【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

本文链接：https://blog.csdn.net/kongzhian/article/details/112061156

点进去，又是一段php代码

```php
<?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>";
}
}
?>
```


extract的使用：

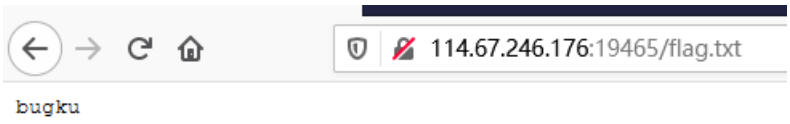
```
$a = "Original";
$my_array = array("a" => "Cat", "b" => "Dog", "c" => "Horse");
extract($my_array, EXTR_PREFIX_SAME, "dup");
echo "\$a = $a; \$b = $b; \$c = $c; \$dup_a = $dup_a";

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



这相当于给答案了，构造payload,得到flag