

# 能麻烦你给我们队报个名吗-cumt ctf1月双月赛wp

原创

地瓜呱  于 2019-01-29 20:17:33 发布  188  收藏

分类专栏: [ctf](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/Nebulacedia/article/details/86694904>

版权



[ctf](#) 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

## 1月双月赛writeup

### WEB

#### 1.签到题

一道简单的代码审计

□

看到了常见的PHP可绕过函数。

用 `%00` 可绕过 `ereg()`, `in_array()` 未设置参数的弱比较, 通过 `数组` 可以绕过 `md5()` 函数。

方法一:

利用 `%00` 截断绕过正则匹配, 再利用 `in_array()` 的宽松比较得到flag。

```
http://202.119.201.199:32790/?0ver=1%00adc&0ver1[]=1&0ver2[]=2
```

方法二

只利用 `in_array()` 的宽松比较得到flag

```
http://202.119.201.199:32790/?0ver=01&0ver1[]=1&0ver2[]=2
```

```
### SimpleUpload签到 查看网页源代码发现有js前端过滤 ``JavaScript function checkFile(){ var file = document.getElementsByName('upload_file')[0].value; if (file == null || file == "") { alert("请选择要上传的文件!"); return false; } //定义允许上传的文件类型 var allow_ext = ".jpg|.png|.gif"; //提取上传文件的类型 var ext_name = file.substring(file.lastIndexOf(".")); //判断上传文件类型是否允许上传 if (allow_ext.indexOf(ext_name) == -1) { var errMsg = "该文件不允许上传, 请上传" + allow_ext + "类型的文件, 当前文件类型为: " + ext_name; alert(errMsg); return false; } }
```

直接修改白名单, 将 `.php` 加入到白名单中然后上传php文件得到flag

### CRYPTO

#### 现代密码签到

根据给出的提示是用了 `DES` 加密, 直接将密文粘贴解密网站进行解密得到flag

## 古典密码签到

LZYGQ326N5QXMYAKORNG42TABJ2FUWS2MNRWG6A= 通过base32解码:

```
phooav`  
tZnj`  
tZZcccX
```

把换行符变为'\n';写代码得到flag:

```
cumtctf{easy_soeasy__hhh}
```

```
askrardyc_qw]qmc_qw]]]fff {  
btlsbsezd rx rnd rx   ggg |  
cumtctf|easy_soeasy__hhh|  
dvnudug|fbtz tpfbtz   iii  
ewovevh}gcu{auqgcu{aaa}jj}
```

## MISC

### MISC签到

百度盲文，对应翻译一下，把A变成1 即得

```
flag{B1IND}
```

### Base全家桶了解一下?

R1kzRE1RWdHRTNET04yQ0dVM1RNTkpXSU0zREdNWIFHWkNETU5KVklZM1RJTVpRR01ZREtSUIIdHTTNUS05TRUc0  
MkRNTVpYR1EzRE1OMkU=

按 [base64-base32-base16](#) 的顺序解码，得到:

```
flag{Welcome_t00_cumtctf}
```

###BXS图标真好看

Hex打开看到是png文件，改后缀名得到图中密文 `fgookwnl{un_gaDy_0p}`

栅栏密码，组数为3，得到flag:

```
flag{Do_you_kn0w_png}
```

###起床改error啦!

Binwalk，发现隐藏的压缩包 提取出来

```
root@digua-kail:~# binwalk 2333.png
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JPEG image data, JFIF standard 1.01
47717	0xBA65	Zip archive data, at least v2.0 to extract, compressed size: 2177, uncompressed size: 10240, name: flag.doc
50922	0xC366	End of Zip archive, footer length: 22

解压缩是一个word文档，显示隐藏的文件得

## REVERSE

### 逆向签到 (NBQXAZK7NBYGQ===)

输入与0-99其中的一个数异或以后得到的字符串与内置字符串s对比  
所以得flag只需把内置的s与0-99分别异或，找有意义的字符串

```

ty cJyv | (u=) wwG!qn} GmG- {wj} e
ys xdM q{/r:. pp@&viz@j@*} pmzb
xr yeL pz. s;/qqA`wh{AkA+} q1{c
{q|zf0|sy-p8,rrB$tkxBhB( rox
zp) {gN} rx, q9-ssC%ujyCiC) snya
eobdxQbmg3n&211\ : juf\v\6 lqf`
dnceyPc1f2o' 3mm];ktg]w]7ampg
gm fzS oe1l$0nn 8hwd t 4bnsd|
flag{Rand0m%100_9ive_u_5core}
akf |Ufic7j^6hhX>nqbXrX2dhubz
`jga} Tghb6k#7iiY?opcYsY3eitc{
cidb Wdka5h 4jjZ<ls ZpZ0fjw x
bhec Vej 4i!5kk[-mralq[lgkvay
mgjlpYjeo;f. :ddT2b}nT T>hdynv
lfkmqXkdn:g/;eeU3c|oU U?iexow
oehnr[hgm9d,8ffV0` 1V|V<jf{1t
ndiosZifl8a-9ggw1a~mW}w=kgzmu
icnht]nak?b* / Pofv]PzP:1 }jr

```

## Eazy-Math

输入s，经过  $s*v5$  以后与内置的字符串v4进行比较；  
所以求v5的逆 计算  $v4*(v5-1)$  输出即可

矩阵A:

第1列	第2列	第3列
274.0000	294.0000	316.0000
262.0000	274.0000	252.0000
380.0000	421.0000	427.0000

矩阵B:

第1列	第2列	第3列
-0.2500	0.7500	-0.2500
0.7500	-0.2500	-0.2500
-0.2500	-0.2500	0.7500

您所输入问题的解C=A\*B如下:

第1列	第2列	第3列
73.0000	53.0000	95.0000
77.0000	65.0000	55.0000
114.0000	73.0000	120.0000

```
flag{i5_MA7r1x}
```

---

ps:令全说 路漫漫其修远兮，吾将上下而求索