信息安全铁人三项赛--资质赛writeup



[博客目录]

- 工具
 - Burp Suite
 - stegsolve.jar
 - 十六进制编辑器
- · 赛题
 - 第一题
 - 第二题
 - 第三题
 - 第四题
 - 第五题
 - 第六题

1-工具:

1.1- Burp Suite

一款可以进行再WEB应用程序的集成攻击测试平台。 常用的功能:抓包、重放、爆破

需求: (建议)Burp Suite + Firefox
介绍: Burp Suite使用介绍
代理设置+证书导入: Firefox+Burpsuite抓包配置(可抓取https)
使用方法:

- Burpsuite神器常用功能使用方法总结
- Burpsuite中爆破功能的使用教程
- Burpsuite教程与技巧之HTTP brute暴力破解
- 用Burpsuite破解网站密码

```
1.2- stegsolve.jar
```

下载&使用

1.3-十六进制编辑器

自己上网找吧!

返回目录

2- 赛题

2.1 第一题:你是管理员吗?

```
题目链接: http://ctf4.shiyanbar.com/web/root/index.php
解题步骤:
```

1. 首先查看源代码,主页面的标题是password.txt,尝试访问password.txt: http://ctf4.shiyanbar.com/web/root/password.txt

	出现字典:
	C () otf/ chivaphar.com/web/root/paceword tyt
	C O Cti4.sniyanbar.com/web/root/password.txt
	iii 应用
	584521
	Johack
	45189946
	hacksb
	hackersb
	heixiaozi
	360
	yushiwuzheng
	witheng
	spider
	lex
	nc
	hackgingshu
	gingshu
	qingshu\$
	SZ
	Suizi shunzi
	12318#
	10#123
	123654
	123654789
	1236547891
	123654789.
	aspaomin
	phpadarn
2	使用Runo Suite爆破.
۷.	这们Duip Outer承认。 若出门马之曲 随届食个门重大部行 甘至百捽放左前阯板。
	日九七次于兴,随便事!七岁不须行,在土且这就让另知认; 打工Dun Quite 如道历日,土土Drange between stranger is a ft 如 1. 之中亦式 between is an
	打开Burp Suite, 制建项目, 点击ProxyIntercept 下面的Intercept IS OII按钮, 值 已变成Intercept IS OII:
	Burp Suite Free Edition v1.7.16
	Burp Intruder Repeater Window Help
	Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Company
	Intercept HTTP history WebSockets history Options
	Forward Drop Intercept is on Action
	Raw Params Headers Hex

再次访问index.php,页面会一直保持载入,说明已经被Burp Suite抓包,点击forward,让页面加载出来,随便输入几个数,试图登录,页面卡住(被抓包),这时回到Burp Suite,在抓包界面(注意raw里面会出现彩色变量username=admin&password=123)点击action按钮,选择Send to Intruder:

Burp Intruder Repeater Window Help Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options Use Intercept HTTP history WebSockets history Options Request to http://ctf4.shiyanbar.com:80 [106.2.25.8] Forward Drop Intercept is on Action Raw Params Headers Hex POST /web/root/index.php HTTP/1.1 Host: ctf4.shiyanbar.com User-Agent: Nozilla/5.0 (Nacintosh; Intel Mac OS X 10.13; rv:59.0) Gecko/20100101 Firefox/59.0 Accept: text/htm1.application/xhtm1;m1,application/xm1;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 Referer: http://ctf4.shiyanbar.com/web/root/index.php Content-Length: 27 Connection: close Upgrade-Insecure-Requests: 1 Username=admintpassword=123				Burp Suite F	ree Editio	n v1.7.16 - T	emporary F	Project	
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options Use Intercept HTTP history WebSockets history Options Image: Request to http://ctf4.shiyanbar.com:80 [106.2.25.8] Image: Request to http://ctf4.shiyanbar.com:80 Intercept is on Action Raw Params Headers Hex Hex Post /web/root/index.php HTTP/1.1 Hoat: ctf4.shiyanbar.com Useriandon/xml;q=0.9,*/*;q=0.8 Accept: Language: zh-CW,zh;q=0.7, zh-HK;q=0.5, en-US;q=0.8 Accept: text/html,application/xhml*xml,application/xml;q=0.9,*/*;q=0.8 Accept:Cometic.elon8 Ac	Burp Intruder Repeater Window Help								
Intercept HTTP history WebSockets history Options Request to http://ctf4.shiyanbar.com:80 [106.2.25.8] Forward Drop Intercept is on Action Raw Params Headers Hex POST /web/root/index.php HTTP/1.1 Host: otf4.shiyanbar.com User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:59.0) Gecko/20100101 Firefox/59.0 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: http://ctf4.shiyanbar.com/web/root/index.php Content-Type: application/x-www-form-urlencoded Content-Type: application/x-www-form-urlencoded Content-Content-Content-Content-Content-Content-Conte	Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User								
Request to http://ctf4.shiyanbar.com:80 [106.2.25.8] Forward Drop Intercept is on Action Raw Params Headers Hex POST /web/root/index.php HTTP/1.1 Action Action Wast- stf4.shiyanbar.com User-Agent: Mozilla/5.0 (Macintosh; Intel Nac OS X 10.13; rv:59.0) Geoko/20100101 Pirefox/59.0 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 Refere: http://ctf4.shiyanbar.com/web/root/index.php Content-Type: application/x-www-form-urlencoded Content-Length: 27 Connection: close Upgrade-Insecure-Requests: 1 username=admin&password=123	Intercept HTTP history	WebSockets history	Options	•		•	•		.
<pre>POST /web/roct/index.php HTTP/1.1 Host: ctf4.shiyanbar.com User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:59.0) Gecko/20100101 Firefox/59.0 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 Referer: http://ctf4.shiyanbar.com/web/root/index.php Content-Type: application/x-www-form-urlencoded Content-Length: 27 Connection: close Upgrade-Insecure-Requests: 1 psername=adminEpasaword=123</pre>	Request to http://ctf4.shiyanbar.com:80 [106.2.25.8] Forward Drop Intercept is on Action								
	<pre>oat: ctf4.ahiyanbar.com aer-Agent: Mozilla/5.0 ccept: text/html,applic ccept-Language: zh-CN,z eferer: http://ctf4.ahi ontent-Type: applicatio ontent-Length: 27 onnection: close pgrade-Insecure-Request aername=admin&pasaword=</pre>	<pre>/ nrr/1.1 (Macintosh; Inte ation/xhtml+xml, sh;q=0.8,zh-TW;q= yanbar.com/web/r yn/x-www-form-url ca: 1 =123</pre>	el Mac OS applicati =0.7,zh-Ht :oot/index Lencoded	x 10.13; r on/xml;g=0 ;g=0.5,en-0 ;ephp	v:59.0) G .9,*/*;g= US;g=0.3,	ecko/20100 0.8 en;g=0.2	l0l Pirəfo	ox/59.0	
点击最上面菜单栏的Intruder选项(变成橘黄色的),点击该页面下的position选项,先点clear清除变量(因为I 中用户名username和密码password双变量,双变量爆破会很慢,因为index中的用户名是固定的admin,我	素击最上面菜单栏的Intru ヨ用户名username和密码	uder选项(变成橘 码password双变	黄色的), 量,双变	点击该页ī 量爆破会很	面下的po 夏慢,因シ	sition选项 与index中的	,先点cle 的用户名员	ar清除变量(是固定的admin	因为B ,我们

确定: Payload Positions Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details. Attack type: Sniper POST /web/root/index.php HTTP/1.1 Hoat: ctf4.shiyanbar.com User-Agent: Mozilla/5.0 (Macintosh; Intel Kac OS x 10.13; xv:59.0) Gecko/20100101 Firefox/59.0

Accept: text/html,application/xhtml+xml,application/xml;g=0.9,*/*;g=0.8	Clear §
Accept-Language: zh-CN,zh;g=0.8,zh-TW;g=0.7,zh-HK;g=0.5,en-US;g=0.3,en;g=0.2	
Referer: http://ctf4.shiyanbar.com/web/root/index.php	
Content-Type: application/x-www-form-urlencoded	Auto §
Content-Length: 27	
Connection: close	Refresh
 Upgrade-Insecure-Requests: 1	
username=admin&password= <mark>g123g</mark>	

然后点击payload按钮(设置字典),在payload options这一块中,将原本的字典复制进剪贴板,然后点paste,或者直接导入文件也行:

Burp Intruder Rep	eater Windov	v Help									
Target Proxy	Spider Sca	nner Int	uder	Repeater	Sequencer	Decoder	C				
3 × 4 ×											
Target Positions	Payloads	Options									
? Payload Se You can defin available for e	ts e one or mor each payload e	e payload s set, and ea	ets. Th ch payl	ie number o load type cai	f payload sets n be customiz	depends o ed in differe	n tł ent				
Payload set:	1		•	Payload	count: 198						
Payload type: Simple list Request count: 198											
Payload Op This payload	type lets you	ple list] configure a	a simpl	e list of strir	is that are us	ed as paylo	ad				
Load	nohack 45189946 hacksb hackersb				D						
Clear	heixiaozi 360 yushiwuzhe wuzheng	eng			Ļ						
Add	Enter a new	item									
Add from lis	it [Pro versi	on only]			Y						

导入后直接点击右上角start attack按钮,等待......

结果是发现密码:Nsf0cuS(一长串的1924都是错误回应,那么一个2063应该很明显了.....)

•••				Intruder a	ttack 1		
Attack Sav	ve Columns						
Results	Target Positions Paylo	oads Options					
Filter: Show	ving all items						?
Request 🔺	Payload	Status	Error	Timeout	Length	Comment	
73	WESKY	200			1924		
79	54321	200			1924		n
75	521	200			1924		
77	521	200			1924		
78	4lert	200			1924		
79	maek	200		-	1924		
80	dreamh	200	ă	Ĩ	1924		
81	Shell	200	ă	ă	1924		
82	Nsf0cuS	200	ŏ	ă	2063		
83	shell	200	ā		1924		
84	10011C120105101	200			1924		
85	fclshark	200			1924		
86	19880118	200			1924		
87	376186027	200			1924		Y
Paused							
- aasea							

3. 找到密码后,我们关掉抓包: Intercept is off或者直接点Forward, 我们将结果输入password.txt页面,发现只能输入五位数!?看来不行,我们得用Burp Suite来登录了,再次开始抓包 Intercept is on(如果之前点forward就不用了, Intercept会一直保持),我们随便输入一些数进去,然后登录,页面再次加 载,我们抓到包后看到raw中的可修改的彩色部分:

Forward	Drop	Intercept is o		Action						
Raw Params Hea	ders Hex									
POST /web/root/ind Hoat: ctf4.ahiyanb. User-Agent: Kozill. Accept: text/html, Accept-Language: z Referer: http://ct: Content-Type: appl. Content-Type: appl. Content-Tength: 29 Connection: close Upgrade-Insecure-Ru username=admin&past	ax.php HTTP/1. ar.com a/5.0 (Macinto application/xh -CN,zh;q=0.8, 54.shiyanbar.c ication/x-www- equests: 1 aword=NsfOc	l ah; Intel Ma tml+xml,appl zh-rw;q=0.7, om/web/root/ form-urlenco	OS X catio h-HK; ndex. ed	10.13; n/xml;g= g=0.5,en php	rv:59.0) 0.9,*/*; -VS;g=0.	Gecko/2(g=0.8 3,en;g=0.	.2			
我们再次点击actio 按钮, Response中 Cookie:newpag	n按钮,选择S u出现信息,发 e=MjkwYmNb	end to Repe 现Set- NZBiN2Rh	ater按 [Tkz2	我们(重) ZGI2Ni	<mark>汝功能)</mark> OOZmEv	,在Red	quest栏中将 DgzYjkuc(子 password改 う Ghw;	∮Nsf0cuS,	点击go
bingo! 但是还是没	有找到flag!				2			,		
Purp Intruder Repeater V	Vindow, Help	Bur	Suite F	Free Editior	n v1.7.16 - T	emporary F	Project			
Target Proxy Spider	Scanner Intrude	r Repeater Se	uencer	Decoder	Comparer	Extender	Proiect options	User options A	lerts	
$1 \times 3 \times 5 \times 6$	· · · · ·						· · · · · · · · · · · · · · · · · · ·			
Go Cancel	< v > v							Target: http	x://ctf4.shiyanbar.	com 🖉 [
Request					Res	ponse				
Raw Params Headers	Hex				Ra	W Headers	Hex HTML	Render		
<pre>POST /web/toot/index.p Host: ctf4.shiyanbar.c User-Agent: Mozilla/5. rv:59.0) Gecko/2010010 Accept: text/html,application/ Accept-tanguage: zh-CN,zh;q=0.8,zh-TW;q Referer: http://ctf4.s Content-Type: applicat Connection: close Upgrade=Insecure=Recue sername=adminEpasswor</pre>	np HTTP/1.1 om O (Macintoah; Ir 1 Firefox/59.0 xhtml+xml,applic =0.7,zh-HK;q=0.5 hiyanbar.com/web ion/x-www-form-u ata: 1 d=NafOcus	tel Mac OS X l ation/xml;g=0. (,en-US;g=0.3,e /root/index.ph rlencoded	1.19; ;,*/*;g ;g=0.2	=0.8	HTTP Serv. Date Cont Conn Vary Set- newp Cont Cont Cont Cont Cont Cont Cont Cont	<pre>1.1 200 00 1.1 200 0 1.1 200 0 1.1 200 0 1.1 200 0 1.1 200 0 1.1 200 0 1.1 200 0 1.1 200 0 1.1 200 0 1.1 200 0 1.1 1 2.1 1 2.1</pre>	<pre>K Mar 2018 08:3 text/html oae ncoding PMP/3536 NhuzEju2RhsTk 'ouiv="Conte '> old "bgcolor= " charset="ut rr: 50%; KARG N: absolute; ign:left;marg ly:'Courier N POST" action= ext" name="us ext" name="us ubmit" value= ed " >这里没有fl </pre>	4:13 GMT INSERTING CONTENT INSERTING CONTENT INSERTING CONTENT INSERTING INSERTINA	580ggxjkucGhw; ="text/html; gold" text="#0(px -370px; WID1 ; 330px"> 3" cellapacing: t-aize: ength="5" value) 08000" CH: ="3"

4. 我们对MjkwYmNhNzBjN2RhZTkzZGI2NjQ0ZmEwMGI5ZDgzYjkucGhw;进行base64解码, 结果为: 290bca70c7dae93db6644fa00b9d83b9.php 关掉抓包: Intercept is off 赶紧访问试试: http://ctf4.shiyanbar.com/web/root/290bca70c7dae93db6644fa00b9d83b9.php 发现又是一个新界面,还没结束!打开抓包,随便输入点东西: 🛃 新手上路 🗎 常用网址 📕 京东商城

小黑留言板



5. flag终于出现!但是!注意这个格式!千万不要以为直接输入上面的数就可以了!错!

【答案格式】: flag{}

flag{flag%7BC0ngratulati0n%7D}

因为%7B和%7D是{和},所以答案应该再进行url解码!

Native/Unicode	Native/UTF-8	Native/ASCII	URL转码		
Url:					编码结果:
flag{C0ngratulati0n	}			• encodeURI	flag%7BC0ngratulati0n%7D
					onent
				URL编码 >	
				 ✔ URL解码 	

返回目录

2.2 第二题: iOS

解题链接: http://ctf4.shiyanbar.com/web/IOS/index.php

1. 打开解题界面后,出现系统升级至iOS99字样,由此可以推出,需要修改User-Agent,打开burpsuite,进入下图选项卡

💈 Burp Suite Free Edition v1.7.03 - Temporary Project — 🗆 🛛 🕹												
Burp Intruder Repea	Burp Intruder Repeater Window Help											
Target Proxy S	pider Scar	ner Intrud	er Repeater	Sequencer	Decoder	Comparer	Extender	Project option	s User options	Alerts]	
	istory Web	Sockets hist	tory Options	I				I				
			optiono									
? Proxy Listeners												
Burp Proxy u	ses listeners	to receive in	coming HTTP re	equests from	your brows	er. You will r	need to conf	igure your brows	ser to use one of t	he listene	ers as its	
proxy server.												
Add	Running	Interface	Invisible	Redirect		Certificat	te					
		127.0.0.1:8	080			Per-host						
Edit	, —											
Remove												Ĩ.
		2	上公田						1 选中	这个	 	- 1
		<u> </u>	从这里						1.2217			- 1
Each installe	tion of Dura				. C			- 001				- 1
certificate for	use in other	tools or anot	own CA certification of the ce	ate that Proxy of Burp.	/ listeners (an use whe	n negotiatin	g SSL connecti	ons. You can impo	ont or exp	ort this	- 1
												- 1
Import / ex	port CA certi	ficate	legenerate CA c	ertificate								- 1
												-1
	lient Reg	lests										- 1
					1							- 1
Use these se	ettings to con	troi which ree	quests are stalle	a for viewing	and editing	In the interc	ept tab.					- 1
Intercept	requests bas	ed on the fol	llowing rules:									- 1
Add	Enabled	Operator	Match type	Relations	hip	Condition	n					
	v		File extension	Does not	match	(^gif\$ ^jp	g\$ ^png\$ ^cs	ss\$ ^js\$ ^ico\$)				
Eait		Or	Request	Contains	parameters	1						
Remove		Or	HTTP method	Does not	match	(get post	(get post)					
		And	UKL	Is in targe	et scope							
do												
											,	7 -

Edit proxy listener	×
Binding Request handling Certificate	
These settings control how Burp binds the proxy listener. Bind to port: 8082 Bind to address: O Loopback only All interfaces Specific address: 127.0.0.1	这里是代理用的端口 号,统一改成8082 好了
	改好之后点这里 OK Cancel

3. 开启浏览器的代理,刷新界面,可以看见出现下图的情况:

	5	Bur	p S	uite	Fre	ee Eo	dition v1.7	7.03 - Te	mporary l	Project					_	- [<
	Burj	p Int	trude	er Re	epea	ter V	Window Hel	р										
	Та	rget	P	оху	S	pider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	Alerts		
	Int	erce	pt	HTT	P hi	story	WebSock	kets history	/ Options									
		Re	ques	t to l	http:	//ctf4	.shiyanbar.c	:om:80 [1(06.2.25.8]		_							
		For	ward				Drop	Interce	pt is on	Action					Comment this	item		?
	Ra	w	Para	ams	H	eader	s Hex											
	GET Host User Accee Cook Cook Cook Cook	/we ::-Ag ::-Ag ::	b/I tf4 tent tent Enc Hm :-In Cont	OS/ .sh xt/: gua odi: p : c sec rol	indvi iyai ozi htm ge:: ng:: vt_: ure: : mo	ex.pmbar Ila/ Ila/ g	hp HTTP/: .com 5.0 (Wind plication CN,zh;q=(p, deflat f7353ab09 uests: 1 ge=0	l.1 hows NT h/xhtml+ l.8,zh-T ce 915a4c58 915a4c58	10.0; Win xml,appl: W;q=0.7,: 2e4516df;	n64; x64; n ication/xm. zh-HK;q=0.1 fbc3=150893	rv:58.0) 1;q=0.9,* 5,en-US;c 36072	Getko/201 7/*;0=0.8 =0.3, m;q	.00101 Fin =0.2 たの	zefox/58.0 这个, 久 repeat	然后点 er"	"se	end	
r.	?	JL	<	+		>	Type a sea	rch term									0 matc	hes:

4. 切换至repeater选项卡,将下图中user-agent部分进行修改

Surp Suite Free Edition v1.7.03 - Temporary Project			_		×
Burp Intruder Repeater Window Help					
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer	Extender Proj	ject options	User options	Alerts	
1 ×					
Go Cancel < v > v		Target:	http://ctf4.shiya	anbar.com	
Request	Response				
Raw Params Headers Hex	Raw				
<pre>GLI / WED/TOS/THDEX.php HTTP/T.T Host: ctf4.shiyanbar.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:58.0) Gecko/20100101 Firefox/58.0 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 Accept-Encoding: gzip, deflate Cookie: Hm_lpvt_34d6f7353ab0915a4c582e4516dffbc3=1508936072 Connection: close Upgrade-Insecure-Requests: 1 Cache-Control: max-age=0</pre>					
? + > Type a search term 0 matches	? < +	+ > Ty	/pe a search ter	m	0 matches
Ready					

5. 修改成下图对应位置的样子之后,点go,右半部分反馈得到flag:

⊱ Burp Suite Free Edition v1.7.03 - Temporary Project	- 🗆 X							
Burp Intruder Repeater Window Help								
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Compa	arer Extender Project options User options Alerts							
1 ×								
Go Cancel < v > v	Target: http://ctf4.shiyanbar.com 🖉 🕐							
Request	Response							
Raw Params Headers Hex	Raw Headers Hex HTML Render							
<pre>GET /web/IOS/index.php HTTP/1.1 Host: ctf4.shiyanbar.com User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 99 like Mac OS X) AppleWebKit/604.1.38 (KHTML, like Gecko) Mobile/15A402 Safari/604.1 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 Accept-Encoding: gzip, deflate Cookie: Hm_lpvt_34d6f7353ab0915a4c582e4516dffbc3=1508936072 Connection: close Upgrade-Insecure-Requests: 1 Cache-Control: max-age=0</pre>	HTTP/1.1 200 OK Server: nginx Date: Sat, 17 Mar 2018 06:57:53 GMT Content-Type: text/html Connection: close Vary: Accept-Encoding X-Powered-By: PHP/5.5.36 flag(LMvBi8w9\$mlTrgK4): Content-Length: 266 <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html> <html< td=""></html<></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html></html>							
? + > Type a search term 0 matches Done	<pre><!-- flag not in hERE--></pre>							

返回目录

2.3 第三题:照猫画虎

解题链接:	http://ctf4.shi	yanbar.com/web/co	p	y/index.php
-------	-----------------	-------------------	---	-------------

1. 打开链接出现如下界面

Lucky Visitor	
The 1234567890th visitor, the prize awarded.	You're 2699th Visitor

2. 根据最下面一排的提示,可以得知,要为第1234567890位用户才可以访问,尝试用burpsuite抓包

🐕 Burp Suite Free Edition v1.7.03 - Temporary Project – 🗆	\times
Burp Intruder Repeater Window Help	
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts	
Intercept HTTP history WebSockets history Options	
Request to http://ctf4.shiyanbar.com:80 [106.2.25.8]	
Forward Drop Intercept is on Action Comment this item	
Raw Params Headers Hex	
<pre>Sol / #E/COPYINGE.pap HIF/1.1 Host: cft3.bhyabar.com User-Agent: Motilla/5.0 (iPhone; CPU iPhone OS 99 like Mac OS X) AppleWebKit/604.1.38 (KHTML, like Gecko) Mobile/154ACC Safar1/604.1 Accept: text/html.application/xhtml+xml.application/xml;q=0.9,*/*;q=0.8 Accept-Encoding: gzip, deflate Cookie: Visitor=My190TowDDEIN2QeZWFhNGQ52GVjYmM42GEwMDFkM22kODA12g%3D%3D; Hm_lpvt_3def7353abd915AacSS2e4516dffbc3=1508936072 Connection: close Upgrade-Insecure-Requests: 1 Cache-Control: max-age=0 </pre>	
	0 matches

3. 可以发现在Cookie那一栏出现:

Visitor=MjY5OTowNDE1NzQwZWFhNGQ5ZGVjYmM4ZGEwMDFkM2ZkODA1Zg%3D%3D;

因为%3D%3D转换之后是==,则可以猜测Visitor=后面所跟的是经过base64加密的字符串,对字符串进行解码,得到 2699:0415740eaa4d9decbc8da001d3fd805f

其长度为32,刚好是2699的32位小写md5编码:

文字加密解密	MD5加密/解密	URL加密	JS加/解密	JS混淆加密压缩	ESCAPE加/	/解密 BASE6	4 散列/哈希	迅雷,快车	,旋风URL加解密
2699				●加密 ○ 32位[小] 加密	解密 ▼ 清空	0415740eaa4d9	decbc8da001d3fd80	5f	

4. 根据页面中出现的You're 2699th Visitor可得cookie中Visitor后的字符串格式为"base64(人数:md5(人数))",将 1234567890进行32位小写的md5加密,得到: e807f1fcf82d132f9bb018ca6738a19f 在该字符串前面加上1234567890:构成 1234567890: e807f1fcf82d132f9bb018ca6738a19f 进行base64编码,得到: MTIzNDU2Nzg5MDp10DA3ZjFmY2Y4MmQxMzJmOWJiMDE4Y2E2NzM4YTE5Zg== 将=转换为%3D后粘贴至repeater下Cookie部分的对应位置。点go,得到flag:



返回目录

2.4 第四题:问题就在这

题目描述: 找答案 GPG key: GhairfAvvewvukDetolicDer-OcNayd# 解题链接: http://ctf4.shiyanbar.com/ste/gpg/john.tar.gz.gpg

- 1. 点击链接后会下载一个文件,文件后缀名是gpg,使用工具https://gpg4win.org/download.html直接输入key解密出文件, 解压后发现是一个后缀名为pcap的数据包文件。
- 2. 利用 wireshark打开后,

🚄 john-in-the-middle.pcap				-		×
文件(E) 编辑(E) 视图(Y) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无	线(W) 工具(I) 帮助(H)					
▲ ■ 22 ❷ ▶ 目 22 ❷ ♀ ● 22 余 ● 22 余 ■ 44 44 44	12			र व	表达式…	+
No. Time Source Destination Protocol Length	1 Info					^
71 0.331603 192.30.252.154 192.30.252.154 HTTP 39 72 0.331650 192.30.252.154 192.30.252.154 HTTP 39	3 GET /js/countdown.js HTTP/1.1 0 GET /js/jquery.js HTTP/1.1					
73 0.331691 192.30.252.154 192.30.252.154 HTTP 39	7 GET /js/bootstrap.min.js HTTP/1.1					
75 0.331775 192.30.252.154 192.30.252.154 HTTP 43	5 GET /images/soonsor/reply_cv.png_HTTP/1.1	先点这里				
76 0.331957 192.30.252.154 192.30.252.154 HTTP 4832 77 0.331983 192.30.252.154 192.30.252.154 TCP 6	<pre>18 HTTP/1.1 200 OK (PNG) 16 39561 → 80 [ACK] Seq=1352 Ack=59458 Win=465536 Len=</pre>	0 TSval=7461089 TSecr=7461089				
78 0.331996 192.30.252.154 192.30.252.154 HTTP 4495 79 0.332015 192.30.252 154 192.30 252 154 TCP 6	7 HTTP/1.1 200 OK (PNG) 6 39565 → 80 [ACK] Seq=691 Ack=50148 Win=305664 Len=0	TSval=7461089 TSecr=7461089				
80 0.332111 192.30.252.154 192.30.252.154 HTTP 43	1 GET /images/sponsor/cini.png HTTP/1.1					~
> Frame 76: 48328 bytes on wire (386624 bits), 48328 bytes of > Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00), D	aptured (386624 bits) 0st: 00:00:00_00:00:00 (00:00:00:00:00:00)					î
> Internet Protocol Version 4, Src: 192.30.252.154, Dst: 192	2.30.252.154					
 Hypertext Transfer Protocol 	(1) Seq. 11150, Ack. 1552, Ech. 40202					
PNG Signature: 89504e470d0a1a0a						
 > Image Header (IHDR) > Background colour (bKGD) 						
> Physical pixel dimensions (pHYs)	一 五大牌上 注田					
> Image last-montrication time (time) > Image data chunk (IDAT)	冉伯键凤这里			• 0.5K/s	35,	
 Image data chunk (IDAT) Image data chunk (IDAT) 				2.3K/s		/
> Image data chunk (IDAT)						~
0160 0a 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44	PNGIHD					^
0180 36 cc 00 00 00 66 62 4b 47 44 00 ff 00 ff 00 ff 6.	bK GD					1
0130 a0 00 a1 93 00 00 00 93 70 48 39 73 00 00 00 13 01a0 00 00 b1 3 01 00 9a 9c 18 00 00 00 07 74 49 4d	tIM					
0160 45 07 df 04 14 0e 21 14 99 9c 8e c6 00 00 20 00 E. 01c0 49 44 41 54 78 da ec bd 79 90 5d d7 7d df 9f 9f 10	ATx y.].}					
01d0 9d 7b df 7b bd 61 07 09 90 58 b9 48 14 b5 50 9b . 01e0 ed 44 b2 1d 3a 55 46 3c 89 cb ca 44 ce ac 1e .D	.{.aX.HP. :UF <d< td=""><td></td><td></td><td></td><td></td><td></td></d<>					
01f0 25 51 99 aa 4a 3c 7f 64 e4 a9 a9 d2 4c 1c c7 a9 %Q 0200 a1 65 5b 8e 66 2a 1c 25 44 95 5d e3 51 26 bb 33 .e	J<.dL [.f*.% D.].Q&.3					
0210 49 34 63 c5 82 e4 88 89 1c 4d 32 71 22 c9 96 c4 14 0220 0d 20 08 82 24 08 f4 fa f6 bb 9c f3 9b 3f ce b9	с					
0230 ef dd d7 68 10 dd e8 6e a0 d1 38 5f d6 e5 7b e8	.hn8{.					~
● Z Portable Network Graphics (png), 47975 字节			分组: 126 · 已显示: 126 (100.0%) · 加载时间: 0:0	.9 配置文	て件: Def	aul t
右键选择"显示分组字节"						
Wiresbark · Portable Network Graphics (ppg)	iohn-in-the-middle				×	٦
	John in the initiale					d,
	r -					
	ſ					
頰 76, Fortable Network Graphics (png), 47,975 学节。						
解码为 无 ▼ 显示为 图像 ▼			开始 0 🚔 🗄	结束 479	75 🗘	
查找:				查找下一	个(N)	F
		AT CO.	復生 日 日			
		打印	夏制 Save as… Close	Hel	lp	
L	0103 94 70 01 01 07 0	ey 90 58 69 48 14 65 50 90		_	-	

3. 保存为png图片,用stegsolve打开,一个一个试就能得到flag了:



返回目录

2.5 第五题: 你最美~

题目链接: http://ctf4.shiyanbar.com/web/root/index.php 解题步骤:

1. 点击之后是一个123.exe用16进制的编辑器(网上随便找一个)打开:

			🦺 12	3.exe			
0	64617461	3A696D61	67652F70	6E673B62	d	ata:image/png;b 💼	
16	61736536	342C6956	424F5277	304B4767	a	se64,iVBORw0KGg	
32	6F414141	414E5355	68455567	41414152	0	AAAANSUhEUgAAAR	
48	67414141	45594341	49414141	41493748	g	AAAEYCAIAAAAI7H	
64	37624141	41465245	6C455156	52346E4F	7	bAAAFRElEQVR4n0	
80	33645557	34624F78	41415153	74343937	3	dUW4b0xAAQSt497	
96	2B796377	4D693447	754E5A36	32713379	+	ycwMi4GuNZ62q3y	
112	44796571	30475077	59685839	2F663331	D	yeq0GPwYkX9/f31	
128	2F412F2F	506E7078	38416667	4D685155		A//Pnpx8AfgMhQU	
144	42494542	41534249	51454153	46425145	В	IEBASBIQEASFBQE	
160	67514542	49452F6A	7638322B	7631476E	g	QEBIE/jv82+v1Gn	
176	754F3347	48516650	69393876	48303354	u	O3GHQfPi98∨H03T	
192	7538652F	6A384135	65386A53	584F6238	u	8e/j8A5e8jSXOb8	
208	4F4B4241	45685155	42494542	41534249	0	KBAEhQUBIEBASBI	
224	51454153	46425145	67514542	49455467	Q	EASFBQEgQEBIETg	
240	505A6779	58376169	63486645	742B3174	P:	ZgyX7aicHfEt+1t	
256	32627A78	382B6638	4B6E6636	4F735342	2	bzx8+f8Knf6OsSB	
272	41514567	53454241	45685155	42494542	A	QEgSEBAEhQUBIEB	
288	41534249	51454153	46423448	49676535	A	SBIQEASFB4HIge5	
304	44502F70	614D3669	5966342F	414F3779	D	P/paM6iYf4/A07y	
320	61682B5A	62625359	2F34526C	6D524943	a	h+ZbbSY/4RlmRIC	
336	416B4341	674A416B	4B43674A	41674943	A	kCAgJAkKCgJAgIC	
352	51494341	6B43516F	4A415035	44646238	Q	ICAkCQoJAP5Ddb8	
368	6D456439	4C644748	662F7248	59504B78	m	Ed9LdGHf/rHYPK×	
384	49456841	51424955	46415342	41514567	I	EhAQBIUFASBAQEg	
400	53454241	45685155	42494550	6A456757	S	EBAEhQUBIEPjEgW	
416	78753868	72576E4B	6C72776F	6F454153	X	u8hrWnKlrwooEAS	
Sign	Signed Int (select some data)						
	1784 out of 1898 bytes						

2. 药~是个base64的图片,上base64图片解码

以下是您的 Base64 代码所解码出来的图片,右键另存为保存图片.



3. 药~打开手机微信扫一下: you're beautiful~

返回目录

2.6 第六题: shellcode

解题链接: http://ctf4.shiyanbar.com/re/shellcode/shellcode.txt

1. 新弹出的界面只包含以下信息,熟悉注入的同学一看就很像shellcode:

\x6a\x0b\x58\x99\x52\x66\x68\x2d\x63\x89\xe7\x68\x2f\x73\x68\x00\x68\x2f\x62\x69\x6e\x89\xe3\x52\xe8\x34\x0



1. 药~丢进十六进制编辑器里面看看:

嗯,提取出内容:

ZmxhZ3tTSEVsbGNvZGVfSVNfc29fQ29vbH0K **真熟悉~**

2. 药~base64解码:

	将代码以	以BASE64方式加密、解密	
Base64₫	E线编码解码GB2312	Base64在线编码解码UTF-8	PHP加密/解密
	请输入	要进行编码或解码的字符:	
ZmxhZ3tTSEVsbG	NvZGVfSVNfc29fQ29vb	HOK	
	编码	¥码 🗌 解码结果以16进制显示	Z
	Ва	se64编码或解码结果:	
flag{SHEllcode_IS	so Cool}		

3. so~cool !

返回目录

转载于:https://www.cnblogs.com/blackay03/p/8590877.html