# **CTF** writeup



上面显示maxlength=10;

所以,利用浏览器自有 Learnxic.sinaap	带插件,我这里用的是Firefox的hackbar插件,直接越过HTML代码直接进行post传递:
🗲 🛈 🔏 tear	nxlc.sinaapp.com/web1/02298884f0724c04293b4d8c0178615e/index.php
INT ~	SQL* XSS* Encryption* Encoding* Other*
<ul> <li>Load URL</li> <li>Split URL</li> <li>Execute</li> </ul>	http://teamxlc.sinaapp.com/web1/02298884f0724c04293b4d8c0178615e/index.php
	Enable Post data Enable Referrer
Post data	text1=zhimakaimen

### flag is:nctf{follow\_me\_to\_exploit}

输入框:		
请输入口	令: zhimakaimen	开门



#### 下载图片,用记事本打开,拉到最后就有flag;

#### 层层递进



打开后一脸懵逼,这和平常的不一样,找了半天也没有头绪,后来看别人的writeup:

清除	全保持	全	部HTM	AL CSS	JavaS	Script	XHR	图片	插件	媒体	字体
🗄 GE	ET stat.h	tm?id	=12609	57102&	485a3	200	OK				z4.cnzz.com
🖃 GE	ET 404.h	tml				200	OK (BF	Cache)			chinalover.sinaapp
¥	人信息 『	向应	HTML #	爱存							
<pre><htm <="" <met="" b0="" h1="" h2="" pre="" sry=""> <pre>A:  <pre></pre> <p< th=""><th>AL&gt;<head> TA HTTP-E TA HTTP-E TLE type= DDY { font 1 { font: 2 { font:</head></th><th><pre>&lt;</pre> <pre>(</pre> <pre></pre></th><th><pre>S&gt;有人偷们 "Content- /css"&gt; t/12pt 宋 /15pt 宋仲 /15pt 宋仲 /15pt 宋仲 /12pt 宋 /12pt /1</pre></th><th>俞先做题, Type<sup>(7)</sup> Co 体 } } n } cellspac the docu .7.2.min .7.3.min .7.3.min .7.3.min .7.3.min .7.3.min .7.3.min .7.3.min .7.3.min .7.3.min .7.3.min .7.3.m</th><th>哈哈飞了 ntent="te ing=10&gt;&lt;1 js"&gt;<th>TR&gt;<td) ext/htm the page cript&gt; cript</td) </th><th>/TITLE&gt; al: char ges load</th><th>l faster</th><th>312"&gt;</th><th></th><th></th></th></p<></pre></htm></pre>	AL> <head> TA HTTP-E TA HTTP-E TLE type= DDY { font 1 { font: 2 { font:</head>	<pre>&lt;</pre> <pre>(</pre> <pre></pre>	<pre>S&gt;有人偷们 "Content- /css"&gt; t/12pt 宋 /15pt 宋仲 /15pt 宋仲 /15pt 宋仲 /12pt 宋 /12pt /1</pre>	俞先做题, Type <sup>(7)</sup> Co 体 } } n } cellspac the docu .7.2.min .7.3.min .7.3.min .7.3.min .7.3.min .7.3.min .7.3.min .7.3.min .7.3.min .7.3.min .7.3.min .7.3.m	哈哈飞了 ntent="te ing=10><1 js"> <th>TR&gt;<td) ext/htm the page cript&gt; cript</td) </th> <th>/TITLE&gt; al: char ges load</th> <th>l faster</th> <th>312"&gt;</th> <th></th> <th></th>	TR> <td) ext/htm the page cript&gt; cript</td) 	/TITLE> al: char ges load	l faster	312">		

看半天才看出来在下面的7.2之前的第一个字符合起来就是flag;



到这里找key
---------

点击进去:

chinalover.sinaapp.com/web8 × +

(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

firebug,直接出来



①作打卡挑战赛
 □流量/现金/CSDN周边激励大奖