BUUCTF练习

原创

abtgu 于 2020-09-26 13:52:41 发布 1021 收藏 1

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/weixin_43790779/article/details/108811114

版权

CTF 专栏收录该内容

22 篇文章 1 订阅

订阅专栏

easycap

题目： 得到的 flag 请包上 flag{} 提交

解题思路： 用wireshark打开，追踪tcp流即可得到flag，flag{385b87afc8671dee07550290d16a8071}

假如给我三天光明

题目： 得到的 flag 请包上 flag{} 提交

解题思路： 查看图片，发现下面是盲文，对照盲文ASCII码解码得到kmdonowg，打开另一个压缩包，kmdonowg即为解压密码。用Audacity打开，发现是摩斯电码，解码即可,flag{wpei08732?23dz}。

FLAG

题目： 感谢 牌森 同学提供题目~注意：请将 hctf 替换为 flag 提交，格式 flag{}

解题思路： 用stegsolve打开，使用Data Extract功能，发现有PK，save bin保存为zip，打开压缩包，发现一个未知类型的文件，在kali中使用strings命令即可找到flag，hctf{dd0gf4c3tok3yb0ard4g41n~~~}。

另外一个世界

题目： 得到的 flag 请包上 flag{} 提交

解题思路： 用notepad++打开图片，发现一串二进制数，将其转换成ASCII码，得到flag，flag{koekj3s}。

[MRCTF2020]Ez_bypass

题目： 无

解题思路： 打开题目，发现源码

```
I put something in F12 for you
include 'flag.php';
$flag='MRCTF{xxxxxxxxxxxxxxxxxxxxxxxxx}';
if(isset($_GET['gg'])&&isset($_GET['id'])) {
    $id=$_GET['id'];
    $gg=$_GET['gg'];
    if (md5($id) === md5($gg) && $id !== $gg) {
        echo 'You got the first step';
        if(isset($_POST['passwd'])) {
            $passwd=$_POST['passwd'];
            if (!is_numeric($passwd))
            {
                 if($passwd==1234567)
                 {
                     echo 'Good Job!';
                     highlight_file('flag.php');
                     die('By Retr_0');
                 }
                 else
                 {
                     echo "can you think twice??";
                 }
            }
            else{
                echo 'You can not get it !';
            }

        }
        else{
            die('only one way to get the flag');
        }
}
    else {
        echo "You are not a real hacker!";
    }
}
else{
    die('Please input first');
}
}Please input first
```

首先，MD5强相等，数组绕过：`?gg[]=1&id[]=2`；
之后，is_numeric()绕过：passwd=1234567%00
得到flag，flag{f8e33de7-c9d4-4e9a-8031-1b412a2ff7a1}。