ctf提示flag在php里,CTF-flag在index里 80

转载

weixin_39884373 于 2021-03-27 16:30:33 发布 341 收藏
文章标签： ctf提示flag在php里
CTF-flag在index里 80

进入链接

点一下

一脸懵逼，百度知道这是文件包含漏洞

将file=show.php改成file=php://filter/read=convert.base64-encode/resource=index.php

得到一串base64密文，进行解码得到：

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}

?>

?

现在具体说说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。

?

解释引用于：

————————————————

版权声明：本文为CSDN博主「安~然」的原创文章，遵循CC 4.0 BY-SA版权协议，转载请附上原文出处链接及本声明。

原文链接：https://blog.csdn.net/zpy1998zpy/java/article/details/80585443

原文：https://www.cnblogs.com/cxl862002755/p/13160446.html