

订阅专栏

使用burpsuite密码爆破,步骤如下,

第一步 设置代理 第二步 随便在原界面输入一个密码 第三步 抓包

然后这里我们可以看到burp已经抓取到刚才输入的数据了 Sup Suite Professional v1.7.33 - Temporary Project - Licensed to surferxy: Urg Brunder Knoben Help Terget Window Help Terget Window Help Terget Window Help Terget Window Help WetSockets hintory (VetSockets hintory (VetSo

## 第四步 抓到包以后准备改包

#### 然后全选



第五步

Burp Su	ite Profes	sional v1	7.33 - Ten	porary Pr	oject - lice	nsed to s	surferxyz						
arget Pr	exy Spide	r Scann	r Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	Alerts		
× 2 ×	3 ×			1									
rget Po	ositions Pa	ayloads (	Options										
Attac Confi	ck Target gure the deta	ails of the t	arget for the a	ttack.									
Host Port:	120.24.86 8002	145											
🗆 U	Ise HTTPS	如界	<b>是是H</b>	<b>TTPS</b>	的则	需要	勾进	HTT	PSg. c	sdn. r	net/	Cliff	ord

然后在Positions中点击clear清除burp认为需要猜测的密码,然后选中12345(也就是我们刚才输入的密码,点击add)

<pre>species Notes Note Notes Notes</pre>	Add 5 Over 5 Add 5 Ratest
reg on the filter filter filter filter filter filter filter filter for the filter filt	Add 5 One 5 Add 5 Refer
2 Particular Section      2 Particular	Add () Char () Add () Rafeet
Provide Text State And Text State And Text State	Add 5 Add 5 Add 5 Refere
Book and the second of the second of the base register. The stack high distances are register to palad proteins - see togs for 16 distances     Constraining and the second of the base register. The stack high distances are register to palad proteins - see togs for 16 distances     Constraining and the second of the se	Add 5 Add 5 Char 5 Add 5 Robush
Product for proteiner dens ingelande will be searched like faile allementers. Here sign is a black huge blace weiger is to glack alle glace allementers. Here sign is a black huge blace allementer alle black data.     Image: Control of the search of the sea	All 5 Over 5 All 1 Refer
No fair line line line line line line line line	All [ Our ] Adv ] Refer
Professional of 3.23. Tengony Project - Scend to surfary: the factor form from the factor form former (comer (former	All 5 Our 5 All 1 Relea
her CSN kiteber honzyk kitebe	All I All I All I Refer
Interpretended (1990) (	Over 1 Auto 1 Rathealt
Invest departy in Charge 3 and registration of a subface 3 and	Ada 1 Rahadi
have finders gins date: Construing in a date: Construing in a date: Construing in a date: Supplish how setting in a date: Supplish how finder: All - Frequency hojes: - Scenad to suffrage: 	Ratest
Deter Spins galaritation marketenedering Spinster Spinster Strategie galaritation marketenedering Spinster Nordsward x12.31 - Temporary Project - Konned Its surferge Promite Report Strategie Strategie Geneter (Engent United Temporary Strategie Compare (Engent United Temporary Str	
Terret cliph 3 Specific Normal Specific Specifi	
Sapada Imanon Rayon, 1 perfections Rayon Markov Million, 17,33 - Temporum Project - Konned Its surfering: 	
and 4000 https://bio.com/source.com/source/s	
hug Sala Holmsiona's 2.31 - Temporay Physics - Konned to surfering: — — — — — — — — — — — — — — — — — — —	
httpp://klig.table.teg http://klig.table.teg these factor factors factor these factors factors factor get [free] factor [factor [factor [factor [factor [factor [factor ] factor]]]	
hug Salah Nofessional x1.2.33 - Temporug Project - Kontead Its surfering:	
herp faith Fudersland +13.31 - Temporary Insject - Icensed to surferge = 0 p Index Fuders Televis NB gel [ <sup>1</sup> /m <sup>2</sup> ] faith [Isaner] [Isa	
hurg Salah Nofesiland x1.2.33 - Temporary Neject - Konned ta surfering: - et al. p Instante Researce Window Neje gen (mmr [ Same ] Same Balance ] Samerer [ Scheder ] Engene and [ Samerer ] Samere ] Samerer [ Samerer ] Same	
http://shift hofestacia/s1/2.32 - Fergeory Project - Formed to suffering = - ( phile frazer: State / S	
j hole Registe (Role N) get Men (Bale Role State) Bilder Route State Corpor (Scote Corpor State New State )	<b>a</b> )
The Constant Sector Sec	
	_
pp [Paulates Payloads Cators	
Poplad Politions	Mart attack
Configure the positions where puplicals will be instantial into the base sequent. The attack type determines the way in which puplicade are assigned to puplicad positions - see help for 6d details.	
Abstige Sept	
Rolf Assertion (RNA )	
Here: C0104861484000	
New Agent Microlle 50 (Binduse NF 10), WOMA, will 00 Gastra 2000001 Parks 800 (	Ones
Annya Language and Langed and the god annual god an end of the god	Ans
Acception of a set of the set of	-
Control Tage 2010 (2011) The Marketing of 1914 Control Tage 2010 (2011) The Marketing of 1914	-
[metaps]	
nttps://blog.csdn.net/Glittor	
neepb., / biog. ebuil. nee, citii	

## 第七步

接下来设置参数,因为只有一个变量,所以Payload SET就是1,数字类型,从10000到99999,步数为1

Target	Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	Alets		
• . I	2.12	11							-			-		
1.1.1.	an jan		. Te		_							_		
Target	Position	s Pay	loads Opt	tions										
?	Payload !	Sets												
1	You can de	efine one	or more pay	yload sets	The numb	er of payload :	sets depend	is on the atta	ack type defi	ned in the Positio	ns tab. Various	payload t	ypes are available	for each payload set.
F	Payload se	e 1			Paylo	ad count: 90.	000							
	Pauload tu	ne No	mbers		-	est count: 90	000							
	a).cas ()	Pr. [100				in their re.								
	Dandarad d	Ontions	Disabas	-1	岩	1字类	利							
2	-ayioad v	option	(Incompet	a)										
	res paytos	so type g	perseraces ins	menc pay	idadis within	a gotes range	e and in a s	pecilied iorin	um.					
1	lumber rai	nge												
1	Type:		() Sequ	ential () F	Random									
1	From:		10000											
1	fo:		99999											
-	Step:		1											
,	How many													
	umber for	mat												
			(C) Deale		law.									
E	Base:		· Decin		HEX.		2011				the second second		1	
8	Base: Min integer	digits:	C Decin		HEA.		h	ttps	:://	blog.	csdn	. ne	t/Cli	ffordF

### 然后设置线程,电脑差不多的就直接设置为100

Target Proxy S	Spider Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	Alerts
1 × 2 × 3 ×										
Farget Positions	Payloads Op	tions 🖌	-							
Request	leaders									
1 magazan										
3 These settin	gs control whether	Intruder up	pdates the c	onligured requ	jest header	s during attac	:KS.			
Update (	Content-Length hea	ader					/			
Set Con	nection: close					/				
Set Con	nection: close					/				
Request E	nection: close				/					
Set Con Request E These settin	nection: close	ine used fo	r making H1	TP requests	when perform	ming attacks				
Set Con     Request E     These settin     Number of th	nection: close ingine gs control the engineeds:	ine used fo	r making HT	TP request	ahen perfori	ming attacks				
Set Con Request E These settin Number of th Number of th	nection: close ingine gs control the engi meads: tries on network fi	ine used fo ailure:	r making HT	TP request	ahen perfori	ming attacks				
Set Con     Request E     These settin     Number of th     Number of re     Pause before	ection: close ingine gs control the engi rreads: tries on network fit e retry (milisecond	ine used fo ailure: fs):	r making HT	TP require	ahen perfor	ming attacks		sdn net	t/Clif	for



### 然后开启猜测

0	Open saved attack							1
								-
arg S	Actively scan defined insertion points Send to Repeater	_					 	-
? L	Save attack config Load attack config Copy attack config	► ► ► as the c	onfigured requ	uest header	s during atta	cks.		
NA	Vew tab behavior Automatic payload positions	*						
C	Configure predefined payload lists							

# 第十步 出结果

## 然后可以点击Length查看哪一个返回值与其他的不同,那么这个就一定是密码了,因为就这一个成功了

🚯 Intru	ider atta	ack 3									-		×
Attack S	ave Colu	mns											
Results	Target	Positions	Payloads	Options				1					
Filter: She	owing all it	tems	/										?
Request	Payload		S	tatus	Error	Timeout	Leng	A Com	ment				
3580	13579		2	00			246						
0			2	00			1327						
1	10000		2	00			1327						1
2	10001		2	00			1327						- 1
3	10002		2	00			1327						- 1
4	10003		2	00			1327						- 1
5	10004		2	00			1327						- 1
6	10005		2	00			1327						- 1
7	10006		2	00			1327						- 1
9	10008		2	00		t+Qe	.1327/1-	100		not	/01	iffo	rdle