-些简单的write up



<u>mini_sailing</u> ● 于 2018-04-19 19:10:47 发布 ● 1270 ☆ 收藏 1 分类专栏: wp 文章标签: ctf 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/mini_sailing/article/details/80009057</u> 版权

版权

wp专栏收录该内容

2篇文章 0 订阅 订阅专栏 刚刚做了几道简单的ctf题,顺便写下write up,做个简单的记录。

在bugku平台上做的题。

首先是杂项栏目的题:

1.这是一张单纯的图片: http://120.24.86.145:8002/misc/1.jpg

根据题目可以猜出这应该是一道很简单的题,保存图片后直接用记事本打开,

(() (?□貯 7]郴沙[y靏嶇1攝□6□李₩ (?氣-痣Z?姶_□ 皨K□r□h . 厈掅皛@?q??);E□ QE□ ₩近x:-□饷腤T警□ヨ??□槜 愍Cr□Wd□?□楔 ((keyyyou are right}僑 ni sailing

最后一行可以明显看出是Unicode编码,直接在线解密,得flag。

Unicode编码	UTF-8编码	URL编码/解码	Unix时间戳	Ascii/Native编码互转	
ke&#	121;{	21;ou&#</th><th>#32;ar</th><th>e </th><th>key{you are right}</th></tr><tr><td>ri&#</td><td>103;h</td><td>16;}</td><td>https:/</td><td>/blog.csdn.ne</td><td>et/mini_sailing</td></tr></tbody></table>			

2.猜: http://120.24.86.145:8002/misc/cai/QQ20170221-132626.png

打开图片发现图片是一个人的半张脸,根据提示知道flag是一个人名,那就百度识图看看就可以了,轻易就发现 了图片上到底是谁~~~

接下来做了几道web的题,因为对web比较感兴趣,就先做了web的。



1.web2: http://120.24.86.145:8002/web2/

直接得到了flag,是一道很简单的题。

2.文件上传测试: http://103.238.227.13:10085/

要求上传PHP文件,找一个PHP文件上传后提示非图片文件,若上传图片则提示非PHP文件,于是用burp 抓包试试,观察到 关键字filename=1.jpg

--WebKitFormBoundarysVJSn3Cwzvlunl9y

Content-Disposition: form-data; name="file"; filename="1.jpg" Content-Type: image/jpeg

直接修改为1.jpg.php,然后Ctrl+R,再forward,在网页上就出现了flag。

3.计算器: http://120.24.86.145:8002/yanzhengma/

也是很简单的一道题,打开题目发现是计算题,想输入答案,但发现无法验证成功,于是查看源代码,发现代码中将答案最大 长度设置为"1",修改最大长度,任一个大于正确答案的长度都行,之后再输入正确答案,就能得到flag了。