CG-CTF—WP (WEB[-])



<u>窝窝头_233</u> ● 于 2019-12-03 19:59:24 发布 ● 501 ☆ 收藏 3 分类专栏: <u>CTFwriteup</u> 文章标签: <u>ctf CG-CTF</u> 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u>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/hahaha233330/article/details/103374420</u> 版权



CTFwriteup 专栏收录该内容

20 篇文章 1 订阅 订阅专栏

CG-CTF-WEB

工具:

①Winhex:图片隐写工具,可通过搜索"ctf""CTF""key""flag"等关键字得到flag。
②在线工具HtmlEncode/BASE64转换:注意源代码里奇怪的字符串,可以尝试解码(分清类型)。
③BurpSuite:抓包工具,这个很好用。
④Wireshark:抓包工具。使用说明

WEB

• **1、签到题** 题目地址 直接F12查看源代码就可以得到flag。

key在哪里?

	● 查看器	▶ 控制台	□ 调试器	{} 样式编辑器	Ω 性能	① 内存	↑↓ 网络
Q捜	索 HTML						
<ht ▶ <</ht 	ml≻ head≻⋯≪/hea	id>					
_ ▼ <	body>						
	<a style="di
key在哪里?</td><th>splay:none"><td>nctf{</td><td>]</td><td>}</td>	nctf{]	}			
│ <, <td>/body> tml></td> <th></th> <td></td> <td></td> <td></td> <td></td> <td></td>	/body> tml>						

• 2、md5 collision

题目地址

先简单学习一下md5()加密解密。 再来看题。题目中的collision是冲突的意思,猜测可能是前后条件矛盾。

源码 (PHP)

https://blog.csdp.pet/bababa233330

只有当 \$a != 'QNKCDZO' && \$md51 == \$md52 的时候才会回写flag。但是这是矛盾的。

这个题目利用了**php弱类型**。比如在==判等时,0exxxx=0xsfdsf=0。而在源代码中给出的 'QNKCDZO' 的md5就是0e开头,使用a传输一个md5也是以0e开头的即可。

***参考: PHP Hash比较存在缺陷,影响大量Web网站登录认证、忘记密码等关键业务

'QNKCDZO' 经过 md5() 解密后是'0e830400451993494058024219903391'。

```
<?php
$str = "QNKCDZO";
echo md5($str);
?>
```

1	php</th
2	<pre>\$str = "QNKCDZO";</pre>
3	<pre>echo md5(\$str);</pre>
4	?>

0e830400451993494058024219903391

构造a=s155964671a(这里用所有0e开头的md5小节都可以),得到flag。



注: 0e开头的MD5小节

0e545993274517709034328855841020: s155964671a 0e342768416822451524974117254469: s214587387a 0e848240448830537924465865611904: s214587387a 0e848240448830537924465865611904: s878926199a 0e545993274517709034328855841020: s1091221200a 0e940624217856561557816327384675: s1885207154a 0e509367213418206700842008763514: s1502113478a 0e861580163291561247404381396064: s1885207154a 0e509367213418206700842008763514: s1836677006a 0e481036490867661113260034900752: s155964671a 0e342768416822451524974117254469; s1184209335a 0e072485820392773389523109082030: s1665632922a 0e731198061491163073197128363787: s1502113478a 0e861580163291561247404381396064: s1836677006a 0e481036490867661113260034900752: s1091221200a 0e940624217856561557816327384675: s155964671a 0e342768416822451524974117254469: s1502113478a 0e861580163291561247404381396064: s155964671a 0e342768416822451524974117254469: s1665632922a 0e731198061491163073197128363787: s155964671a 0e342768416822451524974117254469: s1091221200a 0e940624217856561557816327384675: s1836677006a 0e481036490867661113260034900752: s1885207154a 0e509367213418206700842008763514: s532378020a 0e220463095855511507588041205815: s878926199a 0e545993274517709034328855841020: s1091221200a 0e940624217856561557816327384675: s214587387a 0e848240448830537924465865611904: s1502113478a 0e861580163291561247404381396064: s1091221200a 0e940624217856561557816327384675: s1665632922a 0e731198061491163073197128363787: s1885207154a 0e509367213418206700842008763514: s1836677006a 0e481036490867661113260034900752: s1665632922a 0e731198061491163073197128363787: s878926199a 0e545993274517709034328855841020: s878926199a

3、签到2
 题目地址

既然提示了请输入口令zhimakaimen,输入试试,发现无法"开门"。F12查看源码,发现一行定义输入长度的代码,设定的最大 值是10,数一数"zhimakaimen"一共有11位。原来如此!双击这行代码修改为11。再次输入口令,开门,即可得到flag。

尚未登录或口令错误



	● 查看器	▶ 控制台	□ 调试器	{}样式编辑器	Ω 性能	① 内存
Q捜	溹 HTML					
▶ < ▼ <	head>⋯ body> 尚未登录或口 ^{<} <form action<="" td=""><th>d> 令错误 ="./index.ph</th><th>p" method="p</th><td>ost"></td><th></th><th></th></form>	d> 令错误 = "./index.ph	p" method="p	ost">		
	输入框: <input p="" ty<=""/> <input p="" ty<=""/>	ype="password 令: zhimakaim ype="submit"	d" value="" r en value="开门"	name="text1" maxl	.ength= <mark>"10"</mark>	2
<	/body>					

flag is: 输入框: 请输入口令: zhimakaimen 开门

4、这题不是WEB:
 题目地址

真的,你要相信我!这题不是WEB

这题的确不是web,算misc...

解压下来是个图片。用winhex打开该图片,左上角菜单栏选择Search,选择Find Text(查找文本),输入搜索"ctf" "CTF" "key" "flag"等关键字即可得到flag。

*提示:快捷键:ctrl+F。

HEX WinHex - [2.gif]								
File Edit Search Navigatio	n View Tools	Specialis	t Optior	ns Window	Help			19.8 -
Case Data	🗅 🖊 🖬 😂 📚	🗊 📑 👘 🗠		B 012 A	$\underset{Hex}{\overset{\bullet}{\longrightarrow}} \overset{\bullet}{\longrightarrow} \overset{\bullet}{\to} \overset{\bullet}{\longrightarrow} \overset{\bullet}{\longrightarrow} \overset{\bullet}{\longrightarrow} \overset{\bullet}{\longrightarrow} \overset{\bullet}{\to} \overset$	ا 🕫 🗢 📾 🍐 ک	🏶 🛛 🕄 🖬 🖌 🕨	9
File Edit	2.gif							
	Offset	0 1	234	5 6 7	8 9 10 11 12 13	14 15 Al	NSI ASCII 🔥	Iupregie
	00000000	47 49 4	6 38 39	61 78 00	78 00 E6 7E 00 E4	DE D9 GIF89ax	x æ~ äÞÙ	2 gif
	00000016	FF FF F	F A4 9C	95 48 2C	22 53 4C 4D 8B 7B	83 Сб <u>ÿÿÿ</u> ¤œ∙Н	,"SIM< {fÆ	C:\Llcorc\iiaz
	00000032	BB B7 D	9 D3 CD	99 99 99	69 52 4E E6 E4 E3	ED EC »·ÙÓÍ™™	™iRNæäãíì	C.\Usersylaz
	00000048	EB B3 A	B A8 8A	84 87 C8	B5 A9 85 79 7A 95	8A 88 ë ³ «"Š"‡]	Èμ©…yz∙Š^	File size: 4
	00000064	32 26 2	E AB A5	A4 A9 A1	99 AD 89 76 E7 E3	DE D7 2&.«¥¤©	i™-‰VÇãÞ×	41.838
	00000080	C6 B9 C	B C4 BC	7B 74 77	C7 AB 97 DC D6 D3	CE C7 ƹËļ{t	wÇ«—ÜÖÓÎÇ	11,050
	00000096	C2 EB E	7 E4 A6	95 8C C6	94 8F 5E 47 38 93	84 7A Âëç䦕Œ	Æ″ ^G8""z	Default Edit
	00000112	D2 CB C	5 AD 73	73 D5 CE	CA 8E 6A 51 D3 BB	A8 B9 ÒËÅ-ssõ	ÎÊŽjQÓ»¨¹	State: 0
	00000128	A6 9B 7	6 68 67	B6 97 86	BD B6 B3 ED EB E6	DF DB ;>vhg¶-	t½¶°íëæßÛ	
	00000144	D6 07 0	3 14 9B	92 8C 52	3A 3F 76 61 58 A6	9E A0 Ö >'Œ	R:?vaX¦ž	Undo level:
	00000160	B9 B2 A	D 94 8D	92 DF DC	DB 90 51 51 C6 A5	8D 87 12-" 'ß	ÜÛ QQÆ¥ ‡	Undo reverse
	00000176	73 6C C	3 AC A2	6D 59 61	CD B1 9B 2B 1C 25	77 6C slÃ-¢mY	aͱ>+ %wl	C
	00000192	71 83 6	A 64 15	12 21 B6	9A 97 F3 EE EC 94	7B 75 qfjd !	¶š−óîì″{u	Creation
	00000208	66 66 6	6 97 79	67 D2 BD	B6 A4 8C 81 90 55	66 D3 fff-ygò	≰¶¤Œ UfÓ	
	00000224	C6 C3 B	8 86 85	D2 B6 9F	E4 DF E0 86 6A 77	DB CF #Ã tÒ¶	Ÿäßà†jwÛÏ	Last write 19

See State of the second second

	🏭 文件(I	F) 编辑	(E)	搜索	<u>इ</u> (S)	导航(N)	查看(V)	工具(T)	专业工具(I)
1	案件数据			#	查抄	戈文本(T)			Ctrl+F
	文件(L)	编辑(D	Inł	HE×	查抄	戈十六进制	数值(H)	Ctr	I+Alt+X
				¢.≱	替換	奂文本(X)			Ctrl+H
			0	Å ₽ HE×	替換	奂十六进制	数值(V)	. Ctr	I+Alt+H
			0		细名				
					211				
					整数	效数值(l)			
					浮点	点数值(F)			
			o		Ϋ́Ζ	≿段落(P)	_		
			0			F4×/H(- /-			
			0		继续	卖全局搜索	ξ(G)		F4
			0		继续	卖搜索(S)			haha23 53 30
			0 1						

查找文本 ×	
需要搜索的文本(s):	
flag ~	
 ✓ 匹配大小写 ASCII/Code page ~ 用作通配符(U): 搜索完整语句(y) 	
 搜索(e): 全部 条件:偏移计算 512 = 0 只在选块中搜索 	

	······ 开窗口中搜索(w)
3 列出搜索	结果,最多	10000
MA 确定(O)	取消(A)	

• 5、层层递进:

题目地址

打开链接发现是个网页。用F12查看器发现什么都看不出来。Ctrl+U 查看页面源代码试试。



发现里面还嵌套了一个网页,再点进去。



发现仍然有嵌套,再点。经过好几层SO.html的嵌套,终于发现了一个全新的网页。

39 </style> 40 link href="css/animate.min.css" rel="stylesheet" type="text/css"></link> $41 \langle /head \rangle$ 42 **<body>** 43 <body style="overflow:auto" 44 <iframe runat="server" src+"404.html" width="100%" height="3" frameborder="no" 45 <iframe runat="server" src="http://www.lunzhiyu.com" width="100%" height="3800"

打开网页,F12仔细观察其中代码,终于得到flag。

```
14 <!-- Placed at the end of the document so the pages load faster -->
15 <!--
16 <script src="./js/jquery-17.2.min.js"></script>
```

17	<script< th=""><th>src="./js/jquery-</th><th>7.2.min.js"></th></script<>	src="./js/jquery-	7.2.min.js">
18	<script< th=""><th>src="./js/jquery-</th><th>7.2.min.js"></th></script<>	src="./js/jquery-	7.2.min.js">
19	<script< th=""><th>src="./js/jquery-</th><th>7.2.min.js"></th></script<>	src="./js/jquery-	7.2.min.js">
20	<script< th=""><th>src="./js/jquery-</th><th>7.2.min.js"></th></script<>	src="./js/jquery-	7.2.min.js">
21	<script< th=""><th>src="./js/jquery-</th><th>7.2.min.js"></th></script<>	src="./js/jquery-	7.2.min.js">
22	<script< th=""><th>src="./js/jquery-</th><th>7.2.min.js"></th></script<>	src="./js/jquery-	7.2.min.js">
23	<script< th=""><th>src="./js/jquery-</th><th>7.2.min.js"></th></script<>	src="./js/jquery-	7.2.min.js">
24	<script< th=""><th>src="./js/jquery-</th><th>7.2.min.js"></th></script<>	src="./js/jquery-	7.2.min.js">
25	<script< th=""><th>src="./js/jquery-</th><th>.7.2.min.js"></th></script<>	src="./js/jquery-	.7.2.min.js">
26	<script< th=""><th>src="./js/jquery-</th><th>7.2.min.js"></th></script<>	src="./js/jquery-	7.2.min.js">
27	<script< th=""><th>src="./js/jquery-</th><th>7.2.min.js"></th></script<>	src="./js/jquery-	7.2.min.js">
28	<script< th=""><th>src="./js/jquery-</th><th>7.2.min.js"></th></script<>	src="./js/jquery-	7.2.min.js">
29	<script< th=""><th>src="./js/jquery-</th><th>7.2.min.js"></th></script<>	src="./js/jquery-	7.2.min.js">
30	<script< th=""><th>src="./js/jquery-</th><th>7.2.min.js"></th></script<>	src="./js/jquery-	7.2.min.js">
31	<script< th=""><th>src="./js/jquery-</th><th>7.2.min.js"></th></script<>	src="./js/jquery-	7.2.min.js">
32	<script< th=""><th>src="./js/jquery-</th><th>.7.2.min.js"></th></script<>	src="./js/jquery-	.7.2.min.js">
33	<script< th=""><th><pre>src="./js/jquery-</pre></th><th>.7.2.min.js"></th></script<>	<pre>src="./js/jquery-</pre>	.7.2.min.js">
34	<script< th=""><th><pre>src="./js/jquery-</pre></th><th><mark>r.</mark>7.2.min.js"></th></script<>	<pre>src="./js/jquery-</pre>	<mark>r.</mark> 7.2.min.js">
35	<script< th=""><th><pre>src="./js/jquery-</pre></th><th>.7.2.min.js"></th></script<>	<pre>src="./js/jquery-</pre>	.7.2.min.js">
36	>		https://blog.csdn.net/hahaha233330

• 6、AAencode

题目地址 javascript aaencode

在chrome中打开,发现中文乱码。这是由于还没有安装解码插件。

	homura.cc/CGfiles/aaencode. ×	👽 插件市场	+	-	٥	×
Y	< > C 凸 5 ☆ @	homura.cc/CGfiles/aaencode.txt	🖡 📩 🗸 🖌 🕒 Google	Q	012	Ξ
🔷 PanD	ownload网页版					
	and the second sec	() and all the set of			In the crit	

去扩展程序里下载Charset插件(修改网站的默认编码),将编码格式改为UTF-8。

扩展程序

开发者模式

加载已解压的扩展程序... 打包扩展程序...

立即更新扩展程序





这串字符串就会变成这样。

w /- / III / / - $(\circ \hat{\ } \circ); (\circ \Pi \circ) = \{\circ \Theta \circ : \hat{\ } , \circ \omega \circ / : ((\circ \omega \circ / = 3) + \hat{\ }) [\circ \Theta \circ] , \circ - \hat{\ } / : (\circ \omega \circ / + \hat{\ }) [\circ \hat{\ } \circ - (\circ \Theta \circ)] , \circ \Pi \circ / : ((\circ - \hat{\ } \circ) + \hat{\ }) [\circ \hat{\ } \circ - (\circ \Theta \circ)] , \circ \Pi \circ / : (\circ - \hat{\ })]$ $==3) + '_{-})[\circ -\circ]]; (\circ \pi \circ) [\circ \Theta \circ] = ((\circ \omega \circ /==3) + '_{-}) [\circ -\circ]; (\circ \pi \circ) [' \circ c'] = ((\circ \pi \circ) + '_{-}) [(\circ -\circ) + (\circ -\circ) - (\circ \Theta \circ)]$ $]; (^{\circ} \Pi^{\circ}) [' \circ'] = ((^{\circ} \Pi^{\circ}) + '_{}) [^{\circ} \Theta^{\circ}]; (^{\circ} \circ) = (^{\circ} \Pi^{\circ}) [' \circ'] + (^{\circ} \Pi^{\circ}) [' \circ'] + (^{\circ} \omega^{\circ} / + '_{}) [^{\circ} \Theta^{\circ}] + ((^{\circ} \omega^{\circ} / ==3) + '_{}) [^{\circ} \Theta^{\circ}] + ((^{\circ} \omega^{\circ} / ==3) + '_{}) [^{\circ} \Theta^{\circ}] + ((^{\circ} \omega^{\circ} / ==3) + '_{}) [^{\circ} \Theta^{\circ}] + ((^{\circ} \omega^{\circ} / ==3) + '_{}) [^{\circ} \Theta^{\circ}] + ((^{\circ} \omega^{\circ} / ==3) + '_{}) [^{\circ} \Theta^{\circ}] + ((^{\circ} \omega^{\circ} / ==3) + '_{}) [^{\circ} \Theta^{\circ}] + ((^{\circ} \omega^{\circ} / ==3) + '_{}) [^{\circ} \Theta^{\circ}] + ((^{\circ} \omega^{\circ} / ==3) + '_{}) [^{\circ} \Theta^{\circ}] + ((^{\circ} \omega^{\circ} / ==3) + '_{}) [^{\circ} \Theta^{\circ}] + ((^{\circ} \omega^{\circ} / ==3) + '_{}) [^{\circ} \Theta^{\circ}] + ((^{\circ} \omega^{\circ} / ==3) + '_{}) [^{\circ} \Theta^{\circ}] + ((^{\circ} \omega^{\circ} / ==3) + (^{\circ} (\otimes ((^{\circ} - (^{\circ}) + (^{\circ} (\otimes (^{\circ} / ==3) + (^{\circ} (\otimes (^{\circ}) + (^{\circ} (\otimes (^{\circ} / ==3) + (^{\circ} (\otimes (^{\circ} / =3) + (^{\circ} (\otimes (^{\circ} /$ $-^{\circ}] + ((^{\circ} \square^{\circ}) + '_{-}') [(^{\circ} -^{\circ}) + (^{\circ} -^{\circ})] + ((^{\circ} -^{\circ} ==3) + '_{-}') [^{\circ} \Theta^{\circ}] + ((^{\circ} -^{\circ} ==3) + '_{-}') [(^{\circ} -^{\circ}) - (^{\circ} \Theta^{\circ})] + (^{\circ} \square^{\circ}) ['_{c}'] + ((^{\circ} -^{\circ} ==3) + '_{-}') [^{\circ} \Theta^{\circ}] + (^{\circ} \square^{\circ}) [^{\circ} \Theta^{\circ}] + (^{\circ} \square^{\circ}) [^{\circ} \Theta^{\circ}] + (^{\circ} \square^{\circ}) [^{\circ} \square^{\circ}] + (^{\circ} \square^{\circ}) [^{\circ} \square^{\circ}) + (^{\circ} \square^{\circ}) [^{\circ} \square^{\circ})] + (^{\circ} \square^{\circ}) [^{\circ} \square^{\circ}) [^{\circ} \square^{\circ}) + (^{\circ} \square^{\circ}) [^{\circ} \square^{\circ}) + (^{\circ} \square^{\circ})] + (^{\circ} \square^{\circ}) [^{\circ} \square^{\circ}) [^{\circ} \square^{\circ})] + (^{\circ} \square^{\circ}) [^{\circ} \square^{\circ}) [^{\circ} \square^{\circ}) + (^{\circ} \square^{\circ})] + (^{\circ} \square^{\circ}) [^{\circ} \square^{\circ}) [^{\circ} \square^{\circ})] + (^{\circ} \square^{\circ}) [^{\circ} \square^{\circ}) [^{\circ} \square^{\circ}$ $\begin{array}{c} \Pi_{0}^{\circ} + \Gamma_{0}^{\circ} \\ \Pi_{1}^{\circ} \\ \Pi_{1}^{\circ}$ $==3) + '_{,}) [\circ \Theta^{\circ}] + (\circ \Pi^{\circ}) \cdot \Pi^{\circ} / + ((\circ \Pi^{\circ}) + '_{,}) [(\circ^{-\circ}) + (\circ^{-\circ})] + ((\circ^{-\circ} ==3) + '_{,}) [\circ^{-\circ} \Theta^{\circ}] + ((\circ^{-\circ} ==3) + '_{,})$ $(\circ - \circ) + (\circ - \circ) + (\circ$ $\texttt{P}^{\circ}(\texttt{P}^{\circ}(\texttt{P}^{\circ}) + \texttt{P}^{\circ}(\texttt{P}^{\circ})) + \texttt{P}^{\circ}(\texttt{P}^{\circ}) + \texttt{P}^{\circ}(\texttt{P}^{\circ}$ $(\circ \Theta^{\circ})) + ((\circ_{-0}) + (\circ_{-0})) + (\circ \Pi^{\circ}) [\circ \epsilon^{\circ}] + (\circ \Theta^{\circ}) + (\circ^{-\circ}) + (\circ_{-0}) + (\circ \Pi^{\circ}) [\circ \epsilon^{\circ}] + (\circ \Theta^{\circ}) + ((\circ_{-0}) + (\circ_{-0})) + (\circ^{-\circ}) +$ $[\circ \circ \circ] + (\circ \circ) + ((\circ \circ) + (\circ \circ)) + ((\circ \circ)) + ((\circ \circ)) + (\circ \circ)) + (\circ \circ) + (\circ$ $((\circ_\circ) + (\circ_\circ)) + ((\circ_\circ) + (\circ_\circ)) + (\circ_\circ)) + (\circ_\circ) +$ $(0^{-}0) + (0^{-}0)$ (o^ $(\circ \Theta \circ)) + (\circ \Pi \circ) [\circ \epsilon \circ] + (\circ \Theta \circ) + ((\circ - \circ) + (\circ \Theta \circ)) + (\circ \Theta \circ) + (\circ \Pi \circ) [\circ \epsilon \circ] + (\circ \Theta \circ) + ((\circ - \circ) + (\circ - \circ)) + (\circ - \circ) + (\circ$ $(\circ \Theta^{\circ}) + (\circ \Theta$ $\Pi^{\circ}) \begin{bmatrix} \circ & \epsilon & \circ \end{bmatrix} + (\circ & \Theta^{\circ}) + & (\circ & \Theta^{\circ}) + & (\circ & \Theta^{\circ}) + & (\circ & -\circ) + & (\circ & -\circ)$ $((\circ - \circ) + (\circ - \circ)) + ((\circ - \circ) + (\circ - \circ)) + (\circ - \circ) + ((\circ - \circ) + (\circ - \circ) + (\circ - \circ) + ((\circ - \circ) + (\circ - \circ) + (\circ - \circ) + (\circ - \circ) + ((\circ - \circ) + (\circ - \circ)$ $-^{\circ}) + (^{\circ} \Theta^{\circ})) + (^{\circ} \Pi^{\circ}) [^{\circ} \epsilon^{\circ}] + (^{\circ} \Theta^{\circ}) + ((^{\circ} -^{\circ}) + (^{\circ} -^{\circ})) + ((^{\circ} -^{\circ}) + (^{\circ} \Theta^{\circ})) + (^{\circ} \Pi^{\circ}) [^{\circ} \epsilon^{\circ}] + (^{\circ} -^{\circ}) + ((^{\circ} -^{\circ}) + (^{\circ} -^{\circ})) + (^{\circ} -^{\circ}) + (^{\circ} (\Theta^{\circ})) + (\circ^{\circ} \Pi^{\circ}) [\circ^{\circ} \varepsilon^{\circ}] + ((\circ^{-\circ}) + (\circ^{\circ} \Theta^{\circ})) + (\circ^{\circ} \Theta^{\circ}) + (\circ^{\circ} \Pi^{\circ}) [\circ^{\circ} \circ^{\circ}]) (\circ^{\circ} \Theta^{\circ})) ('_{-}');$

全部复制到 console (控制台) 里,回车键enter一下。



$$\begin{split} & \varepsilon^{\circ} \left[+ (^{\circ} \Theta^{\circ}) + (^{\circ} \Theta^{-} \Theta^{\circ}) + ((^{\circ} - ^{\circ}) + (^{\circ} \Theta^{-} \Theta^{\circ}) + (^{\circ} A^{\circ}) \right] (^{\circ} \varepsilon^{\circ} \right] + (^{\circ} \Theta^{\circ}) + (^{\circ} - ^{\circ}) + (^{\circ} \Theta^{\circ}) + (^{\circ} A^{\circ}) \right] (^{\circ} \varepsilon^{\circ}) + (^{\circ} \Theta^{\circ}) + (^{\circ} - ^{\circ}) + (^{\circ} \Theta^{\circ}) + (^{\circ} A^{\circ}) \right] (^{\circ} \varepsilon^{\circ}) + (^{\circ} \Theta^{\circ}) + (^{\circ} - ^{\circ}) + (^{\circ} \Theta^{\circ}) + (^{\circ} \Theta^{\circ$$

来自 homura.cc	
nctf	
	确定

跳出一个窗口,得到flag。

• 7、单身20年

题目地址

这题可以靠技术也可以靠手速! 老夫单身二十年, 自然靠的是手速!

链接打开,看到提示,点击。

← → C ⁽¹⁾ (i) chinalover.sinaapp.com/web8/	
---	--

到这里找key

发现什么也没有,这就奇怪了。

 $(\leftarrow) \rightarrow \mathbb{C}$ (i) chinalover.sinaapp.com/web8/no_key_is_here_forever.php

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

思考用burpsuite抓包。设置intercept is **on**,开始抓包。 刷新网页,发现Target变成黄字,应该是抓到了什么,去看看。

Target(目标)——显示目标目录结构的的一个功能

Target Proxy Spider Scanner Intruder R	epeater	Sequencer	Decoder	Comparer	Extender	Project
Site map Scope						
Iter: Hiding not found items; hiding CSS, image ar	nd genera	I binary conte	nt; hiding	4xx respons	es; hiding er	mpty fold
🕞 http://chinalover.sinaapp.com	Cont	ents				
http://detectportal.firefox.com	Host		Meth	od URL		Par
	http://	/chinalover.sin	GET	/web8/		
	http://	/chinalover.sin	GET	/web8/no	_key_is_he.	
	http://	/chinalover.sin	GET	/web8/se	earch_key.ph	р
	http://	/chinalover.sin	GET	/		_
	Rec	uest Respo	nse Hex HT	ML Rende	r	
	HTTP/	1.1 200 OK				A
	Date:	: nginx Tue: 03 Dec 2	019 11.21.	57 GMT		
	Conter	nt-Type: text/h	itml			
	Conne	ction: close				
	Via: 10)08 at Longth: 100				
	Conter	it-Length. 100				
	<scrip< td=""><td>>window.lo</td><td>cation="./</td><td>no_key_is_h</td><td>ere_forevei</td><td></td></scrip<>	>window.lo	cation="./	no_key_is_h	ere_forevei	
	php";			· _		
	KCJ 15	. neu		a.csdn.net		33330

哈哈,果然有flag。

• 8、php decode

见到的一个类似编码的shell,请解码

了解php的都知道,eval不能回写,正确应为echo。

见到的一个类似编码的shell, 请解码

```
<?php
function CLsI($ZzvSWE) {
    $ZzvSWE = gzinflate(base64_decode($ZzvSWE));
    for ($i = 0; $i < strlen($ZzvSWE); $i++) {
        $ZzvSWE[$i] = chr(ord($ZzvSWE[$i]) - 1);
    }
    return $ZzvSWE;
}</pre>
```



修改为echo。运行即可得到flag。

```
1 < ?php
 2 function CLsI($ZzvSWE) {
 3
       $ZzvSWE = gzinflate(base64_decode($ZzvSWE));
 4
 5
       for ($i = 0; $i < strlen($ZzvSWE); $i++) {</pre>
 6
 7
           $ZzvSWE[$i] = chr(ord($ZzvSWE[$i]) - 1);
 8
 9
       }
10
11
       return $ZzvSWE;
12
13
          LsI("+7DnQGFmYVZ+eoGm1g0fd3puUoZ1fkppek1GdVZhQnJSSZq5aUImGNQBAA=="));
   echo(
```

phpinfo();	
flag:nctf	}

• 10、单身一百年也没用

题目地址 是的。。这一题你单身一百年也没用

看题目就知道这题与第七题很像,也是考验"手速"。还是按照第七题的方法来做,bp抓包,得到flag。