

攻防世界Misc新手区部分题解

原创

Outman8 于 2021-04-19 23:44:06 发布 252 收藏 1

分类专栏: [Misc](#)

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/outman23/article/details/115876901>

版权



[Misc 专栏收录该内容](#)

3 篇文章 0 订阅

订阅专栏

攻防世界Misc新手区部分题解

[this_is_flag](#)

[pdf](#)

[如来十三掌](#)

[give_you_flag](#)

[坚持60s](#)

[gif](#)

this_is_flag

this_is_flag 113 **最佳Writeup由王兆敏提供**

难度系数: **★★2.0**

题目来源: 暂无

题目描述: Most flags are in the form flag{xxx}, for example:flag{th1s_!s_a_d4m0_4!a9}

题目场景: 暂无

题目附件: 暂无

<https://blog.csdn.net/outman23>

这题没什么说的, flag

在题目上

[pdf](#)

pdf 84 **最佳Writeup由S_O_L_R提供**

难度系数: ★★★ 3.0

题目来源: csaw

题目描述: 菜猫给了菜狗一张图, 说图下面什么都没有

题目场景: 暂无

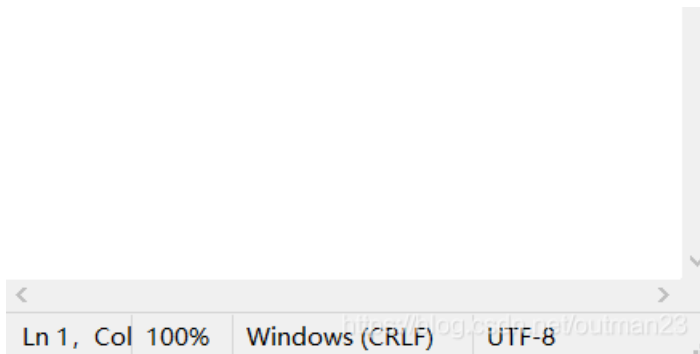
题目附件: 附件1 <https://blog.csdn.net/outman23>

用浏览器打开附件, 不要下载, 然后鼠标扫过图片, 会有一行代码。



然后复制到文本上, 得到flag.

```
*新建文本文档.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
flag{security_through_obs}
```



如来十三掌

如来十三掌

👍 115 最佳Writeup由flag{not_here} · 渣渣禹提供

难度系数: ★★★★★ 3.0

题目来源: 暂无

题目描述: 菜狗为了打败菜猫, 学了一套如来十三掌。

题目场景: 暂无

题目附件: [附件1](#)

<https://blog.csdn.net/outman23>

下载附件后打开

夜哆悉諳多苦奢陀奢諦冥神哆盧穆幡三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀
諳怖奢智侄諸若奢數菩奢集遠俱老竟寫明奢若梵等盧幡豆蒙密離怯婆幡礙他哆提哆
多鉢以南哆心曰姪罰蒙呐神。舍切真怯勝呐得俱沙罰娑是怯遠得呐數罰輸哆遠薩得
槃漫夢盧幡亦醢呐娑幡瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿幡沙蘇
輸奢恐豆侄得罰提哆伽諳沙楞鉢三死怯摩大蘇者數一遮

此处应用佛语转换

链接: [佛语转化](#)

将需要解码的文字输入在下面的文本框里, 记得带上『佛曰: 』或『如是我闻: 』的文字, 点击『参悟佛所言的真意』按钮, 就能在上面的文本框里得到解码后的文字。

然后这段文字前面加上“佛曰: ”

转化后得到

与佛论禅

MzkuM3gvMUAwnzuvn3cgozMlMTuvqzAenJchMUAeqzWenzEmLJW9

听佛说宇宙的真谛

参悟佛所言的真意

普度众生

刹那便是永恒

佛曰：夜哆悉諳多苦奢陀奢諦冥神哆盧穆幡三侄三即諳諳即冥迦冥隸數顛耶迦奢若吉佉諳怖奢智侄諳若奢數菩奢集遠俱老竟寫明奢若梵等盧幡豆蒙密離佉婆幡礙他哆提哆多鉢以南哆心曰姪罰蒙訥神。舍切真佉勝訥得俱沙罰娑是佉遠得訥數罰輸哆遠薩得槃漫夢盧幡亦醯訥娑幡瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿幡沙蘇輸奢恐豆侄得罰提哆伽諳沙楞鉢三死佉摩大蘇者數一遮

<https://blog.csdn.net/outman23>

由题目如来"十三"掌 易知可能为 ROT13形式
转码后

ROT13 编码： (字母)

ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

ROT47

ROT18

ROT13

ROT5

复位

再进行一次base64解码即可得到flag

ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

清空

加密

解密

解密结果以16进制显示

```
flag{bdscjhbkmznmfrdhbvcki jndskvbkjdsab}
```

复制

<https://blog.csdn.net/outman23>

give_you_flag

give_you_flag

👍 86 最佳Writeup由testtestzs提供

难度系数: ★★★★★ 4.0

题目来源: 暂无

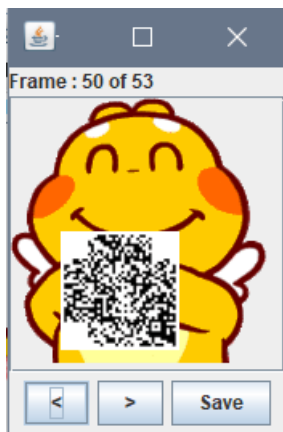
题目描述: 菜狗找到了文件中的彩蛋很开心, 给菜猫发了个表情包

题目场景: 暂无

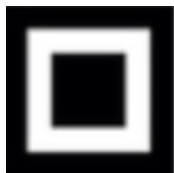
题目附件: [附件1](#)

<https://blog.csdn.net/outman23>

下载附件后, 是一个gif动画, 用图片隐写破译软件stegsolve打开进行逐帧查看, 得到残缺的二维码。



在二维码残缺的3个角落加上定位点（如下）



得到如下二维码



然后用QR Research扫描得到flag



坚持60s

坚持60s

👍 14

最佳Writeup由不要让我起名提供

难度系数:



题目来源:

08067CTF

题目描述: 菜狗发现最近菜猫不爱理他, 反而迷上了菜鸡

题目场景: 暂无

题目附件:

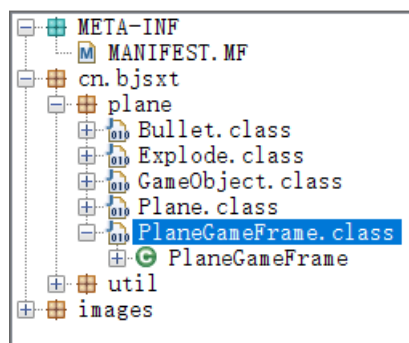
附件1

<https://blog.csdn.net/outman23>

下载附件打开后是一个动图, 并且是java环境, 所以我们用一个Java查看源码的软件——Java Decompiler,

打开后

找到这个路径



即可看到源码

```
    this.p.draw(g);
    for (int i = 0; i < this.bulletList.size(); i++) {
        Bullet b = this.bulletList.get(i);
        b.draw(g);
        boolean peng = b.getRect().intersects(this.p.getRect());
        if (peng) {
            this.p.setLive(false);
            if (this.bao == null) {
                this.endTime = new Date();
                this.bao = new Explode(this.p.x, this.p.y);
            }
            this.bao.draw(g);
        }
    }
    if (!this.p.isLive()) {
        printInfo(g, "兄弟就死了的嘛", 50, 150, 200);
        int period = (int)((this.endTime.getTime() - this.startTime.getTime()) / 1000L);
        printInfo(g, "你的持久度才" + period + "秒", 50, 150, 250);
        switch (period / 10) {
            case 0:
                printInfo(g, "真·头顶一片青青草原", 50, 150, 300);
                break;
            case 1:
                printInfo(g, "这东西你也要抢着带?", 50, 150, 300);
                break;
            case 2:
                printInfo(g, "如果梦想有颜色, 那一定是原谅色", 40, 30, 300);
                break;
            case 3:
                printInfo(g, "哟, 炊事班长呀兄弟", 50, 150, 300);
                break;
            case 4:
                printInfo(g, "加油你就是下一个老王", 50, 150, 300);
                break;
            case 5:
                printInfo(g, "如果撑过一分钟我岂不是很没面子", 40, 30, 300);
                break;
            case 6:
                printInfo(g, "flag{RGFqaURhbG1fSmlud2FuQ2hpamk=}", 50, 150, 300);
                break;
        }
    }
}
```

<https://blog.csdn.net/outman23>

然后base64解码得到flag

gif

gif 👍 50 最佳Writeup由不要让我起名提供

难度系数: ★★★★★ 4.0

题目来源: 暂无

题目描述: 菜狗截获了一张菜鸡发给菜猫的动态图, 却发现另有玄机

题目场景: 暂无

题目附件: 附件1

<https://blog.csdn.net/outman23>

下载附件, 解压后打开文件夹得到许多一黑一白的图片



大胆猜测是二进制，即0是白色，1是黑色。

把所有图转换为二进制得到如下。

```
011001100110110001100001011001110111101101000110011101010100111001011111011001110110100101000110011
1101
```

可以用脚本进行破译，当然也可以采用工具

二进制转换文本网址：<http://www.txttool.com/t/?id=Mzky>

在线二进制转换字符串[EN]

输入二进制文本:

```
0110011001101100011000010110011101111011010001100111010101001110010111110110011101101001010001100111101
```

转换后的文本:

```
flag{FuN_giF}
```