bugku web writeup(持续更新)



youshangfashi ↓ 7 2018-10-04 10:21:04 发布 ② 223 ↓ 收藏 分类专栏: <u>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/youshangfashi/article/detaik/82935500</u> 版权



CTF 专栏收录该内容 2 篇文章 0 订阅 订阅专栏

web2

打开以后就长这样,眼睛差点瞎掉



不用想先F12一下先



看到阴影部分了没,对就是它。

•

==========

19+53=2	输	Æ		
				来源: <u>BugKu-ctf</u>

先F12一下



然后就在Sources中的index文件里看到了这个,对你没有看错,就是这个。

4 m

web基础\$_GET

打开以后就长这样



然后看这个意思是让输进去一个what=flag呗,所以就输进去"?what=flag",然后



左边的插件是Hacker,右边是输出来的结果,对就是它。

web基础\$_POST

打开以后是这样的



在下面的框里输入"what=flag"



然后flag就出来了,对就是它。

==	4 m		
•	m	•	
矛	盾		

打开以后是这样的



代码的意思就是输入的num不是数字或者数字字串,所以输入"?num=1e+0"

 Bugku_百度授索 × ← → C² 合 ☆ 最常访问 益 百度一下,你就知道 	120.24.86.145:8002/get/index1.+ x + ① 120.24.86.145:8002/get/index1.php?num=1e+0
<pre> Hackbar ></pre>	<pre>\$_GET['num']; if(lis_numeric(\$num)) { echo \$num; if(\$num==1) echo 'flag(*********)'; } 1e Oflag(bugku-789-ps-ssdf)</pre>
Enable Post data	

对就是它, flag就蹦出来了。

==		
•	III	4

web3

打开以后是长这样的



然后先F12,就是这样了

BCX-MBI X	Puperti-more x +		😂 🛪 🖉 🖉 🖉 🖬 🕹 📽 😫	- 0 >
-) → × @	© 120.24.86.145.0032/web3/	& Q. 10.0	IN 14 🖬 🔟 🗭	🖓 🛛 🖬 🕴
янин алк-т. снол			_	
Hadder - X		G Date Stren Date (Leciste Stat C	FRE 2 RE 8 ME CASKS	
Tenter Tenter		#27 AR E (rdot +		
Laad 2 tyle 0 that		 O COLLECTION I MARTINIANINA I MARTINIANINA I MARTINIANINA 		
tp://120.24.86.145:5002		C protect Address Martin Control of State		
end/		 9 non-commission Martink 2004/25 		
		 O metosok Martink Score (%) Martink Score (%) 		
Cold Box Car		And the second s		
7804 781 082	*1117	and the second s		
	C REAL PROPERTY OF	C High Rivers		
		Design of a second seco		
	H 2	sant's weeks		
Stable Referen		Here's Barry Street of		
		starts to source as		
		adart for application of a		
		and the second second		
		adares (A. Manager)		
		alare (Viagel Medal) a alare (Viagel Medal)		
		Address (CAL SACRAFT)		
		alart (% 0000 F) alart (*) alart (*) alart		
		11 TO LOCAL BARD, BARD, BARD, BARD, BARD, BARD, BARD, BARD,		
		10 total		
		10		
		111		
from to maniference	RR 1002436.145			and the second designed in the

可以看出,下面有一行比较明显的字符编码,复制出来

(KEY{J2sa42ahJK-HS 明显是Unicode,然后转ASCII码就行了。 < _____

Þ.

转换的网址(http://tool.chinaz.com/tools/unicode.aspx)得到

111



对就是它。

______ • Þ.

剩下的稍等