

[ACTF2020 新生赛]Include

原创

绪风1128 于 2021-05-17 20:00:53 发布 28 收藏

分类专栏: [CTF](#) 文章标签: [web](#)

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/qq_56224547/article/details/116946714

版权



[CTF 专栏收录该内容](#)

3 篇文章 0 订阅

订阅专栏

[ACTF2020 新生赛]Include

首先打开题目场景

Can you find out the flag?

然后我们按照习惯查看一下源代码, 然而并没有什么有价值的发现

无意间看见

```
ffde3960-2362-4b11-8811-f86a0ae608ce.node3.buuoj.cn/?file=flag.php
```

猜测或许是文件包含漏洞,

可能是伪协议, 我们尝试构造payload

```
PD9waHAKZWNobyAiQ2FulHlvdSBmaW5kiG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7NjI5MjlyNDYtYjZjOS00MTgxLWlzNjltMjI4MGRIMjY5NDZhQo=
```

得到一串代码

我们在网页上搜索base64在线解码

请输入要进行 Base64 编码或解码的字符

```
PD9waHAKZWNobyAiQ2FulHlvdSBmaW5kiG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7NjI5MjlyNDYtYjZjOS00MTgxLWlzNjltMjI4MGRIMjY5NDZhQo=
```

编码 (Encode)

解码 (Decode)

↕ 交换

(编码快捷键: **Ctrl** + **Enter**)

Base64 编码或解码的结果:

编/解码后自动全选

```
<?php  
echo "Can you find out the flag?";  
//flag{62922246-b6c9-4181-b362-2280de26946a}
```

https://blog.csdn.net/qq_56224547

Flag就出来了