉啊~这不是CTF的经常用到的答案格式 嘛,哈哈哈哈哈

120.78.92.198:8009/manager.ph; × +			
(←) → ♂ ŵ	(i) 120.78.92.198:8009/manager.php		
📄 火狐官方站点 🏮 新手上路 📄 常用网	网址 🕀 微博 🕀 携程旅行 🕀 百度 🕀 网址大全 🕀 京东商城 🗾		
KEY{p08eqfu1q4g0a}			

over! 结束!