## 攻防世界weak\_auth

## 原创

LEO-max ● 于 2020-01-22 10:08:31 发布 ● 2157 ☆ 收藏 2 分类专栏: CTF学习 生活会辜负努力的人,但不会辜负一直努力的人——Leo的个人博客。

本文链接: <u>https://blog.csdn.net/zouchengzhi1021/article/details/104067829</u>

版权



CTF学习 专栏收录该内容

32 篇文章 3 订阅

订阅专栏

此题的登入界面不知道为何做完之后就打不开了,所以我就不在这黏贴界面。

首先要我们随便输入username和password,跳出的check.php界面要求username为admin,所以我们只要知道密码就OK了。 用burpsuite破解

Surp Suite Professional v1.6 - licensed to LarryLau –											
Burp Intruder Repeater Window Help											
Target Proxy Spider Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extend	er Options	Alerts			
Intercept HTTP history WebSocke	ts history	Options									
Filter: Hiding CSS, image and general binary content									?		
# 🔺 Host	Method	URL			Params	Edited	Status	Length	MIME 1		
1 http://111.198.29.45:42786	POST	/check.p <mark></mark>				0	1		HTML 🔺		
2 http://detectportal.firefox.com	GET	/success	http://111.198.	29.45:42786	/check.php		200	384	text		
3 http://detectportal.firefox.com	GET	/success	Add to scope				200	384	text		
4 http://detectportal.firefox.com	GET	/success	Spider from he	re			200	384	text		
5 http://detectportal.firefox.com	GET	/success	Do an active so	an			200	384	text		
6 http://detectportal.firefox.com	GET	/success	Send to Intrude	er.		Ctrl+I	200	384	text		
7 http://detectportal.firefox.com	GET	/success	Send to Renea	tor		Ctrl+R	200	384	text		
8 http://detectportal.firefox.com	GET	/success	Sond to Soque	ncor		ounit	200	384	text		
9 http://detectportal.firefox.com	GET	/success	Send to Seque	ncer			200	384	text		
10 http://detectportal.firefox.com	GET	/success	Send to Compa	arer			200	384	text		
11 http://detectportal.firefox.com	GET	/success	Request in bro	wser		•	200	384	text 🔽		
•			Engagement to	ols		•		_			
Request			Show new histo	ory window			-				
Request			Add comment								
Raw Params Headers Hex			Highlight			•					
Dogm (she she timp)(1, 1			Delete item								
Host: 111.198.29.45:42786			Clear history								
User-Agent: Mozilla/5.0 (Wi	ndows N	т 10.0	Copy URL				0101 Fire	efox/72	. 0		
Accept: text/html,applicati	.on/xhtm	l+xml,	Copy as curl co	ommand			*/*;q=0.8	3			
Accept-Language: zh-CN,zh;c	{=0.8,zh	-тพ;q=	Save item				0.2				
Accept-Encoding: gzip, defl	.ate		Proxy history h	elp			-				
Referer: http://111.198.29.45:42786/											
Content-Type: application/x-www-form-urlencoded											
Origin: http://111.198.29.4	15:42786	j									
Connection: keep-alive											
Upgrade-Insecure-Requests:	1										
Cache-Control: max-age=0											
username=1&password=1											

## 打开intruder选项卡

2

Burp Suite Professional v1.6 - licensed to	_		×								
Burp Intruder Repeater Window Help	Burp Intruder Repeater Window Help										
Target Proxy Spider Scanner Intrude	Repeater	Sequencer	Decoder	Comparer	Extender	Options	Alerts				
Target Positions Payloads Options											
Payload Positions Configure the positions where payloads will assigned to payload positions - see help for Attack type: Sniper POST /check.php HTTP/1.1 Host: 111.198.29.45:42786 User-Agent: Mozilla/5.0 (W. Gecko/20100101 Firefox/72.1) Accept: text/html, application/xhtml8 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7, Accept-Encoding: gzip, def. Referer: http://111.198.29. Content-Length: 21 Origin: http://111.198.29. Connection: keep-alive Upgrade-Insecure-Requests: Cache-Control: max-age=0 username=admin&password=\$14	be inserted in r full details. .ndows NT .+xml, appl .ate 45:42786/ c-www-form 15:42786	to the base red 10.0; Win .ication/x 0.5, en-US; n-urlencod	quest. The a	ttack type det rv:72.0 , image/w n;q=0.2	ermines the v	way in which	h payloads Clea Aut Refr	are I§ ar§ esh			
2											

## 注意:要把admin两边的符号给删了,只保留psaaword的

☑ 文章管理-CSDN博客 X ☑ 文章管理-CSDN博客 X ☑ 写文章-CSDN博客 X +	- 0 ×
$\leftarrow \rightarrow C$ (a) editor.csdn.net/md?articleId=104067829	☆ 🖻 🕒 :
👬 应用 M Gmail 🖸 YouTube 【 Maps 🍹 Translate 🔮 News 🧭 BUUCTF 💋 DWWA安装数程-ci 🤦 CSDN-专业IT技术 🖄 php 弱类型总结	
< 文章管理 攻防世界weak_auth  Surp Suite Professional v1.6 - licensed to LarryLau - ロ ×	保存草稿    发布文章
B I H S 注 注 活 66 〈/〉 加組 斜体 振題 删除线 无序 有序 符办 引用 代码块	帮助文档 X
1 ×     2 ×        Target     Positions     Payloads     Options	快捷键
Payload Sets	
![在这里插入图片描述]( <u>https://imq-blog.csdnimg.cn/2020012209</u> ) OSS-	撤销: Ctrl/Command + Z 重做: Ctrl/Command + Y
	J山祖: Ctri/Command + B

注意:要把admin两边的符号给删了,只保留 <u>psaaword</u> 的	年用原文用学名和奇趣部分 3395g報子典 txt 11日間 11日間 11日間 11日間 11日間 11日間 11日間 11日	插入代码: Ctrl/Command + Shift + K 插入题片: Ctrl/Command + Shift + L 插入图片: Ctrl/Command + Shift + G 查找: Command + F 替换: Command + G
Markdown 587 字政 9 行政 当前行 8, 当前列 0 文章已保存10-00:59 팩	Add trom list Payload Processing You can define rules to perform various processing tasks on each payload before it is used.	## 1级标题 ### 2级标题 ### 3级标题

进入Payloads选项卡,在Payloads Option 中选中load,找到你下载的字典。

4	Bur	p Suite Profe	ssional v1.6 - licensed to La	arryLau					_		×
Bui	p	ntruder Repea	ter Window Help	_							
Т	arç	Start attack		Repeater	Sequencer	Decoder	Comparer	Extender	Options	Alerts	
	=	Open saved a	ttack								
1	×	Actively scan	defined insertion points								
Т	arç	Send to Repe	ater								
		Save attack co	onfig 🕨 🕨								
	?	Load attack co	onfig 🕨								
		Copy attack c	onfig 🕨 🕨	number of	payload sets o	lepends on t	the attack typ	e defined in t	the Position	stab. Var	ious
		New tab behav	vior	et, and eac	h payload type	e can be cus	tomized in dif	ferent ways.			
		Automatic pay	defined readered lists	_							
		Configure pre	defined payload lists	Payload	count: 7,501						
		Payload type:	Simple list	Request	count: 7,501						
	?	Payload Opt	ions [Simple list]								
		This payload ty	/pe lets you configure a simple	list of string	s that are used	as pavload	s.				
			, - · · · · J - · · · · · J - · · · · · ·								
		Paste	ĩ» ¿admin								
			admin12								
		Load	admin888								
		Demons	admin8								
		Remove	admin123								
		Clear	sysadmin								
		$\square$	adminxxx								
			admina								
		Add	Enter a new item								
		Add from list									
		Add from fist									
	?	Payload Pro	cessing								
		You can define	rules to perform various proce	essing tasks	on each pavlo	ad before it i	is used.				
<b>~</b>											

🗲 Intrude	attack 1						- 0	×
Attack Sav	e Columns							
Results	Target Positions Payloads	Options						
Filter: Show	ving all items							?
Request 4	Payload	Status	Error	Timeout	Length	Comment		
29	135246	200			434			
30	135246789	200			434			
31	123456	200			437			
32	654321	200			434			
33	12345	200			434			
34	54321	200			434			
35	123456789	200		<u> </u>	434			
30	1234567890	200			434			
37	102	200		U	434			
30	123qweaed	200			434			
40	nweasd	200			434			
			0	0				
Request	Response							
								_
I Kaw I I	arama neaders nex							_
POST /ch	eck.php HTTP/1.1 1 108 20 45-42786							-
User-Ade	nt: Mozilla/5.0 (Windo	ows NT 1	0.0; Wina	64; x64;	rv:72.	0) Gecko/20100101 Firefo	x/72.0	
Accept:	text/html, application/	/xhtml+xr	ml, applid	cation/x	cml;q=0.	9,image/webp,*/*;q=0.8		- 11
Accept-L	anguage: zh-CN,zh;q=0.	8,zh-TW	;q=0.7,z]	h-HK;q=0	).5,en-U	IS;q=0.3,en;q=0.2		- 11
Accept-E	<pre>ncoding: gzip, deflate http://111 100 20 45.</pre>	9 . 42786/						- 11
Content-	Type: application/x-w	w-form-1	urlencode	ed				- 11
Content-	Length: 30							- 11
Origin:	http://111.198.29.45:4	42786						- 11
Connecti Ungrade-	on: close Insecure-Requests: 1							- 11
Cache-Co	ntrol: max-age=0							- 11
username	=admin&password=123456	8						- 11
								- 11
								- 11
								- 11
								- 11
								Ŧ
? <	Type a search t	term					0 mat	ches
Finished							https://blog.csdn.net/zouchengzhi	021

在出现的result界面中进行一系列字典密码进行尝试,我们需要找到Lenth不同的密码,这个密码就是正确密码。

🧲 Result	31   Intruc	der attack	:1	_	
Payload: Status: Length: Timer: Request	123456 200 437 51 Respons	e			Previous Next Action
Raw He	aders	lex HTN	IL Render		
□ DOCTYN<br <html lan<br=""><head> <meta <tit </tit </meta </head> <body></body></html>	PE html ng="en" a chars le> <b>weak</b>	> > et="UTH auth </td <td>7-8"&gt; /title&gt;</td> <td></td> <td></td>	7-8"> /title>		
cyberpead	ce{4b77	58f8dd3	20eb80692	2 <mark>d836c3db9bc5}</mark> maybe you need a dictionary-</td <td>-&gt;</td>	->
 					V
? <	) + (	> Ty	pe <mark>a s</mark> earch <mark>t</mark> er	m https://blog.csdn.net/zou	ichen Ozmatches

打开正确密码的界面就可拿到flag.