

【bugku_writeup】web30 txt????

原创

kzaaa 于 2021-01-01 16:26:36 发布 39 收藏

分类专栏: [ctf bugku_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/kongzhian/article/details/112061156>

版权



[ctf bugku_writeup](#) 专栏收录该内容

13 篇文章 0 订阅

订阅专栏

点进去, 又是一段php代码

```
<?php
extract($_GET);
if (!empty($_$ac))
{
    $f = trim(file_get_contents($_$fn));
    if ($_$ac === $f)
    {
        echo "<p>This is flag:" . " $_$flag</p>";
    }
    else
    {
        echo "<p>sorry!</p>";
    }
}
?>
```

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

extract的使用:

```
$a = "Original";
$my_array = array("a" => "Cat", "b" => "Dog", "c" => "Horse");
extract($my_array, EXTR_PREFIX_SAME, "dup");
echo "\$a = $a; \$b = $b; \$c = $c; \$dup_a = $dup_a";
```

输出: \$a = Original; \$b = Dog; \$c = Horse; \$dup_a = Cat

EXTR_PREFIX_SAME: 如果有冲突, 加上前缀, 在后面加上
"dup" 前缀

\$_GET 所有参数形成数组

其实这两部就是把get参数的键和值变为php中的变量赋值方向

file_get_contents() 将整个文件返回一个字符串

trim() 默认清除两边的空白字符, 第二个参数为制定两边删除的字符

关键是读取文件内容那块

题目提示了txt????

根据经验尝试进入flag.txt, 没有经验也可以利用burpsuite中的spider扫一下

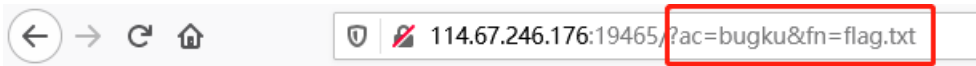


进入txt



bugku

这相当于给答案了，构造payload,得到flag



```
<?php
extract($_GET);
if (!empty($ac))
{
$f = trim(file_get_contents($fn));
if ($ac === $f)
{
echo "<p>This is flag:" . " $flag</p>";
}
else
{
echo "<p>sorry!</p>";
}
}
?>
```

This is flag: flag{f113acf878e55672a78987614663b2d6}

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