2018·i春秋圣诞欢乐赛官方WriteUp

原创

可乐' 于 2019-01-09 19:21:23 发布

分类专栏： CTFwrite 文章标签： CTF

gift

打开页面

考点: snow html隐写

```
snow 是一款在html嵌入隐写信息的软件，
它的原理是通过在文本文件的末尾嵌入空格和制表位的方式嵌入隐藏信息，
不同空格与制表位的组合代表不同的嵌入信息。
```

解密网址：http://fog.misty.com/perry/ccs/snow/snow/snow.html
密钥为题目名字

gift php

Do you know .swp file? 非正常关闭vi编辑器时会生成一个.swp文件
访问.index.php.swp下载下来， vim-r.index.php.swp还原即可 源码

```
<?php
function areyouok($greeting){
    return preg_match('/Merry.*Christmas/is',$greeting);
}

$greeting=@$_POST['greeting'];
if(!areyouok($greeting)){
    if(strpos($greeting,'Merry Christmas')!==false){
        echo 'Merry Christmas. '.'flag{****}';
    }else{
        echo 'Do you know .swp file?';
    }
}else{
    echo 'Do you know PHP?';
}
?>
```

要求post一个 greeting参数，经过areyouok函数正则过滤后如果返回false，
就进入下一个if，如果 greeting参数包含 MerryChristmas则打印flag。
可以利用strpos函数的一个漏洞，传入一个数组，会返回 NULL， NULL不强等于false，即可绕过。

gift php plus

这题是在gift php的基础上加上了is_array的判断，不允许使用数组来绕过。

所以上一道题的思路不能再用了。 这里需要用到正则回溯，可以参考p牛的文章：https://www.leavesongs.com/PENETRATION/use-pcre-backtrack-limit-to-bypass-restrict.html

PHP为了防止正则表达式的拒绝服务攻击（reDOS），给pcre设定了一个回溯次数上限 pcre.backtrack_limit，默认为100万。当正则回溯超过这个上限时，就会返回false。

因此我们只要post100万个字符，让它回溯大于100万次，函数就会返回false，从而绕过if判断。