DROPS攻防平台部分writeup



1、比较大小

题目链接:

http://lab1.xseclab.com/base10_0b4e4866096913ac9c3a2272dde27215/index.php

	Challenge	23 Solves			3	×						
		۲ł	较大小									
	30 提示: F12还挺好用的											
<	只要比服务器	是的数字大就可以了	!									
	传送门:题目	链接										
	已解决!		确定									

先输入一个数字,发现只能输入三位数。然后想到修改源代码。

999	提交
-----	----

F12调出开发者工具修改"3",只要比3大就行,然后再在输入框中输入比999大的数字,点击提交,即可得到 key。

● 开发者工具 - lab1.xseclab.com/base10_0b4e4866096	913ac9c3a2272dde27215/ind	ex.php	o - http://l	ab1.xseclab.com/b	ase10_0b4e4		×
□ 🔓 😳 查看器 🖸 控制台 🕞 调试器 {}样式	編輯器 ④ 性能 《卟内存	<u> </u>	网络 😫	存储 🕘 HackB	ar 🛛 🔊 Adb	lock Plus	• •••
+	Q 搜索 HTML	ě	规则	计算值 布局	动画 字体		
<html> event</html>			♡过滤	样式		+	cls.
<pre>\thead></pre> Cody			▶ 伪元素	ŧ			
<pre>w<form action="" method="post"></form></pre>			此元素				
<pre><input maxlength="3" name="v" type="" 提交"=""/> bmit"></pre>		元素 中 { 内联 目					
<pre>> <div class="conter
none;" id="translate-man-app">:>:</div></pre> /div> event 	y:	<pre>(用户代理) quirk.css:196 input:not([type="image"]), textarea 中 { box-sizing: border-box; }</pre>					
		<pre>input:-moz-read-write, (用户代理) forms.css:224 textarea:-moz-read- write 中 { -moz-user-modify: read-write !important; }</pre>					
html > body > form > input			input -moz	} { -annearance: te	(用户代理) xtfield:	forms.c	ss:89 🗸

999999	提交
_	

2、nmap我用过

题目链接: http://www.zzti.edu.cn/

Challenge	26 Solves	×									
	nmap我用过										
提示: 主林	30										
渗透测试要了解可能开放的服务(flag是端口号没有空格)											
传送门:题目	销链接										

这个题目就是考察nmap的使用,用kali linux或windows系统的nmap工具扫描,输入扫描命令:nmap 202.196.32.7

稍等片刻即可得到开放的端口,flag就是所有端口写在一起,中间没有空格。



3、111

题目链接: http://120.24.86.145:8002/web2/

Challenge	24 Solves			×
		111		
		50		
web第一步	查看源码你会么	>		
传送门: 题	目链接			
已解决!			确定	

用F12打开开发者工具即可得到答案。

● 开发者工具 - BK-CTF-WEB2 - http://120.24.86.145:8002/web2/			X
□ □ 查看器 □ 控制台 □ 调试器 {}样式编辑器 ④ 性能 □ □ 内存	<u>=</u> 🛛	网络 😂 存储 🧶 HackBar 🚇 Adblock Plus	• •••
+ Q 搜索 HTML	ř	规则 计算值 布局 动画 字体	
<pre><!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> event</html></pre>		♥ 过滤样式 + ▶ 伪元素	داs آت
<pre>> <head></head></pre>		此元素	
<pre><!--flag KEY </pre--></pre>		元素	内联
<pre><script src="js/Snow.js" type="text/javascript"></script></pre>		<pre>body { margin: 0; padding: 0; position: relative; background-image: url(images/xh.jpg); background-position: center; background repeat: no repeat; width: 100%; height: 100%; </pre>	内联:2
html > body#body		<pre>background-size: 100% 100%; }</pre>	-

4、冒充登录用户

题目链接: http://lab1.xseclab.com/base9_ab629d778e3a29540dfd60f2e548a5eb/index.php

	Challenge	20 Solves										
		冒充登陆用户										
		70										
<	小明来到一个网站,还是想要key,但是却怎么逗登陆不了,你能帮他登陆 吗2											
	传送门:题目	链接										
	已解决!	确定										

您还没有登陆呢!

本题主要考察抓包工具 burpsuite的使用。



抓包后右键点击Send to Repeater,点击Repeater按钮,

Burp Intruder Repeater Window Help											
Target Proxy Spid	er Scanner	Intruder	Repeater	equencer	Decoder	Comparer	Extender	Project options	User options	Alerts	
Intercept HTTP histor	WebSocket	s history	Options								
Request to http://lab1.xseclab.com:80 [202.108.35.226]											
Forward Drop Intercept is on Actio											
Raw Params Headers Hex											
GET /base9_ab629d77	8e3a29540d:	fd60f2e54	18a5eb/in	dex.php H1	TT 1.1						
Host: labl.xseclab.	com										
User-Agent: Mozilla	/5.0 (Windo	ows NT 6.	1; Win64,	; x64; rv:	61.0 Ge	cko/20100	101 Firef	ox/61.0			
Accept: text/html,a	pplication,	/xhtml+xm	al,applica	ation/xml;	;q=0.9 \ */	*;q=0.8					
Accept-Language: zł	-CN, zh;q=0.	8, zh-TW;	q=0.7,zh	-HK;q=0.5,	en-US;qे≓	0.3,en;q=	0.2				
Referer: http://cti	.dropsec.xy	/z:8080/d	challenge								
Cookie: Login=0											
Connection: close											
Upgrade-Insecure-Re	quests: 1										
Cache-Control: max-	age=0										

看到下面的界面, Cookie: Login=0, 把"0"改成"1", 然后点击"go",即可得到key。





5、抓到就能改

题目链接: http://lab1.xseclab.com/base6_6082c908819e105c378eb93b6631c4d3/index.php

Challenge	Challenge 20 Solves											
	抓到就能改											
70												
据说信息安全 须通过HAHA 门,但是如何	的组最近出了一款新的浏览器,叫 浏览器才能答对。小明同学坚决不 可才能过这个需要安装HAHA浏览器	HAHA浏览器,有些题目必 要装HAHA浏览器,怕有后 才能过的题目呢?										
传送门:题目	链接											
已解决!		确定										

该题也是考察burpsuite工具的使用,修改User-Agent的参数值,根据题目提示,只用修改浏览器名称为 HAHA,然后点击go。就可得到答案。

只允许使用HAHA浏览器,请下载HAHA浏览器访问!

Target Proxy Spide	r Scanner I	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender P	roject options	User options	Alerts			
Intercept HTTP history	WebSockets	history	Options										
Request to http://lab1	.xseclab.com:80	[202.108	.35.250]										
Forward	Drop	Intercept	is on	Action							Co	mment this item	?
Raw Headers Hex													
GET /base6_6082c908	819e105c378e	b93b663	31c4d3/in	dex.php HT	TP/1.1								
User-Agent: Mozilla,	/5.0 (Window	SNTE	1. Win64	· v64 · rw-	EL OL Gec	ko/201001	.01 Firefox	/61.0					
Accept-Language: zh	-CN, zh;q=0.8	Do	nd to Spider an active sc	an	I=0	,q-0.8 .3,en;q=0	. 2						
Connection: close	.dropsec.xyz	Ser	nd to Intrude	r	Ctrl+I								
Upgrade-Insecure-Re Cache-Control: max-	quests: 1 age=0	Ser	nd to Repeat	er	Ctrl+R								
		Ser	nd to Compa	rer									
	Send to Decoder												
Request in browser send to sqlmap													
	Engagement tools												
		Cha	ange reques	t method									
		Cha	ange body e	ncoding									
Burp Intruder Repeater	Window Help		\sim										
Target Proxy Spid	er Scanner	Intruder	Repeater	Sequence	Decoder	Compare	r Extender	Project optio	ns User optio	ons Ale	erts]	
Intercept HTTP histor	y WebSocket	s history	Options										
Request to http://lab	1.xseclab.com:8	30 [202.10	08.35.250]										
Forward	Drop	Interce	pt is on	Action								Comment this item	
Raw Headers He	ĸ												
GET /base6_6082c900 Host: labl yseclab	8819e105c378	3eb93b6	631c4d3/:	index.php 1	HTTP/1.1								
User-Agent: Mozilla	a/5.0 (Windo	ws NT (6.1; Wine	54; x64; r	7:61.0) G	ecko/2010	00101 Fire:	fox/61.0					
Accept: text/ntml, Accept-Language: zl	h-CN, zh; q=0.	8,zh-T	хmi, аррі: W;q=0.7,	zh-HK;q=0.	5,en-US;q	=0.3,en;c	q=0.2						
Connection: close	f.dropsec.xy	/z:8080,	/challeng	ge									
Upgrade-Insecure-R Cache-Control: max	equests: 1 -age=0												
Target Proxy Spide		ntruder I	Reneater	Sequencer	Decoder	Comparer	Extender P	roject options	User ontions	Alerts	1		
	× 5 × 6	× 7 :	×))										_
Go Cancel	<	>								Targe	et: ht	ttp://lab1.xseclab.com	?
Request							Response			_			
Raw Headers Hex						_ _	Raw Head	ers Hex	HTML Render				_
Host: labl.xseclab.	10-105-055	ມສ30663	10402/111	uex php HT	18/1.1	A H	LIP/I.I 200	JUK					
User-Agent: Mozilla Gecko/20100101 HAHA	319e105c378e com		,		-	Se	erver: ngin	1X					^
A manufacture of the second se	319e105c378e com (5.0 (Window	s NT 6.	1; Win64	; x64; rv:	61.0)	Da Da	erver: ngin ate: Mon, 1 ontent-Type	nx 16 Jul 2018 e: text/htm	3 13:15:57 G al	MT			1
text/html,application	519e105c378e com 5.0 (Window on/xhtml+xml	s NT 6.	l; Win64	; x64; rv: 1;q=0.9,*/	61.0) *;q=0.8		erver: ngin ate: Mon, 1 ontent-Type onnection: ia: 1525	hx 16 Jul 2018 e: text/htm close	3 13:15:57 G al	FMT			1
<pre>text/html,applicatio Accept-Language: zh-CN,zh;q=0.8,zh-TW</pre>	319e105c378e com (5.0 (Window on/xhtml+xml	rs NT 6. .,applic K;q=0.5	l; Win64 ation/xm	; x64; rv: 1;q=0.9,*/ =0.3,en;q=	61.0) *;q=0.8 0.2	Se Da Ca Ca V: Ca	erver: ngin ate: Mon, 1 ontent-Type onnection: ia: 1525 ontent-Leng	nx 16 Jul 2018 e: text/htr close gth: 185	3 13:15:57 G Ml	GMT			4
<pre>Accept: text/html,applicatio Accept-Language: zh-CN,zh;q=0.8,zh-TU Referer: http://ctf. Connection: close</pre>	<pre>319e105c378e com (5.0 (Window on/xhtml+xml w;q=0.7,zh-H .dropsec.xyz</pre>	rs NT 6. .,applic K;q=0.5 ::8080/c	l; Win64 cation/xm 5,en-US;q challenge	; x64; rv: 1;q=0.9,*/ =0.3,en;q=	61.0) *;q=0.8 0.2		erver: ngin ate: Mon, 1 ontent-Type onnection: ia: 1525 ontent-Leng ntml> <heta< td=""><td>nx L6 Jul 2018 e: text/htm close gth: 185 ead></td><td>3 13:15:57 G ml</td><td>MT</td><td></td><th></th><td>4</td></heta<>	nx L6 Jul 2018 e: text/htm close gth: 185 ead>	3 13:15:57 G ml	MT			4
<pre>Accept: text/html,applicatio Accept-Language: zh-CN,zh;q=0.8,zh-TU Referer: http://ctf. Connection: close Upgrade-Insecure-Red Cache-Control: max-/</pre>	<pre>319e105c378e com (5.0 (Window on/xhtml+xml w;q=0.7,zh-H .dropsec.xyz quests: 1 aq==0</pre>	rs NT 6. .,applic K;q=0.5 ::8080/c	l; Win64 cation/xm 5,en-US;q challenge	; x64; rv: 1;q=0.9,*/ =0.3,en;q=	61.0) *;q=0.8 0.2		erver: ngin ate: Mon, J ontent-Type ia: 1525 ontent-Leng ntml> <het <met< td=""><td>nx 16 Jul 2018 2: text/htm close gth: 185 2: a http-eqn xt/html:ch/</td><td>3 13:15:57 G al liv="content arset=utf=8"</td><td>GMT -type" '></td><td></td><th></th><td>4</td></met<></het 	nx 16 Jul 2018 2: text/htm close gth: 185 2: a http-eqn xt/html:ch/	3 13:15:57 G al liv="content arset=utf=8"	GMT -type" '>			4
Accept: text/html,application Accept-Language: zh-CN,zh;q=0.8,zh-TT Referer: http://ctf. Connection: close Upgrade-Insecure-Rec Cache-Control: max-A	<pre>319e105c378e com com com com com com com com com com</pre>	rs NT 6. ,applic K;q=0.5 :8080/c	l; Win64 cation/xm 5,en-US;q challenge	; x64; rv: 1;q=0.9,*/ =0.3,en;q=	61.0) *;q=0.8 0.2		erver: ngi: ate: Mon, J ontent-Type onnection: ia: 1525 ontent-Leng html> <hei <hei <hei <hei <heid></heid></hei </hei </hei </hei 	nx Lé Jul 2014 e: text/htm close gth: 185 ead> ca http-equ ct/html;ch4	3 13:15:57 G al miv="content arset=utf-8"	SMT -type" '>			4
Accept. Lext/html,application Accept-Language: zh-CN,zh;q=0.8,zh-TT Referer: http://ctf Connection: close Upgrade-Insecure-Red Cache-Control: max-o	<pre>319e105c378e com com cs.0 (Window on/xhtml+xml W;q=0.7,zh-H .dropsec.xyz quests: 1 age=0</pre>	rs NT 6. ,applic K;q=0.5 :8080/c	l; Win64 cation/xm 5,en-US;q challenge	; x64; rv: 1;q=0.9,*/ =0.3,en;q=	61.0) *;q=0.8 0.2		erver: ngi ate: Mon, J onnent-Type onnection: ia: 1525 ontent-Leng html> <hd <hd <hd <hd> <hd <hd> <hd <hd> <hd <hd> <hd <hd> <hd></hd></hd></hd </hd></hd </hd></hd </hd></hd </hd></hd </hd </hd 	hx LG Jul 2016 e: text/htm close gth: 185 ead> ca http-equ ct/html;ch.	3 13:15:57 G al aiv="content arset=utf-8"	SMT S-type" '>			4
Accept: text/html,application Accept-Language: zh-CN,zh;q=0.8,zh-TT Referer: http://ctf. Connection: close Upgrade-Insecure-Rec Cache-Control: max-a	<pre>319e105c378e com com com com com com com com com com</pre>	rs NT 6. .,applic K;q=0.5 ::8080/c	l; Win64 cation/xm 5,en-US;q	; x64; rv: 1;q=0.9,*/ =0.3,en;q=	61.0) *;q=0.8 0.2		<pre>zver: ngii ate: Mon, J ontent-Typ onnection: ia: 1525 ontent-Leng html></pre>	1x 16 Jul 2016 2016 2017 2	3 13:15:57 G al uiv="content arset=utf-8"	-type"			4

6、misc1

18 Solves

misc1

100

一张图片

传送门:题目链接

改题目主要是考察工具WinHex的使用,将图片下载后,用WinHex打开,发现文件头没有错,再往下看,发现图 片大小不对,高度为0。

misc1.png																	
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	▲
00000000	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	44	52	%PNG IHDR ≡
00000016	00	00	02	D3	00	00	00	00	08	02	00	00	00	58	A3	66	Ó X£f
00000032	CĘ	ŲΟ	00	20	00	49	44	41	54	78	01	ED	DD	D9	СВ	7D	Î IDATx 1ÝÙË}
00000048	FØ	Бc	07	70	9E	नुसः	² 9A	8F	94	24	9C	98	22	D3	81	E1	ýÜ pžœš "\$œ~"Ó á
00000064	80	32	84	Α4	28	63	52	C4	8D	52	32	DD	86	42	86	42	€2"¤(cRÄ R2݆B†B
00000080	4E	24	43	51	52	A6	50	12	6E	43	71	60	28	37	8A	90	N\$CQR P nCq`(7Š
00000096	03	43	72	E0	C8	14	7F	80	E7	F3	3C	5F	BE	7D	5B	7в	CràÈ €çó<_¾}[{
00000112	5 F	FR	R3	7 F	7ח	F٦	FF	FD	FR	F۵	R9	5F	ਸ7	81	F7	RR	û° xõhíëú1 ∸ c≫

所以,修改高度和宽度一样大小,点击保存,再次打开就可以看到key。

flag{}}	

7 misc2

题目链接: http://123.207.139.209/ctf/misc2.txt

misc2

150

你需要py

传送门:题目链接

S01ZRENXU1NJVkhGUVZKUkpaRkZNMjNJSTVLVk1XU0xLV1ZYQV1LU050TkU0VExLS1pGRkdWQ1dKUkxHV01LWUtVWUhRVENXT1J0R1NVS1d0UkdGS01CVko1S0dXVkpRS1pDWFFUQ1R0U11FT1VUTE1STFZDTUxFSk5LV1 c2Q01LWV1EQ1RDWetWMkZNVjJWTkJKRk1SS09MQktHWVNTUEtKV0U0V1NUR0ZTRTZWTExNUkRWR01CUk10TEdXM1pSS01ZR01XQ1d0T11GRVVaUk9CQ0ZPU1NHS1ZJVENVU1BLV1dHWVJTVUdGTEZLVkNGR0ZKVk1SuzJJ UktGSzZDR0t0V1RLVENXR0ZSVEVVS1F0UkdGT1ZUTU1WSVRDVVNFSzVDWE1WMk50Tk5FNFZUS0pKTFZJMjJLSk5KR1dNS1RLTV1EU1RLUk50MkVRVjJXS1pLRktSTFVKTkxEQVZKUUtaV0U0VktTR0J0Rk1VU1VMSkxWSV JMWUpaS1dXVVNYS01ZRENRM1Z0T1dFN1ZDRk1STUUyTUxRS05KVEFNSzJLSV1HWVdDUkdGU0U2VkRNT1JEVkVWU1dNRktXV09LREtFWUZVVUNWT1JIRVFVW1JMSkZGTVJLT0taS1RDUVNNS1pXR01TQ1hLWkZGSVZTVk1S RF2JUksyS1JMR1dUU0hLSV1GVVMyV050V0ZHVkwySkpGRksyM1VJNUpVVVdTRUtJWUhJVDJXT1JKRV1WU0ZKWk1GRU1DMkt0TEVLV1NXS05XRU1UM1Z0T1NF1zCUkxKS1ZJVkxNSzVKVk1VU0VLWkxFNFJTVFBKTEVJVj JGT1JMVTIyW1ZKNUtHV05LR0paREZVVktUR0JZRVdWQ0dMSkZFMjJJS0pSS1dXTktMS01ZV01UU1RHRkpFWVZDV05SQ1ZLTUtTS1JLV1d0S1BKV1ZWTVVTV05KRkZRVTNNT0JHRkUyM1VLTktFTVZTTEtSV1hRU0NYS1JG RH0k5FV1ZTRk1aSEZHNINLS1TKVk0zQ01LNUxHSVTDVk50U0VPVkpRS1pKRk1WU1NKVk+HV1NTRk+KV1dTViTWR0ZTRTRVVExPUk1GTU1CWkpSSkVLNUNHSzVLV1VWU1dLVkhGT1ZETUpKRVZEV1NHS1pWV11TU05LT1ZW VVIyVUtaRkVZVkjRT1JRVkdNS1NJUktWTVRTTOtNWVhBVONTR0JXRk1VS1J0QkdGTzIyMkk1S1ZNV1NES1ZLV01WM1R0Uk5FVVZMTE90NFZHMONLS1ZKRENaQ1ZLVV1HUVRDVEtaV0VPV1NXS1Y0Vk1NQ1ZKNUxEQVdTSU V1NQS1JXRTRSU1VHRktYU1ZSUVBCR1ZHTUsySkpMR1c2Q1ZLSV1GVVMyV0dGU0ZRVkpRSEZHRk9WVE1LWkhFTVNTVUtaREVFUzJVSVZMRVVWVE1KSkpWSTNDS0pWTEZJU0xaSzVXR1VTMk9LVjJFUVYyV0tKS0ZFTURVSj VLRutXU1dLW1ZVNFdDVU5NWURBV1NWTVJMRTJNQ1JKVkpXV1ZTSEt0TEZVVEtYS1YyRVdVM01NUk5GTU1LT0pWS1RBM0MyS11ZR11WS1ZHRkpFUVVUTE9CREZPV1MySVJMREF0S1RLRV1WVVRDVutWMkZJVTNNSkpHRk1N TEVKNUpUQ1FTTEtaV0ZVVjJVS1pMRk1WU1FHVkZWRTIyMktKTEZJVFNPS1FZRVVTQ1N0TktYU1RKUktaR0ZJMjNVSVpLRk1XU1VLUkNYSVUyV05SVUZFVkxMT1JKVkdNTFFKNUpGTVpDWEtNWVZVVUNWT1JERk9WQ1ZHRk NGTTIZRU10S0VLV1NLS1VZVTRXQ1RHRkZGUVVTV0taS1UvM0NPSiVLR11aQ0hLUkxGVVMvVk5NWVZHVTIGTEpHRTIvU09MSkpVVVZTTUtKV1RDVkNWR0EvVV1WM0xPUk1WQ1ZTV1BGTEVLTktUS1VZR1VVU1dTWkpFMIUz ZNV1JSTEpLRkUyM01NRkpVS1dTSUpaV000VENUT1JGRVdWVExHQjVGQ01ETUpSSEZLNkNJS05MRVVSQ1d0TTJVN1ZKUUtaSUZNMjNRS0pKVENWVEJLS1ZUQTZLTk5SSEVXVjNMT1JFRk9WU09LUkpHvzVEQktaV0ZVVFNXtUQ1VOUk5GT1ZTV0pGNF2NVkxVTUZKR1dWuzJLW1ZVVVVTVUdGRkZFV1RMTVJIRkdNS09KSktXVzVDWEtSTEZFVkNVR0IyRTRWM1dMSkxGTU1DT0tSSkrBU1NZS0pWV11WU1ROUkZFN1VMTE1SRFZJN1NKUEZHV1cyW1JL T1dGVVRTV0dCNEdDVVpRT0JMVk1SU09LWkdXWVdTTUs1V1RLU1NXS1p0RTJWQ0ZIRkhVNFJTMkpCR1RBVFNNS05XR1VTM1NJVkhHQ1VKUkxKR0ZNV1RNSkJLVk1VU0VLWkNYSV1LV0dCTEZBV1RNS1pNRkczQ1pHQkxHV0 1LT0tGV0ZVUzJPS1Y0RUtVS1dNUktGR1ZMVU1GTEdZMkNRS1pWWE1WS1VOTTJWVVVVkhGTEZNUkxZS0JLR1VVU1dKV1ZUQ1RDV0dCWUVXVTJGTEpHRTRSS09NRkpUQzRDTktJWUdZVjJSR0ZIRV1WVEtKSkRGTVZTW1BG TEdXTktESOpW1VUU1Z0TkhFWVZDRkpKR0ZFUxNS1JLVEE2Q01LT1ZYUVNDWEtaTVhTV1RMTVJCVkkyM1dMQkxHVVRTTktJWUZVUktXTk5MRk9VM01KSkZGSzIzRUxCTEhVV1NFS1ZDWE1VM1JHRk5FNFZTRkpaTUZJM0 Vk1WU05QRkxEQU5LT0s1TEZVVFNXTk5ZRkVVW1JPQkVGRTJaWVBGR1RDMONLSzVW1FSU1VLWkhGSVZTVk9SUVZFUktXSVpLWFVTU1dLTkxGVVRLU0taTEZPV1NGR0ZGVkcyM1FLNUpWSVRTRUtNWUhBVjJVSVZORVVWS1 F001FWRzZIV0xCSkdZV1NVS1ZWVFNU01d0SkZFTVZLV0xKS1ZLVkxFSzVKREFXU0dLUktWRVVTVutWTkVXVVNWT1TNRktNTEVKUkxXWVdTWkt0TEZVVENWR0TTRUdVVExMSkxGTVZTT0xCS0ZNU1N0S1pWVTRUU1NTVkxF V1ZUTE9CTUZNTUxFS1JKREE0Q1hLW1ZWTVZTV050SEZLVVJRSkp0RkUyM0VLWkdUQU1LT0tWV1RDUjJUS1JFWFVWU1ZPQkxWRzNDU01KR1RBVExaS01ZV11XU1NHR1dGT1VaUkxKRUZFMjNRSVpLVk1WU1ZLUkNUU1EyU0 1WTkZEV1RNS1Y0VkdWU0tKVkpFS1JTUEtNWVZFVENTS1pXRk9WU1dLSkNGTVZMVUs1R1dXV1NLS1pLRTRUU1R0T11FUVVUTEdGSEZJUktXSk5IRs0Q1ZLRV1VTVZDVU1WMkdDV1JRTEpMRk0yU0tLWkpUQzRDTktKV1dZ VjJWT1JERVFWVExMSkxWRVZDS1BGR1dXNUNMS1JDV1VTU1dJWkhGQVVaUk1aTkZFV1NXS1JJVENUU1BLU1ZYSVdLVkdGSkVXVkxMT1JRVkVNQzJKSkdXVVRT0tOTEhBVENTTk1ZV1FWS1JLWkdGSzIyT0xGS1ZNVkxaS1 12 RetVM1 dLV k5 FTV ZUTFBCR1Z JTU tLSk5 MR1 daQ09 LUkRFTVMy T0 tWWUVPVkNXT0 JDRk9 STFVKWkxWTV dTV0 taS100V jJV11 JGRU tVVEx IRkxWQ01 LMkpCSkdXVFNIS1 JLRVM2U1NLV1 dFN1 vaUutaR0ZPM jJPTEpKV1 k0 and and and an antibal structure and antibal structure and an antibal structure and antibal structure antibal structure and antibal structure antibQ01LWktGRVYvVkdGSkVRVUxNTVTEVk1WU1dLUkxEQTVEQktNWVZLNkt0R0,TIRkFVM0tLWkdGRU1MTU1GSVRBMkNNS1ZWWFFSM1dLWkdYU1ZUTEdWSFUvMjNFSVTMRk1TU1RLUkNYQV,TU0tSRVhTVkpRSEZHVkcvM1FMRk

看到一堆乱码,做过这种类题的,知道这是一串base64编码。

推荐一个base64, base32, base16在线编码解码工具: http://www.qqxiuzi.cn/bianma/base64.htm 先进行base64解码,再把解码后的代码进行base32解码,就这样一直循环,知道最后得到flag。

Base64编码转换

TzIzVUk1S1RDVVNVS1ZLWE1UU1hLWk5GTVZMMkpKS0ZHV1MySVZKR11SU1hLT1dFTVQyUk50U0VPVQySkY1Rk1WTExHRktFS1dTT0tZWVU0V1NUROZXR1VV U1JOUkxVMjJaWkpKTEdXNkNIS1pMR1VWS1RHQ11HQ1VSUkxKR0ZLMjNVS1JKVk1XU05LSV1XSVZLVkdBNFVZVVRNTVJERk1WU05QRkxHV05LUEpaQ1ZNVENX S1YyRk1VW1FPQkNGRTIyV0t0S0VNV1NMS1pLWE1SU1RHR1NGSVZSUU9STEZPV1NWR0JMREFUU1ZLSV1GVVdTU0taSEZNV1NGR0ZGVk8yM11JNUtIVVRTRUtJ WUhBVjJUT1JTR1FWM0xKWk1WR01EUUpSSkZNV1MyS01ZV1VUM1V0SkZFT1VSUktaS1ZLM1pSS05LRktXU0tLUktWRVZTVE5SWUVXV1NGS1VZRkNNTE1KUkpX WVdTVktFWVZLNktVTk0yVkdWQ0ZLWk5GTTJTT0pWS1VLU1NGS0pWV01WM1ZQSkZFWVZMTFBCRUZNTUJSS1JMRUs1Q0hLW1dGVVRDVutWSEZPVkRNSkpFRk9S U09LWkdXWVdTUUtGV1dJVjJTS1VZVTJVU1ZPUkpWR01LU01STEVNVFNPS01ZVVVWM1dLUkpGT1RMTUtKRUZDVkNTS1pMVk1XU01LW1ZUU1UyVE50TkZBV1RM T1JLRkdNS0tKVkpHVzVDVktVWvdJVENUS1pXRU1VW1FHRktGTT1zVUtKTFZLVVNVS1pLVTRWU1NHQkNURVZLVUdBNFZBVkJRSFU9PT09PT0=

加密 解密 解密结果以16进制显示

KMYDCWSSIVHFQVJRJZFFM23II5KVMWSLKVVXAYKSNNNE4TLKJZFFGVCWJRLGWMKYKUYHQTCWNRNFSUKWNRGFKMBVJ5KGWVJQKZCXQTCTNRYEOUTLMRLVCMLE JNKWW6CIKYYDCTCXKV2FMV2VNBJFMRK0LBKGYSSPKJWE4VSTGFSE6VLLMRDVGMBRINLGW3ZRKMYGIWCWNNYFEUZROBCFORSGKVITCUSPKVWGYRSUGFLFKVCF GFJVIRS2IRKFK6CGKNVTKTCWGFRTEUJQNRGFOVTMIVITCUSEK5CXIV2NNNNE4VTKJJLVI22KJNJGWMKTKMYDSTKRNN2EQV2WJZKFKRLUJNLDAVJQKZWE4VKS GBNFIUSULJLVIRLYJZKWWUSXKIYDCQ2VNNWE6VCFMRME2MLQKNJTAMK2KIYGYWCRGFSE6VDMNRDVEVSWMFKWWOKDKEYFUUCVNRHEQUZRLJFFMRKOKZKTCQSM KZWGISCXKZFFIVSVMRDVIRK2JRLGWTSHKIYFUS2WNNWFGVL2JJFFK23UI5JXUWSEKIYHIT2WNRJEYVSFJZMFEMC2KNLEKVSWKNWEMT2VNNSEOVBRLJKVIVLM K5JVMUSEKZLE4RSTPJLEIV2FNRLU22ZVJ5KGWNKGJZDFUVKTGBYEWVCGLJFE22SKJRJWWNKLKIYWITSTGFJEYVCWNRCVKMKSJRKWWNKPJVVVMUSWNJFFQU3M OBGFE23UKNKFMVSIKRVXQSCKKRFETUIZQORQVMMCVGBIGW5CWKRWEUR2SNI4VMVTRWRHVK23YK5KFMSSNKZKXAUZTNRSFOTTI.IZMVGMDMI.ITEKTSSTWWFIT2U

Base编码系列: Base64 Base32 Base16

Base32编码解码

MFITA3CMKJWFURSWKZEXSVSVORQVIVTIKRLGYUSNKIYVUQ2WNNKXSTLKJJFV023UI5JTCUSUKVKXITSXKZNFMVL2JJKFGVS2IVJGYRSXKNWEMT2RNNSEOUT2 JF5FMVLLGFKEKWSOKYYU4VSTGFWFUURRNRLU22ZZJJLGW6CHKZLFUVKTGBYGCURRLJGFK23UJRJVMWSNKIYWIVKVGA4UYUTMMRDFMVSNPFLGWNKPJZCVMTCW KV2FMUZQOBCFE22WKNKEMVSLJZKXIRSTGFSFIVRQORLFOVSVGBLDATSVKIYFUWSSKZHFMVSFGFFV023YI5KHUTSEKIYHAV2TNRSFQV3LJZMVGMDQJRJFMVS2 KMYVUT2UNJFEOURRKZJVK2ZRKNKFKWSKKRKVEVSTNRYEWVSFJUYFCMLMJRJWYWSVKEYVK6KUNM2VGVCFKZNFM2S0JVKUKSSFKJVWIV2VPJFEYVLLPBEFMMBR JRLEK5CHKZWFUTCUKVHFOVDMJJEFORSOKZGWYWSQKFVWIV2SKUYU2USVORJVGMKSIRLEMTSOKMYUUV2WKRJFOTLMKJEFCVCSKZLVMWSMKZVTSU2TNNNFAVTL ORKFGMKKJVJGW5CVKUYWITCTKZWEMUZQGFKFM23UKJLVKUSUKZKU4VSSGBCTEVKUGA4VAVBQHU=====

编码 解码

S01ZRENXU1NJVkhGUVZKUkpaRkZNMJNJSTVLVk1XU0xLVIZYQVILU05OTkU0VExLSIpGRkdWQ1dKUkxHV01LWUtVWUhRVE NXTIJORINVS1dOUkdGS01CVko1S0dXVkpRS1pDWFFUQ1ROUIIFT1VUTE1STFZDTUxFSk5LV1c2Q0ILWVIEQ1RDWEtWMkZNVj JWTkJKRk1SS09MQktHWVNTUEtKV0U0VINUR0ZTRTZWTExNUkRWR01CUkIOTEdXM1pSS01ZR0IXQ1dOTIIGRVVaUk9CQ0ZP UINHS1ZJVENVU1BLVIdHWVJTVUdGTEZLVkNGR0ZKVkISU2JJUktGSzZDR0tOVIRLVENXR0ZSVEVVSIFOUkdGT1ZUTUIWSVRDV VNFSzVDWEIWMk5OTk5FNFZUS0pKTFZJMJJLSk5KR1dNS1RLTVIEU1RLUk5OMkVRVJJXSIpLRktSTFVKTkxHWTJDS0taV0U0Vkt VTIJGRU9VU1dOUkxWTVJMVUpSSIdXNkNYS0IZRENRMIZOTIdGT1UzTExKR0UyTUNPS0ZKVEFNSzJLSVIHWVdDUkdGU0VRVV RMTkJERkdWU1dNRktXV09LREtFWUZVVUNWTJJIRVFVWIJMSkZGTVJLT0taS1RDUVNNS1pXR0ITQ1hLWkZGSVZCUUdWSIZJU ksySIJMR1dUU0hLSVIGVVMyV05OV0ZHVkwySkpGRksyM1VJNUpVVVdTRUtJWUhJVDJXTIJKRVIWU0ZKWktGRU1DMktOTEVL VINXS05XRU1UU1ZOTINFT1UyV0xKS1ZJVkxUR0ZKV1dXU09LWVIVNFJTVFBKTEVJVIJSTIJMVTIyWIZKNUtHWVRR0tOTEZVVk NTtk00VUdVM01MSkVGSVZMWUtKSIdZV1NMS0IZV0IUU1RHRkpFWVZDV05SQ1ZLTUTSIJLV1dOS1BKVIZWTVVTV05KRkZR VTNNT0JHRkUyM1VLTktFTVZTTEtSVIhRUktSS1pORVdWS1ZPUIFWTU1DVkdCTEVJU1NXS1JXRVVSMINOTIdGTVZKUk1SSEZL MJNZSzVLRk1TU05LWktYQVUyVE5SU0ZRVFRMSIpNVkdNRE1MSkpFS1RTU0pWV0ZVVDJVTIJTRU1UVE1MSkNGRTJaUktOS0Z LVkxaS1JLWFFVU1RHQTJVV1ZTRkIaSEZHNINLSIJKVk0zQ0ILNUxHSVJDVk5OU0VPVkpRS1VaRk0yMINKWktHWVNTRktaVIZN VJJWR0ZTRTRVVEXPUk1GTU1CWkpSSkVLNUNHSzVLVIVWU1dLVkhGT1ZETUpKRVZFVINHS1pMV1ITU05LTIZWVVJVVU3VUtaRkVZ

		Base32编码解码	
	TJMNSX2===		
		编码解码	
flag(
Base编码系列: Base64	Base32 Base16		

8、密码学100

题目链接: https://pan.baidu.com/s/1pLQK1Ov



点击题目链接,下载后解压打开txt文件,发现是一串乱码,本题是一道密码题,因此可以想到密码的加密方式,根据题目提示,可以百度一下"凯撒"和"栅栏",发现是凯撒加密和栅栏加密的结合,先进行凯撒解密,再进行栅栏解密。在这里推荐两个在线加解密网站:

凯撒加解密: http://tool.bugku.com/jiemi/

栅栏加解密: http://www.qqxiuzi.cn/bianma/zhalanmima.php

▶ 软	(仁	D:)	学100		- - - 4	· 搜索 密码学100
I	.具(T) 帮助(H))			
Ť	JED	刻录	新建文件夹			
	^	名称	<u>^</u>	修改日期	类型	大小
		📄 Tiao T	iao.txt	2017/11/28 13:11	文本文档	1 KB
			TiaoTiao.txt - 记事本 文件(F) 编辑(E) 格式(O) 查看(aTMzgjzQvp_zb_Xm{11}	V) 帮助(H)		

将txt文件中的代码复制到下图的密文框中,选择凯撒密码,因为不知道位移数,所以可以点击列出所有组合, 经过以往做题经验,再经过仔细观察发现,位移-5或21位后的密文,同时存在"flag"这四个单词。说明即为经过 栅栏加密过的结果。

○ 栅栏密码 ④ 凯撒密码 ◎ 凯撒移位(中文版) ◎ 维吉尼亚密码 ◎ 摩斯电码 ○ 百度/Google/网页字符 ◎ MD5 ◎ 置换密码 ◎ 替代密码

清空拼音频率	去空格 每隔2	个字符 加空	格 横/竖	大写	小写	倒序	词倒序
		替抄	1. 计算	十进制	▼ > -	+六进制	▼ 转换

凯撒密码

在下面的文本框输入明文或密文, 点加密或解密, 文本框中即可出现所得结果

加密 解密 列出所有组合 征密文框:	立移数(-25~25):
aTMzgjzQvp_zb_Xm{11}	密文
bUNahkaRwq_ac_Yn{11}	
cVObilbSxr_bd_Zo{11}	
dWPcjmcTys_ce_Ap{11}	
eXQdkndUzt_df_Bq{11}	
fYReloeVau_eg_Cr{11}	根据做题经验,同时存在"flag"四个字母的为结果
gZSfmpfWbv_fh_Ds{11}	
hATgnqgXcw_gi_Et{11}	

然后将这个结果复制到下图中的上方输入框中,通过每组字数从2开始,往后试,最终得出,当每组数字为5时,就是flag。

栅栏密码加密解密

fYReloeVau_eg_Cr{11}	
每组字数 5 🔄 加密 解容	

9、贝斯家族

题目链接: https://pan.baidu.com/s/1hsamci4

Challenge	0 Solves	×
	贝斯家族 150	
想挑战贝斯家	家族36位64大将和一位16元帅团结的权威?你可以试试。	
传送门:题目	链接	
已解决!	确定	

根据题目提示:贝斯家族。可以得出该题为base加密。

推荐一个base在线加密解密的网站: http://www.qqxiuzi.cn/bianma/base.php

点击题目链接,下载解压后得到一个txt文件,文件比较大,建议用notepad++打开,发现是一长串数字加字母,可以想到是十六进制编码。

在这里推荐一个在线十六进制转文本字符串的网站: http://www.5ixuexiwang.com/str/from-hex.php

在线16进制到文本字符串的转换

输入16进制文本:

7468566B7047546C5A6156324A5961444E61523368685A455578566C704863476C5356465932566A4A3059575179 526C6454626B7071556C646F5746567465474668526D5258576B553556303157536A46564D6A457756544A4B526D 4E476246685762457049576B52424D574D786345645762457070566C5A7764315A475A44425A566B6C345657786B 57474A59556D395A61315A3354555A77566C64744F56646956842615756566B62316473576C646A534570585957 74614D315674637A465852315A485647317355315A36617A4257625442335A5555315231645962464E6952314A565 66A426B4E47497856586461526B3559556D78774D566B77566B7469526B707A56327861566D4A5961444E5A6131 704C5A455A5763564A735A4664C61315633566D7853516D564753586C5561325259596B645356466C73576B5A6 B4D566C3456323147614531566244525861326858566D314B57565673556C56575256704D566A4261595649785A48 52536258524F566C525757566455516D465A566D5249556C6877566D4A4861465A576258683354544677574756475 A4774534D4456485644466181315978576B5A5862476858596C686F56465A71526D466A4D5535315532786B56314 A77363466857567A4577566D733156315A725A464E5752336853566C5A52643039525054303D

转换后的文本:

Vm0wd2QyUXIVWGxWV0d4V1YwZDRWMVI3WkRSV01WbDNXa1JTVjAxV2JETIhhMUpUVmpBeFYySkVUbGhoT VVwVVZtcEJIRII5U2tWVWJHaG9UVIZ3VIZadGNFSmxSbGw1VTJ0V1ZXSkhhRzIVVmxaM1ZsWmFkR05GU214U2J HdzFWVEowVjFaWFNraGhSemxWVm14YU0xWnNXbUZrUjA1R1UyMTRVMkpIZHpGV1ZFb3dWakZhV0ZOcmFHa FNIbXhXVm0xNFIVMHhXbk5YYIVacIVqQTFSMVV5TVRSVk1rcEIaSHBHVjFaRmIzZFdha1poVjBaT2NtRkhhRk5sYIh oWFZtMHhORmxWTUhoWGJrNVIZbFZhY2xWcVFURINNVIY1VFZSU1ZrMXJjRWxhU0hCSFZqRmFSbUI6WkZkaG ExcG9WakJhVDJOdFJraGhSazVzWWxob1dGWnRNSGhPUm14V1RVaG9XR0pyTIZsWmJGWmhZMnhXY1ZGVVJ sTk5WbFkxVkZaU1UxWnJNWEpqUId4aFUwaENTRIpxUm1GU2JVbDZXa1prYUdFeGNHOVdha0poVkRKT2RGSnJh R2hTYXpWeIdXeG9iMWRHV25STINHaFBVbTE0VjFSVmFHOVhSMHB5VGxac1dtSkdXbWhaTW5oWFkxWkdWVk pzVGs1V2JGa3hWa1phVTFVeFduSk5XRXBxVWxkNGFGVXdhRU5UUmxweFVtMUdVMkpWYkRaWGExcHJZVW RGZUdOSE9WZGhhMHBvVmtSS1QyUkdTbkpoUjJoVFIYcFdlbGRYZUc5aU1XUkhWMjVTVGxOSGFGQIZiVEUwV mpGU12tRkhPVmhTTUhCNVZHeGFjMWR0U2tkWGJXaGFUVzVv0ZreFdrZFdWa3B6VkdzMVYySkdhM2hXYTFwa

将代码复制粘贴到上图文本中,可以看到转换后的文本,发现为base64编码,在 http://www.qqxiuzi.cn/bianma/base64.htm里解码得到下图

Base64编码转换

EZMVjFkR1NWTnNaR2xTTVVwSVYyeFdhMVF4VGxkVGJrNV1ZbGQ0V0Zwc1dsZE5NVnB4VW0xR1dsWXdNVFZXUnpWUFdWWk9SMU5zVWxwaVIx SjJWbXRhYzJOdFJrW1RiWFJPVmpGS05sWnRNSGhTTVZwV1RWWmthVkpGT1ZaV2JYaDNaR3hhZEUxV1phcG1SVFY2VjJOYWQyR1dTbkpqUld oWFVteGFhRmRXWkU5V01WSjFVMjEwVTJKRmNGbFhWbEpIWkRBMWMxcEdWbEppV1Zwd1ZGZDBZVk14VWxkWGJYUm9Za1Z3TUZwV1dt0VdiVX BaWVVkb1dsWldjSEpXYWtaM1VtczFXR1ZHVG1sU1Z6azBWbTB3ZUU1R1dYbFNiR1JVVjBkNGIxVXdaRk5YUmxwMVkwVktiRkpzV2xaVmJYa DNZa1pLZEZWcVJsZFdla1V3VmxSQmVGSX1Ua2RYYkdSVF1sWkZkMV14V21GaE1VbDRXa2hXVm1KWVVsU1VWRVpMVjBaYVIxZHRSbXR0V1RW WVdUQmFZVmRIU1hwVmJHaFZWbXh3TTFwWGVGZGtSMDVHVDFaa1YxWkZXbGhXY1hoVFZqRmFjMU51U2xkV1JscFhWVzEwVms1V1ZrZFNWR3h SV1ZRd09RPT0=

加密 解密 网络密结果以16进制显示

Vm0wd2QyUX1VWGxWV0d4V1YwZDRWMV13WkRSV01WbDNXa1JTVjAxV2JET1hhMUpUVmpBeFYySkVUbGhoTVVwVVZtcEJ1R115U2tWVWJHaG9 UV1Z3V1ZadGNFSmxSbGw1VTJ0V1ZXSkhhRz1VVmxaM1ZsWmFkR05GU214U2JHdzFWVEowVjFaWFNraGhSemxWVm14YU0xWnNXbUZrUjA1R1 UyMTRVMkpIZHpGV1ZFb3dWakZhV0Z0cmFHaFN1bXhXVm0xNF1VMHhXbk5YY1Vac1VqQTFSMVV5TVRSVk1rcE1aSHBHVjFaRm1zZFdha1poV jBaT2NtRkhhRk5sY1hoWFZtMHh0RmxWTUhoWGJrNV1ZbFZhY2xWcVFUR1NNV1Y1VFZSU1ZrMXJjRWxhU0hCSFZqRmFSbU16WkZkaGExcG9W akJhVDJ0dFJraGhSazVzWWxob1dGWnRNSGhPUm14V1RVaG9XR0pyT1ZsWmJGWmhZMnhXY1ZGVVJsTk5WbFkxVkZaU1UxWnJNWEpqU1d4aFU waENTR1pxUm1GU2JVbDZXa1prYUdFeGNH0Vdha0poVkRKT2RGSnJhR2hTYXpWe1dXeG9iMWRHV25ST1NHaFBVbTE0VjFSVmFH0VhSMHB5VG xac1dtSkdXbWhaTW5oWFkxWkdWVknzVGs1V2IGa3hWa1phVTFVeFduSk5XRXBxVWxkNGFGVXdhRU5UUmxweFVtMUdVMkpWYkRaWGExcH1ZV

Base编码系列:Base64 Base32 Base16

然后再将解密后的文本代码进行base64解密,就这样一直循环,直至最后得到flag。

Base64编码转换

ZmxhZ [°]	/GRfOWFtaWx5fQ==		
加密解密	■解密结果以16进制显示		
flag	· · ·)		

Base编码系列:Base64 Base32 Base16

10、文件上传比想象的难一点

题目链接: http://teamxlc.sinaapp.com/web5/21232f297a57a5a743894a0e4a801fc3/index.html

	Challenge	8 9	Solves				×
			文件上传比杰 5	見象的X 0	十二章	ī	
(文件上传 传送门:题目) 目链接					
	已解决!				确定		
解题	包路: 00社	載断、	路径构造				

解题方式:

1、上传任意php文件,使用burpsuite抓包,发送至Repeater后直接GO,页面提示需要上传图片文件;

文件上传

Filename: 浏览... 333.php Submit

Array ([0] => .php [1] => php) 不被允许的文件类型,仅支持上传jpg,gif,png后缀的文件

2、将filename构造为如下形式,使用00截断,仍提示需要上传图片文件;



["filen ["filename"]=> string(3) "333

</html>

br>00000flag000<@>flag:nctf

and the state of t

4、Go之后即可得到flag。

-----114782935826962--

Content-Disposition: form-data; name="submit

Submit

11、一道简单的ctf题目

题目链接: http://103.238.227.13:10085/

----114782935826962



1、根据题目要求先上传任意php文件,文件大小不超过1M,如下图。



2、点击Submit提交后,得到如下提示。

非图片文件

3、用burpsuite抓包,发送至Repeater,直接点击go,也提示非图片文件,观察Request中的信息,发现 Content-Type: application/octet-stream。

直接将其类型改为image/jpeg,再点击go即可得到flag。



12、签到题

题目链接: http://chinalover.sinaapp.com/web1/

key在哪里?

	← → ୯ ଝ	7
	另存页面为(P)	
	发送页面到设备(D)	•
	查看背景图像(W)	
	全选(<u>A</u>)	
	查看页面源代码(V)	
	查看页面信息(1)	
	查看元素(Q)	
ଷ	Search Shodan for current website	;
Т	用[Google 翻译]翻译此页面	

签到题就是简单,主要是考察查看源代码。直接点击题目链接,空白处右键点击查看页面源代码,即可得到 flag。

13、没有人的密码会这么简单

题目链接: http://lab1.xseclab.com/vcode1_bcfef7eacf7badc64aaf18844cdb1c46/index.php

登陆密码是4位纯数字数,	第一位不为0
User: admin	
Password: ••••	Show
Vcode: xf94	
X F 9 4	
submit	

根据提示,用木头超级字典生成器生成符合题目条件的字典,然后用burpsuite抓包,右键点击send to Intruder。设置payloads,将字典加载上去,点击start stack

POST /vcodel bcfef7eacf7badc64aaf18844cdblc46/login.php HTTP/1.1	
Host: labl.xseclab.com	
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0	
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://labl.xseclab.com/vcodel_bcfef7eacf7badc64aaf18844cdblc46/index.php	
Content-Type: application/x-www-form-urlencoded	
Content-Length: 48	
Cookie: PHPSESSID=9e53e7835b303031aa27db6d579fe7d5	
Connection: close	
Upgrade-Insecure-Requests: 1	
username=admin&pwd= <mark>\$1234\$</mark> &vrode=qsmn&submit=submit	

?	Payload Se	ets				
	You can defin	e one or more payl	oad sets. The	number of payloa	d sets d	epends on the attack type defined in the Positions tab. Various payload types are a
	Payload set:	1	•	Payload count:	9,000	
	Payload type:	Simple list	•	Request count:	9,000	
?	Payload O This payload t	ptions [Simple ype lets you config	list] ure a simple lis	st of strings that a	ire used	as payloads.
	Paste	1000				
		1001				
	Load	1002				
	Demons	1003				•
	Remove	1004				
	Clear	1005				
		1006			-	
		1007			V	
	Add	Enter a new item	1			
	Add from list	t		•		



🔁 Intruder attack 3									
Attack Sa	Attack Save Columns								
Results	Target Positio	ns Payloads (Options						
Filter: Shov	wing all items								?
Request	Pavload		Status	Error	Timeout	Longth	•	Comment	
239			200			321			*
20	1019		200			307			
27	1026		200			307			
31	1030		200			307			
32	1031		200			307			
50	1049		200			307			
54	1053		200			307			
60	1059		200			307			
63	1062		200			307			
83	1082		200			307			
95	1094		200			307			
102	1101		200			307			T
Request	Request Response								

可以看到length和其他的不一样的就是密码。输入密码后即可得到key。

key is !

14、我说的是真的

题目链接: http://chinalover.sinaapp.com/web8/



点击链接"__到这里找key_"

这里真的没有KEY,土土哥哥说的,土土哥哥从来不坑人, PS土土是闰土,不是谭神

按照出题人的套路,肯定不是这样的,所以先不要点击"_到这里找key_",首先右键点击空白处,选择查看页面 源代码。

```
1 <html>
2 <head>
3 <meta http-equiv="content-type" content="text/html;charset=utf-8">
4 </head>
5 <body>
6 <a href="../search_key.php">.到这里找key_</a>
7 </body>
8 </html>
```

发现一个链接,点击它,即可得到key。

```
1 <script>window.location="./no_key_is_here_forever.php"; </script>
2 key is :
```

15、你会改后缀吗

答案又是啥

题目链接: http://chinalover.sinaapp.com/web2/index.html



看到一个gif图片,查看源代码,没有什么发现。把gif图片下载下来,用notepad++打开,可以再文件末尾找到 flag。



16、本机登录

题目链接: http://39.107.92.230/web/web3/index.php



根据题目提示,用burpsuite抓包,send to Repeater 直接点击qo,友现只有本地地址才能	上能允许通过	发现只有本地地址才能允许	beater.直接点击do,	send to Re	psuite抓包,	示,用bur	根据题目提示
--	--------	--------------	----------------	------------	-----------	--------	--------



那么就在Request里加上一个条件X-Forwraded-For: 127.0.0.1,再点击go即可得到flag。



17、仔细看看源代码

题目链接: http://chinalover.sinaapp.com/web3/

🍯 Я	授者工具 - Sup	perSo by:p0t	t1 - http://	china	lover.sinaapp.	com/web3	/					8 - j	l		
	○ 查看器	□ 控制台	□ 调试器	{	} 样式编辑器	④ 性能	◎肉存	∋ 网络	8	存储	Hacke	Bar ≫			
	来源	大	纲		SO.html	so.js	iframe.js ×	>>	⊳	\triangleright \bigcirc	⊻ ⊉_⊉			۲	http://chinalover.sinaapp.com/web3/
- 3	chinalover.sir	aapp.com		1	'use strict'	;					TEAM				http://chinalover.sinaapp.com/web3/SO.html
	🗀 web3			2	(function(wi	n) {		_		沃加	ロド加またず				http://chinalover.sinaapp.com/web3/S0.html
▶ 63	blob://			4	(1011012011(112		/			70%04	4000 120-49-42-2-44			_	http://chinalover.sinaapp.com/web3/SO.htm
) ⊨ di	• 扩展			5	var exports	= {};				▼ 断点	(_	http://chinalover.sinaapp.com/web3/S0.htm
0	w.cnzz.com			7	(function(ex	ports) {				V 5	常处暂停				http://abinalover.sinaapp.com/web3/404.html
	Webpack			8	var utils	= {					2 忽略捕获的	的异常			http://www.lunzhiyu.com/#/home
0	webpack			10	normaliz	eUrl: func	tion(url) {				140-142				http://www.lunzhiyu.com/#/home
0	www.iunzniyi	1.com		11	return	this.hash	Url(url) r	ull:		₩ Vij/H	14年138				http://www.lunzhiyu.com/#/home
				13			V V H ·	-		▼ 范围					http://www.lunzhiyu.com/#/home
				14 15	35					▼Ξ坊	њ. 				

F12打开开发者工具,点击排列方式,发现有一个不正常的地址,点开查看源代码可以看到不一样的东西。

```
A:visited { color: maroon }
10 </STYLE>
11 </HEAD><BODY>
12 (center)
13 <TABLE width=500 border=0 cellspacing=10><TR><TD>
14 < !-- Placed at the end of the document so the pages load faster -->
15 <!--
16 <script src="./js/jquery-n. 7.2.min.js"></script>
17 <script src="./js/jquery-c. 7.2.min.js"></script>
18 <script src="./js/jquery-t. 7.2.min.js"></script>
19 <script src="./js/jquery-f.7.2.min.js"></script>
20 <script src="./js/jquery-{.7.2.min.js"></script>
21 <script src="./js/jquery-t.7.2.min.js"></script>
22 <script src="./js/jquery-h. 7.2.min.js"></script>
23 <script src="./js/jquery-i.7.2.min.js"></script>
24 <script src="./js/jquery-s. 7.2.min.js"></script>
25 <script src="./js/jquery-_. 7.2.min.js"></script>
26 <script src="./js/jquery-i.7.2.min.js"></script>
27 <script src="./js/jquery-s.7.2.min.js"></script>
28 <script src="./js/jquery-_. 7.2.min.js"></script>
29 <script src="./js/jquery-a.7.2.min.js"></script>
30 <script src="./js/jquery-_. 7.2.min.js"></script>
31 <script src="./js/jquery-f.7.2.min.js"></script>
32 <script src="./js/jquery-1.7.2.min.js"></script>
33 <script src="./js/jquery-4.7.2.min.js"></script>
34 <script src="./js/jquery-g. 7.2.min.js"></script>
35 <script src="./js/jquery-}.7.2.min.js"></script>
```

37

仔细观察即可得到flag。

18、/X00

题目链接: http://teamxlc.sinaapp.com/web4/f5a14f5e6e3453b78cd73899bad98d53/index.php

view-source:

```
if (isset ($_GET['nctf'])) {
    if (@ereg ("^[1-9]+$", $_GET['nctf']) === FALSE)
        echo ' 还须输入数字才行';
    else if (strpos ($_GET['nctf'], '#biubiubiu') !== FALSE)
        die('Fiag: `.$fiag);
    else
        echo ' 骚年, 继续努力吧啊~';
}
```

直接给了一个源码,php代码审计,可以看到两条重要语句,根据ereg()函数的%00截断漏洞,不懂的可以自行 百度。

构造URL: http://teamxlc.sinaapp.com/web4/f5a14f5e6e3453b78cd73899bad98d53/index.php? nctf=1%00%23biubiubiu

其中%23为#的url编码后的值。

在地址栏输入这个URL即可得到flag。

19、web4

题目链接: http://120.24.86.145:8002/web4/

Submit

根据提示,查看源码,如下图,可以看到有三句明显的url编码后的代码。



a=document.getElementById("password");if("undefined"!=typeof a){if("67d709b2b

p2=aa648cf6e87a7114f1"==a.value)return!0;alert("Error");a.focus();return!1}}document.getElementById("levelC

%35%34%61%61%32经过编码后的结果为54aa2,再根据eval(unescape(p1)+ unescape('%35%34%61%61%32'+p2));这条与语句,可以知道最后需要提交的数据为p1+54aa2+p2

即67d709b2b54aa2aa648cf6e87a7114f1,把其输入到输入框中,点击submit即可得到flag。

看看源代码?

a2aa648cf6e87a7114f1 Submit

		Submit
KEY{	}	

20、 web5

题目链接: http://120.24.86.145:8002/web5/





查看源码可以发现一长串括号,百度一下,得知是jother编码,用在线jother解码也行,或者F12打开控制台直接 将代码复制到输入框中,点击回车,即可得到flag。

注意flag格式,全部改成大写。

21, cookie

题目链接: http://chinalover.sinaapp.com/web10/index.php

点击题目链接,发现什么也没有。根据提示cookie,想到用burpsuite抓包。

```
GET /web10/index.php HTTP/1.1
Host: chinalover.sinaapp.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:61.0)
Gecko/20100101 Firefox/61.0
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://ctf.dropsec.xyz:8080/challenge
Cookie Login=0
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

send to Repeater后可以看到cookie是Login=0,把0改为1,然后点击go。即可在Response中看到flag。

Go Cancel < v > v	Target: http://chinalover.sinaapp.com				
Request	Response				
Raw Params Headers Hex	Raw Headers Hex				
GET /webl0/index.php HTTP/1.1	HTTP/1.1 200 OK				
Host: chinalover.sinaapp.com	Server: nginx				
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:61.0)	Date: Thu, 19 Jul 2018 06:10:52 GMT				
Gecko/20100101 Firefox/61.0	Content-Type: text/html				
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	Connection: close				
Accept-Language:	Via: 1527				
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	Content-Length: 43				
Referer: http://ctf.dropsec.xyz:8080/challenge					
Cookie: Login=1	flag:nctf{				
Connection: close					
Upgrade-Insecure-Requests: 1					
Cache-Control: max-age=0					

22、矛盾

题目链接: http://120.24.86.145:8002/get/index1.php



```
$num=$_GET['num'];
if(!is_numeric($num))
{
    echo $num;
if($num==1)
    echo 'flag{*********}';
}
```

根据题目提示,可以知道考察numeri()函数,构造url: http://120.24.86.145:8002/get/index1.php?num=1a即可 得到flag。

\$num=\$_GET['num'];
if(!is_numeric(\$num))
{
echo \$num;
if(\$num==1)
echo 'flag{*********}';
}
1aflag{

23、头有点大

题目链接: http://ctf5.shiyanbar.com/sHeader/

Tips	http	header
------	------	--------

Forbidden
You don't have permission to access / on this server.
Please make sure you have installed .net framework 9.9!
Make sure you are in the region of England ard browsing this site with Internet Explorer

根据页面提示,可以知道要用burpsuite抓包修改User-Agent和Accept-Language。修改后点击go即可得到key。

CVT (cHoodor / HTTD/1 1	
West / Sheader/ Milf/1.1	
Host: ctis.shiyanbar.com	<div id="tempiatemo_menu"></div>
User-Agent: Mozilla/5.0 (IE 9.0;.NET CLR 9.9 Win64; x64;	
rv:61.0) Gecko/20100101	
Accept:	http header
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-gb q=0.3, en; q=0.2	
Referer: http://ctf.dropsec.xyz:8080/challenge	<pre><div id="templatemo content wrapper"></div></pre>
Cookie: Hm lvt 34d6f7353ab0915a4c582e4516dffbc3=1531831966;	
Hm cv 34d6f7353ab0915a4c582e4516dffbc3=1*visitor*%E6%B8%B8%E5%A	<pre><div id="templatemo content"></div></pre>
B\$A2	-
Connection: close	<pre><div class="content_title_01">Forbidden</div></pre>
Upgrade-Insecure-Requests: 1	<div .<="" td=""></div>
Cache-Control: max-age=0	class="horizontal divider 01">
	<div class="cleaner"> </div>
	You don't have permission to access
	/ on this server.
	br> the key is:
	<pre><div class="cleaner"> </div></pre>