**Pass-03黑名单绕过**

先上传一个后缀.php的文件。



可以看到，服务器端做了一个黑名单过滤，过滤了 asp、aspx、php、jsp。

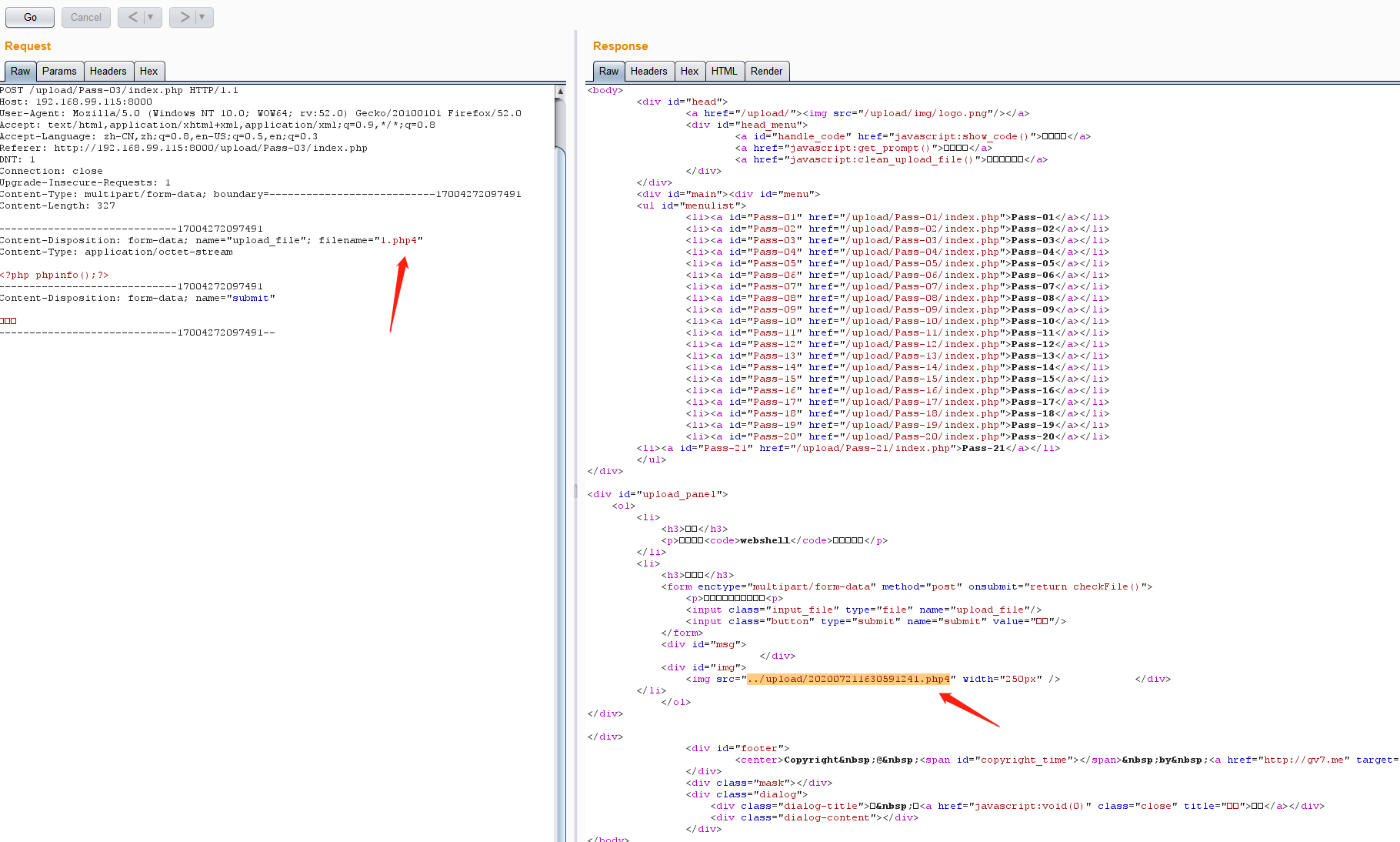
**绕过方法**

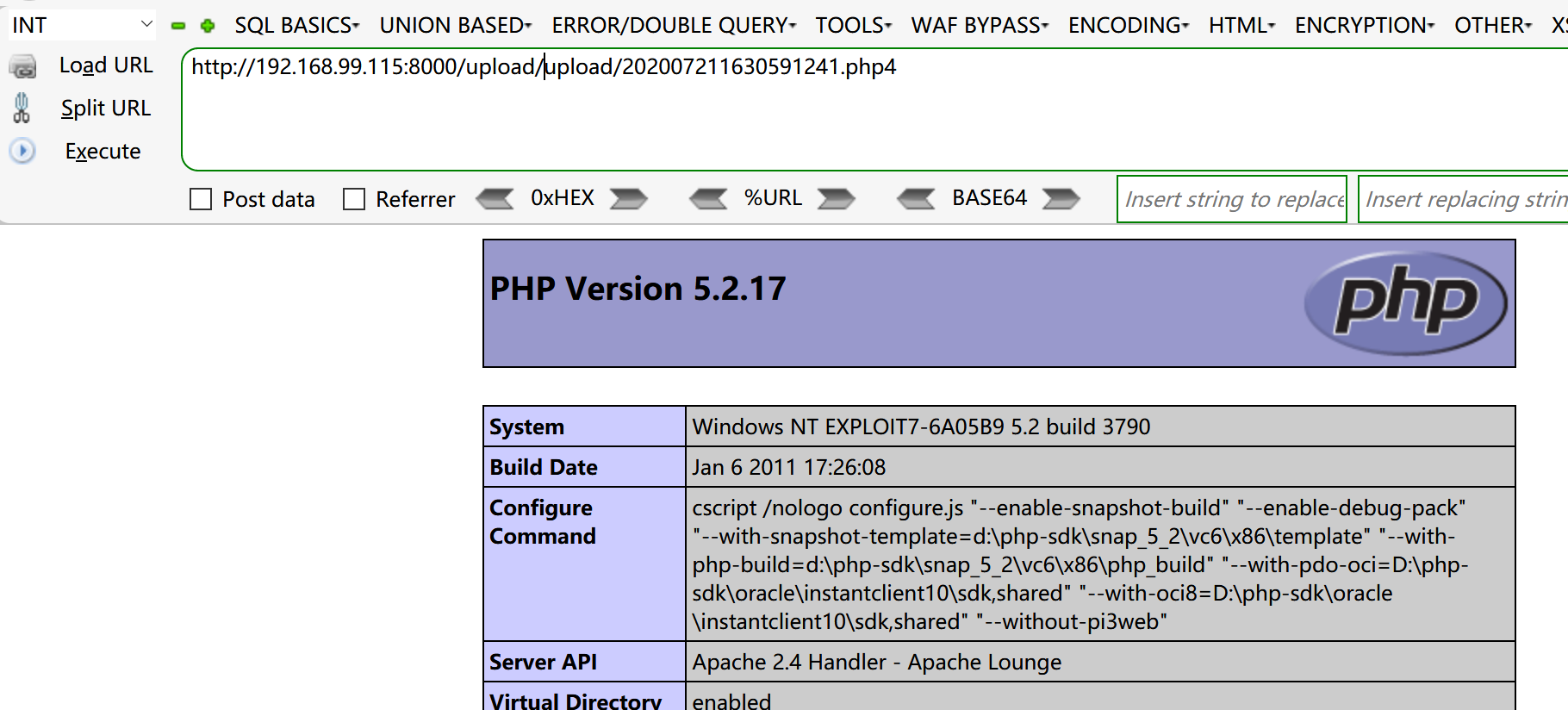
不允许上传.asp,.aspx,.php,.jsp后缀文件，但是可以上传其他任意后缀。比如说:.phtml .phps .php5 .pht，但如果上传的是.php5这种类型文件的话，如果想要被当成php执行的话，需要有个前提条件，即Apache的httpd.conf有如关于AddType命令的作用解释如下

AddType 指令  
作用：在给定的文件扩展名与特定的内容类型之间建立映射  
语法：AddType MIME-type extension [extension] ...  
AddType指令在给定的文件扩展名与特定的内容类型之间建立映射关系。MIME-type指明了包含extension扩展名的文件的媒体类型。  
AddType 是与类型表相关的，描述的是扩展名与文件类型之间的关系。



发现是黑名单判断，于是尝试用php3,phtml绕过





此处黑名单没有过滤.htaccess后缀，故此处也可上传.htaccess文件进行绕过。  
*注: .htaccess文件生效前提条件为1.mod\_rewrite模块开启。2.AllowOverride All*

.htaccess文件是Apache服务器中的一个配置文件，它负责相关目录下的网页配置。通过htaccess文件，可以实现：网页301重定向、自定义404错误页面、改变文件扩展名、允许/阻止特定的用户或者目录的访问、禁止目录列表、配置默认文档等功能IIS平台上不存在该文件，该文件默认开启，启用和关闭在httpd.conf文件中配置。

构造.htaccess文件，内容如下:AddType application/x-httpd-php .jpg  
这里代码的意思可以让 .jpg后缀名文件格式的文件名以php格式解析，因此达到了可执行的效果。所以我们可以把要上传的php文件的后缀名改为.jpg格式从而绕过