ctf读取index.php,CTF/CTF练习平台-flag在index里【php://filter的利用】，ctf-flag

转载

直江信纲二号机 于 2021-03-10 23:17:40 发布 295 收藏
文章标签： ctf读取index.php
CTF/CTF练习平台-flag在index里【php://filter的利用】，ctf-flag

原题内容：

http://120.24.86.145:8005/post/

Mark一下这道题，前前后后弄了两个多小时，翻了一下别的博主的wp感觉还是讲的太粗了，这里总结下自己的理解：

首先打开这道题，页面只给你click me? no

点击进去显示test5

第一步，查看源代码，无果

第二步bp，无果

结合到题目，flag在index里，大胆尝试http://120.24.86.145:8005/post/index.php，可惜和之前一样

注意到了传值为http://120.24.86.145:8005/post/index.php?file=show.php

file这个变量应该是关键，可惜无果

参考到别的博主的wp：

file传值为

php://filter/read=convert.base64-encode/resource=index.php

结果如下：

base64解密下就得到flag了

可能很多人到这里并不太理解，这里我做具体解释：

首先来解释下这段代码的意思：

即以base64加密的方式读取resource的内容

然后我们来看一下php://filter的限制

要求将传进来的参数进入include()；在这题即是$file //这里就打乱了我的胡思乱想，哈哈哈，还以为所有题目都可以呢

这点要求在后来拿到的题目源码中也可确认：

Bugku-ctf
error_reporting(0);

if(!$_GET[file]){echo 'click me? no';}

```
$file=$_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}
?>
```

下面演示通过php://filter读取本包含漏洞脚本的源码

接下来只要将base64编码后的字符串通过base64解码就可得到PHP文件的源码了

看到一个大佬的博客讲的特别棒，我已转载至我的博客，大家可以前去一看

谈一谈php://filter的妙用

参考原文

http://blog.csdn.net/qq_35078631/article/details/69488266

http://www.freebuf.com/articles/web/14097.html

http://www.dengb.com/fwqyw/1341588.htmlwww.dengb.comtruehttp://www.dengb.com/fwqyw/1341588.htmlTec
练习平台-flag在index里【php://filter的利用】，ctf-flag 原题内容： http://120.24.86.145:8005/post/ Mark一下这道题，前前后后弄了两个多小时，...