Hgame week2 write up

easy_php

拿到题目,标题是 where is my robots, 百度知道有个叫做 robots.txt 的文件,所以访问 /robots.txt ,提示要去 /img/index.php

```
草榴社区.jpg

<?php

error_reporting(0);

$img = $_GET['img'];

if(!isset($img))

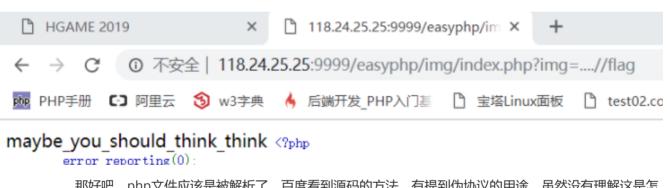
$img = '1';

$img = str_replace('../', '', $img);

include_once($img.".php");

highlight_file(__FILE__);
```

意思是将所有的 . . / 替换成 , include_once , 如果没有设置过 img 的话将其设置为 1 , 猜测flag在 flag.php 中,所以传 img=flag , 但是啥也没有,而过滤了 . . / 所以猜测是在上一个文件夹下的文件 (好吧其实是问学长的) , 因此传 img= // flag , 因为 // 过滤后正好是 . . / ,然后。。。



。。。。。那好吧,php文件应该是被解析了,百度看到源码的方法,有提到伪协议的用途,虽然没有理解这是怎么个用法,但是照猫画虎得到payload: img=php://filter/read=convert.base64-

encode/resource=..../flag,得到base64加密后的源码

PD9waHAKICAgIC8vJGZsYWcgPSAnaGdhbWV7WW91XzRyZV9Tb19nMG9kfSc7CiAgICBIY2hvICJtYXliZV95b3Vfc2hvdWxkX3RoaV error_reporting(0); \$img = \$_CBT['img']; if(!isset(\$img)) \$imx = '1':

解密一下

● UTF16加密(\x开头) ● UTF16解密(\x开头)

```
<?php
//$flag = 'hgame{You_4re_So_g0od}';
echo "maybe_you_should_think_think";</pre>
```

拿到flag,其他好多题都是卡一半不会绕过了 \ (*。>Д<)o \degree