# [.htaccess 文件 在文件上传中的使用](https://www.cnblogs.com/hmbb/p/9689436.html)

 首先让我们来看看什么是.htaccess文件（百度一下）



可以看到这个文件能实现很多功能，其他的功能先不管，我们只需要知道.htaccess文件能够设置服务器解析文件的格式。比如设置 匹配到xxx 就用php的格式来解析。

.htaccess文件(或者”分布式配置文件”）提供了针对目录改变配置的方法，也就是在一个特定的文档目录中放置一个包含一个或多个指令的文件， 以作用于当前目录及其所有子目录。作为用户，所能使用的命令受到限制。（其实每个目录中都可以添加一个这样的文件）

因为.htaccess文件是Apache服务器下的配置文件，所以这里用的还是phpstudy环境。

Apache要使.htaccess文件生效需要在httpd.config 中进行配置。

<Directory />

Options FollowSymLinks

AllowOverride None

</Directory>

改为：

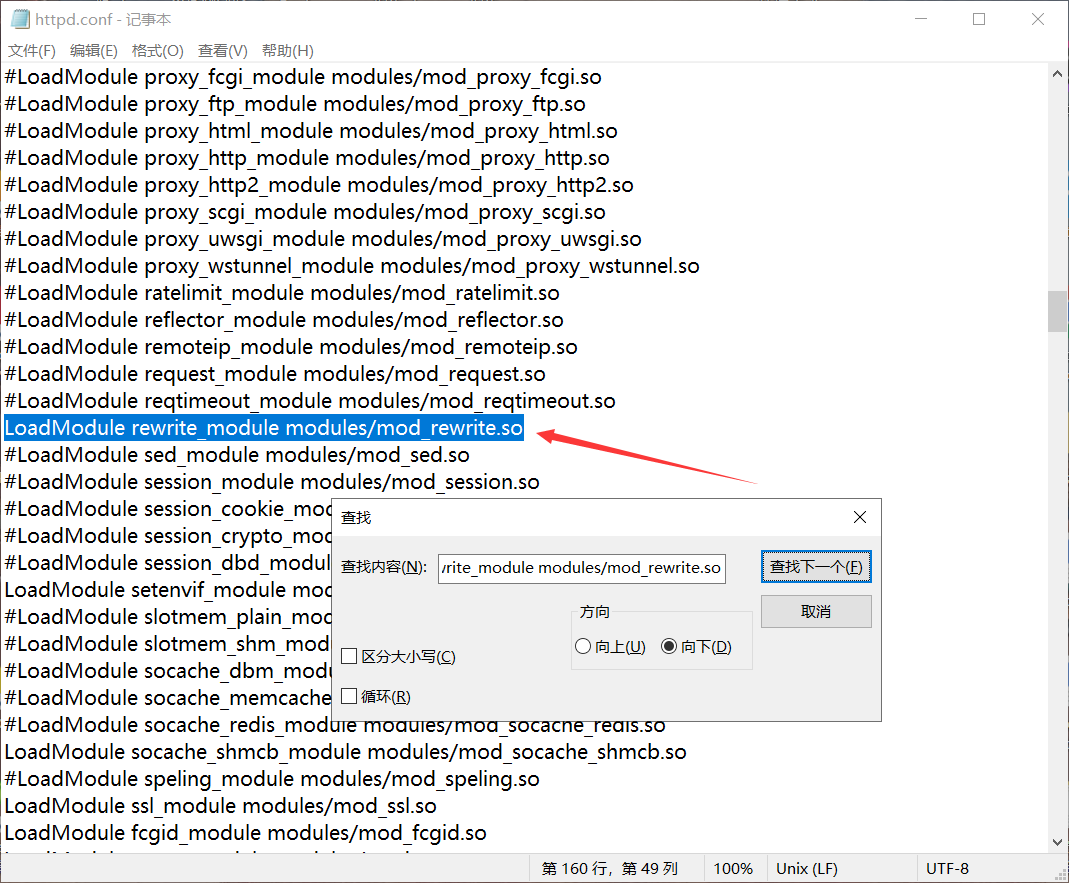
<Directory />

Options FollowSymLinks

AllowOverride All

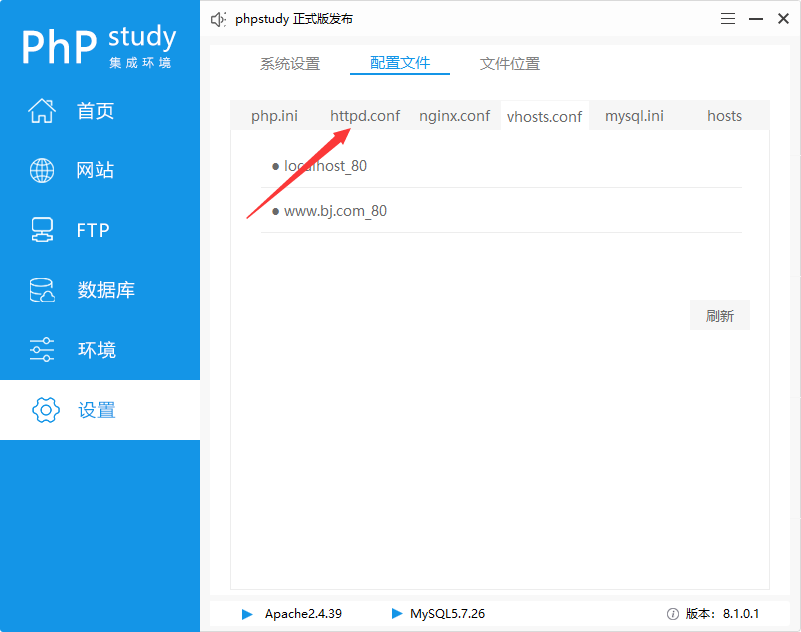
</Directory>

并且还需要将LoadModule rewrite\_module modules/mod\_rewrite.so前面的注释符号#删除。集成环境phpstudy中默认就是启用了的。

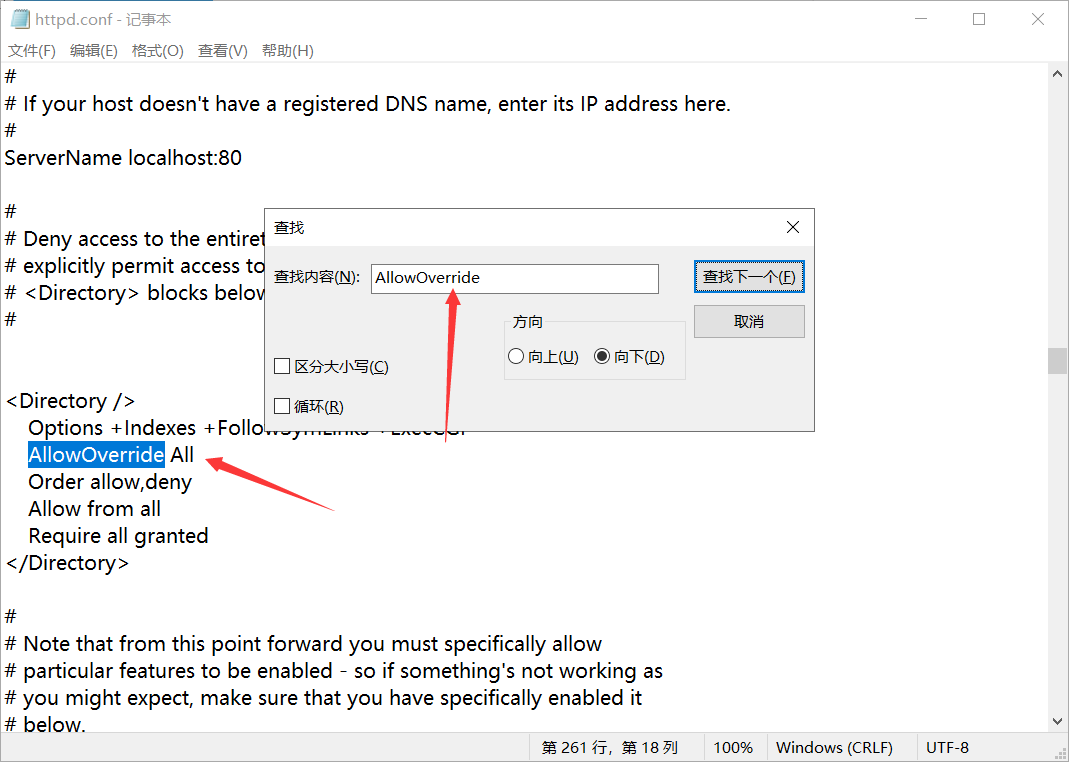


AllowOverride启用了.htaccess文件，则Apache需要在每个目录中查找.htaccess文件。对于每一个请求，都需要读取一次.htaccess文件。

下面先打开phpstudy环境



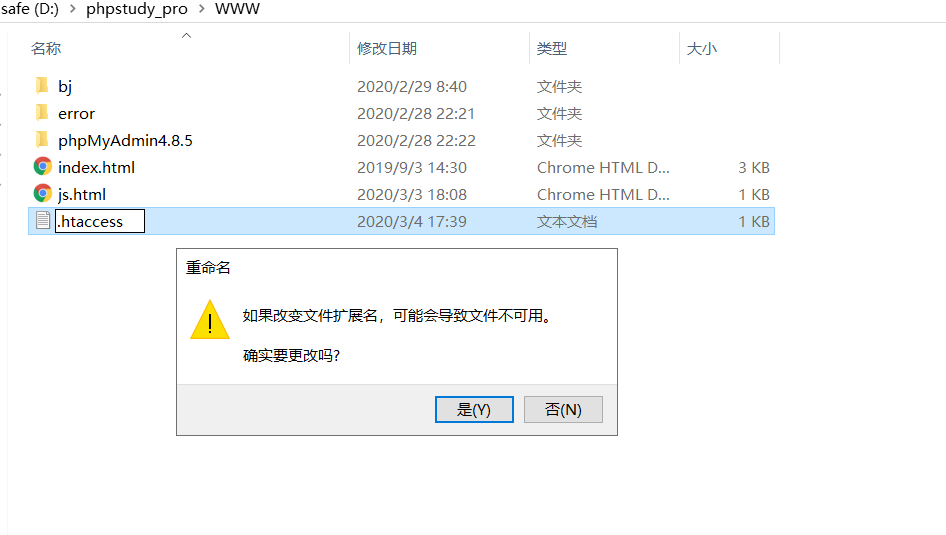
点击图中箭头处可以直接进行修改（小技巧：打开之后直接Ctrl+f可以进行搜索定位）



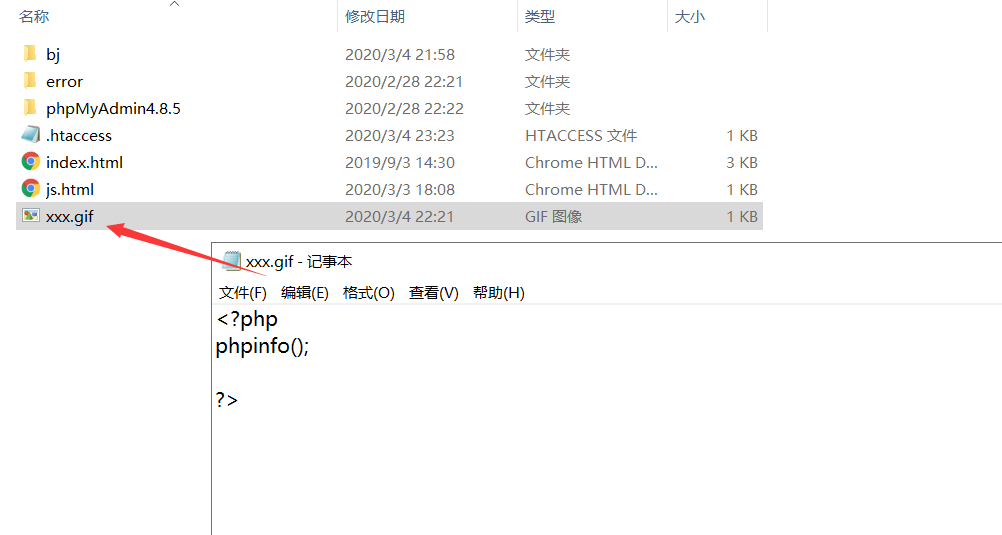
修改完成之后，重启一下服务器。然后在www目录中写入一个.htaccess文件



保存后记得重命名一下

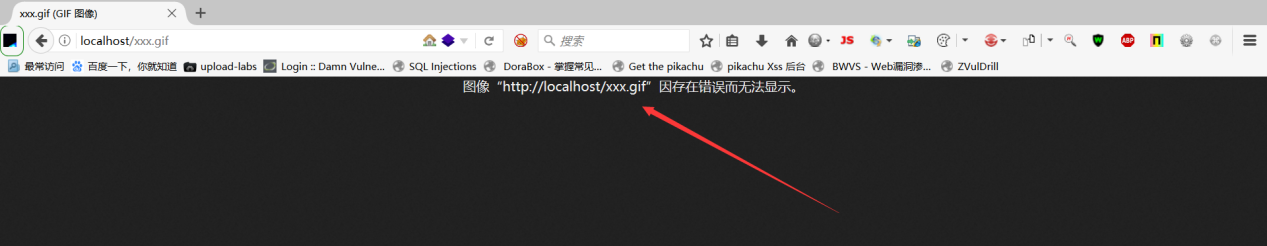


这里写入配置的意思是当匹配到文件名中含有xxx的字符时就以php形式去解析该文件。所以同样在www目录中写一个文件名含有xxx的文件



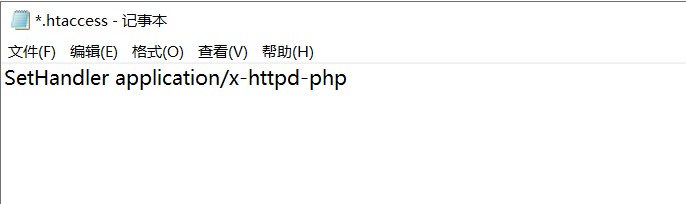
这样在浏览器中访问当前目录下的该文件的时候，服务器会先去读取当前目录下的.htaccess文件。所以会将xxx.gif文件用php的格式进行解析。

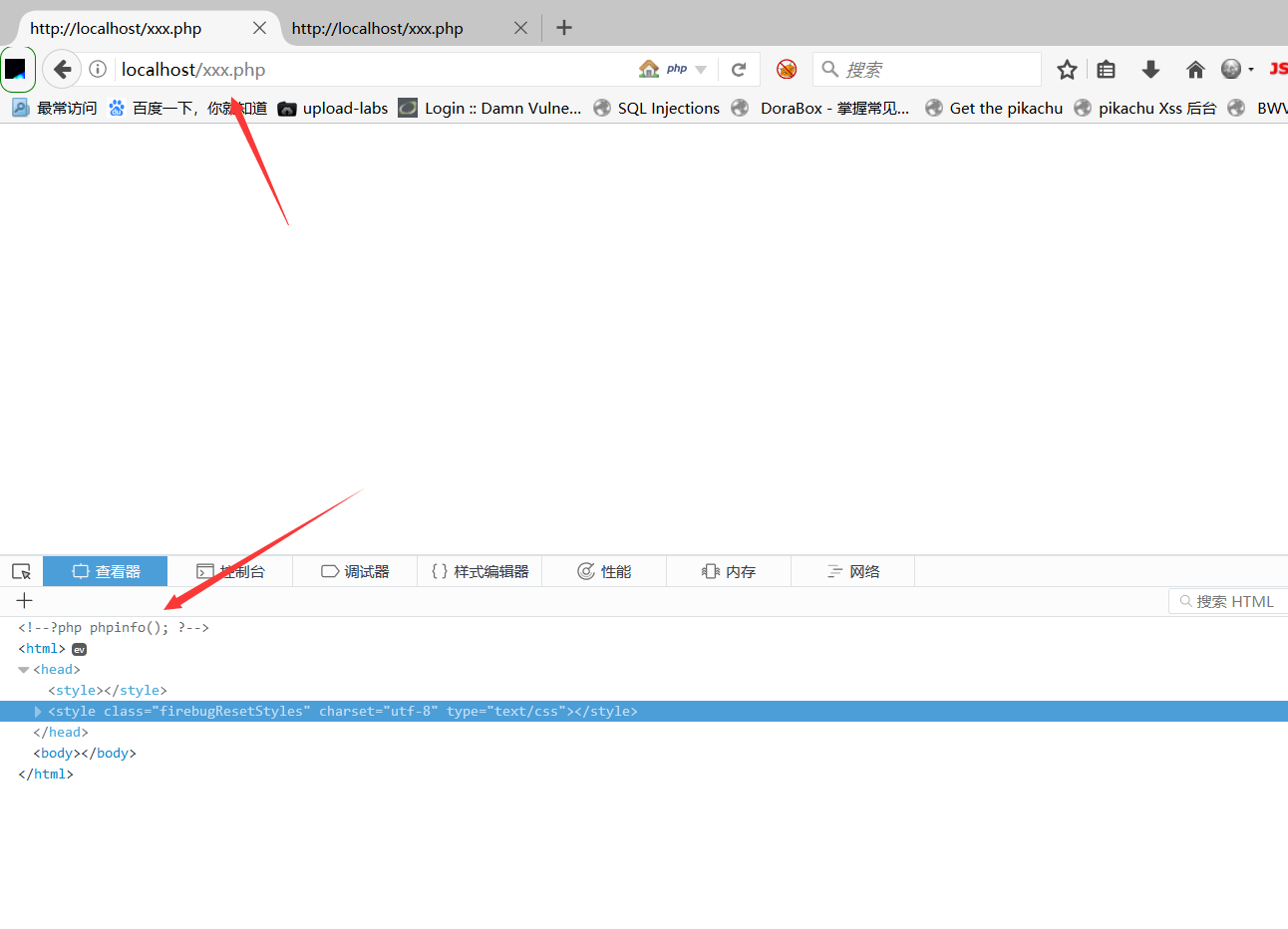
你以为本文到这里就结束了吗？真是too yonug too simple。万万没想到当访问文件时出错了。

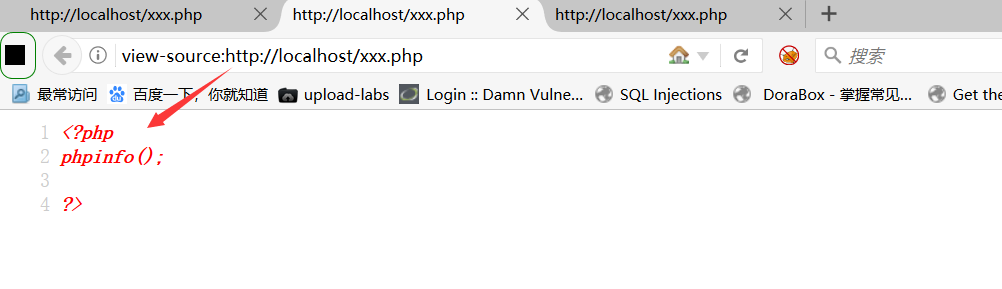


不是说好用php格式进行解析吗，怎么这样了。

接下来就是漫长而艰辛的测试环节了，我先把htaccess文件的配置改为了所有的文件都按照php格式进行解析。

然后访问xxx.gif发现还是一样。于是将后缀名改成原来的php进行访问

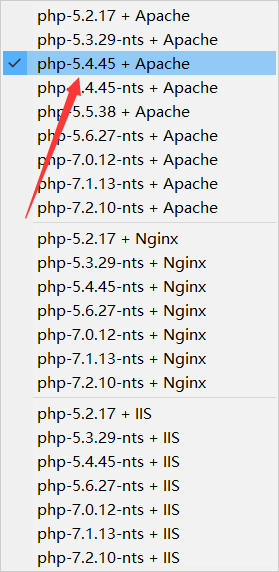




直接连php文件都无法解析了，在源码中发现不知道怎么已经被放到了注释里面。

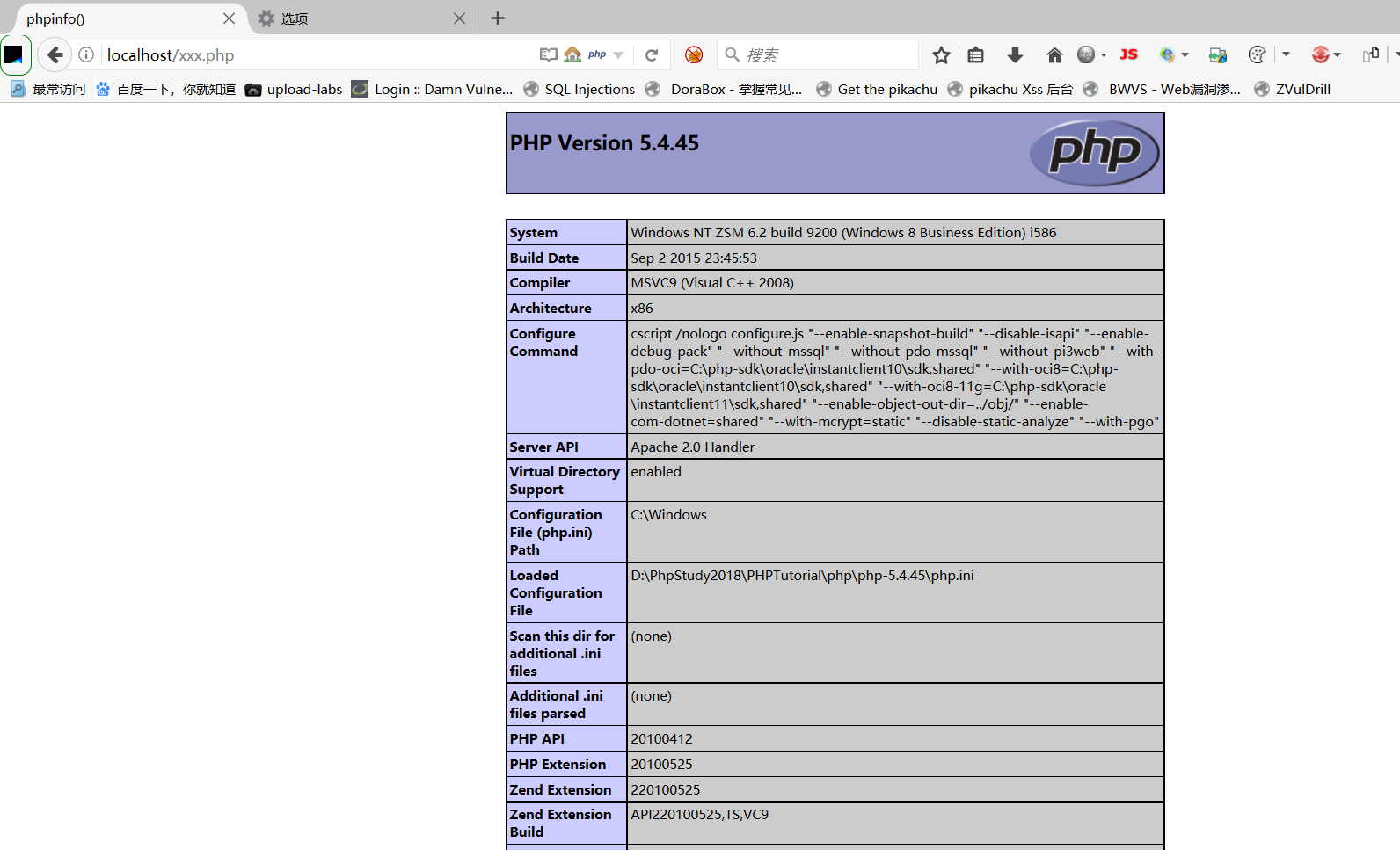
都说有问题问百度，结果搜索三小时测试仍无果，就在想要放弃的时候，在原来的phpstudy版本中实现了复现。最后发现这全都是nts搞的鬼。在新版中php环境默认都是带nts的，而在旧版本中则可以选择不带。接下来看图说话

这里在旧版先选择一个不带nts的PHP环境

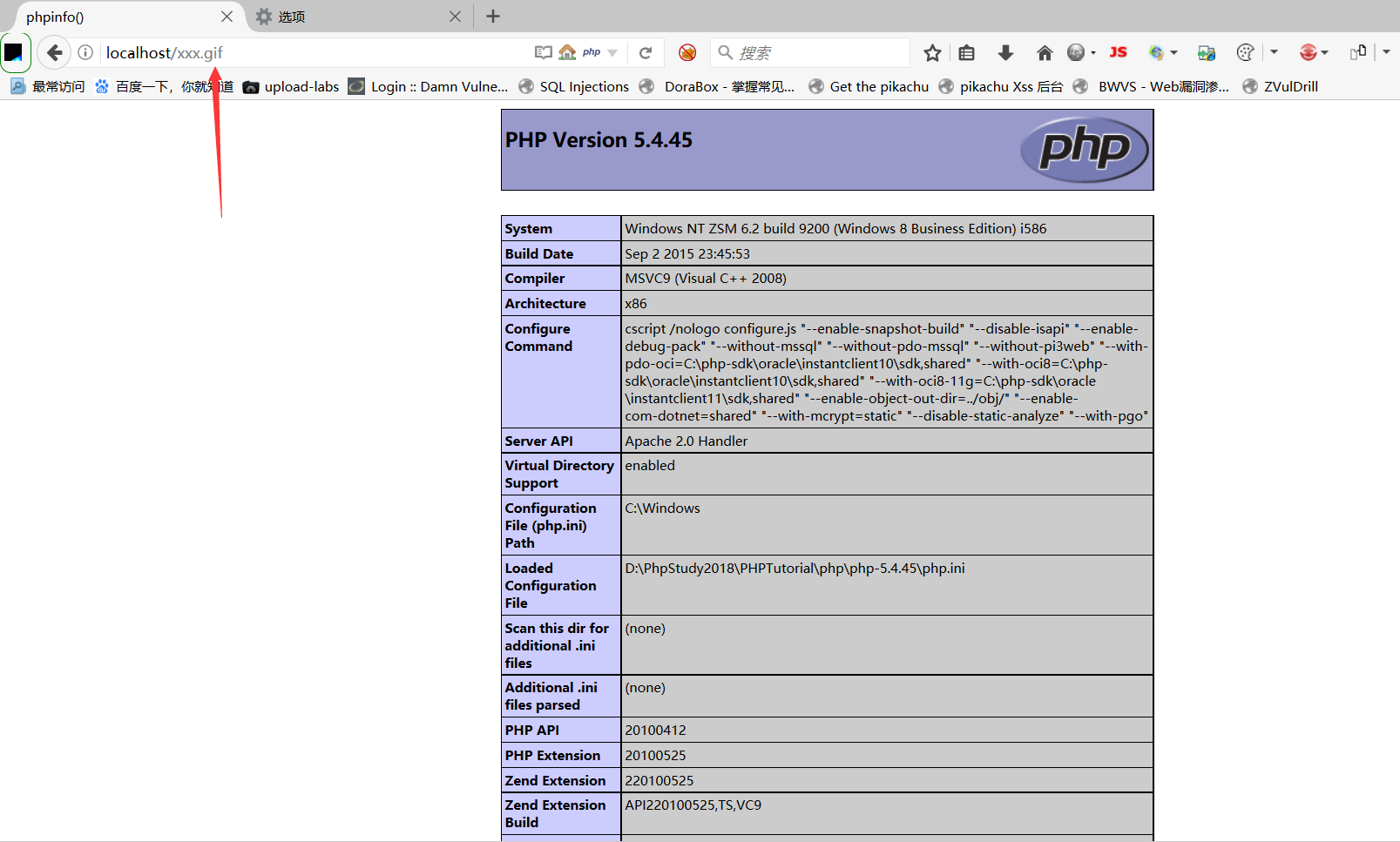


然后继续访问xxx.php

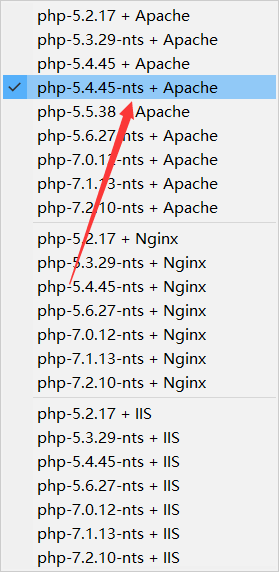
发现成功访问了



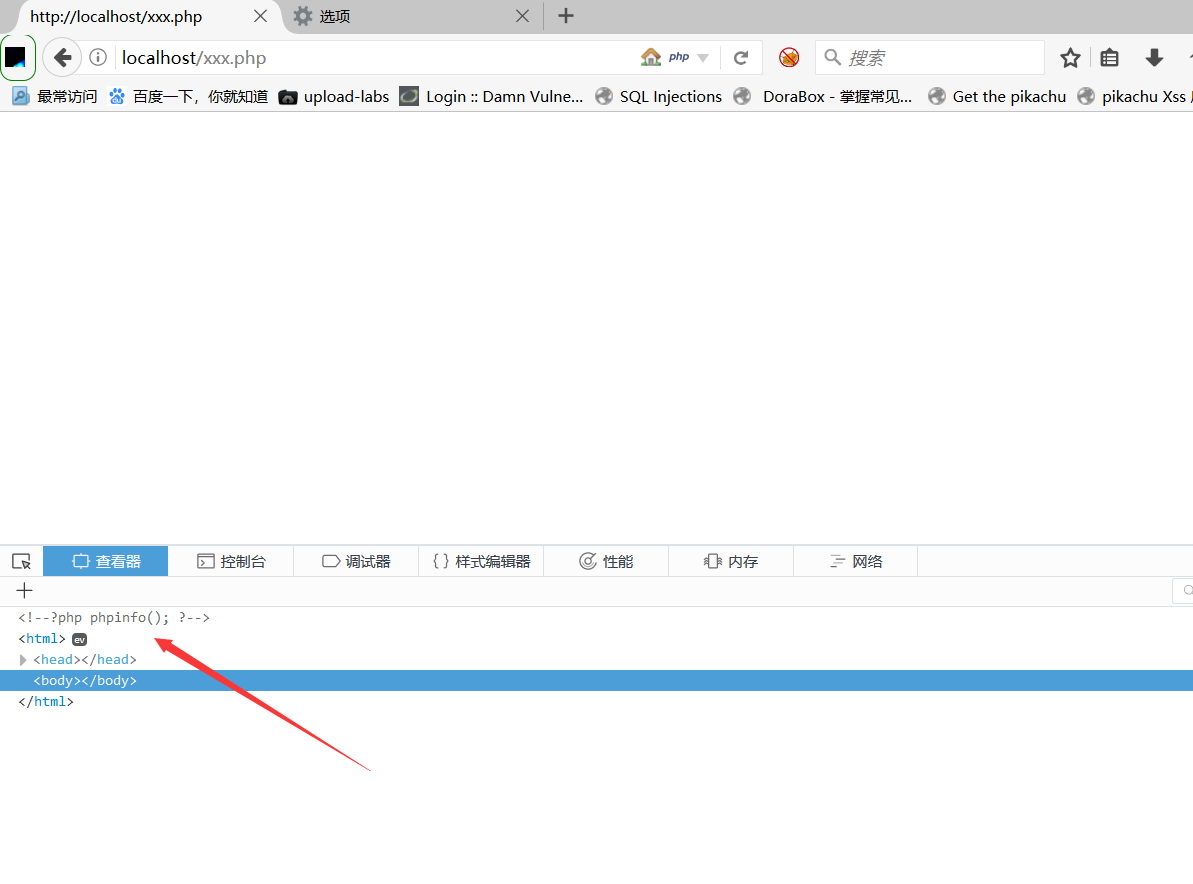
把后缀改为gif再测试发现确实也被解析为php格式了



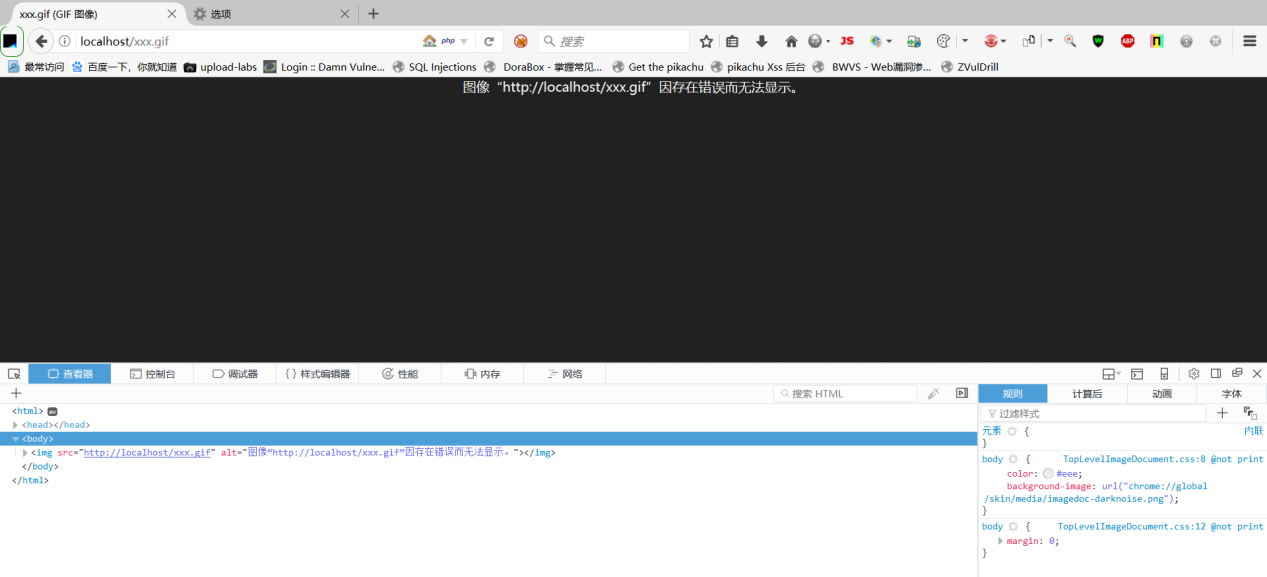
为了证明确实是nts的问题，我们再选择一个带nts的php环境测试



首先访问xxx.php,发现情况如同新版一样



再继续访问xxx.gif，结果一样



测试到此为止，之前复现失败确实是因为nts的原因。至于具体为什么待我下去弄清楚了再发文。今天的主题貌似有些跑偏了，不过个人认为许多初学者在做upload-lads靶场想要复现这个操作的时候，及其有可能遇到跟我一样的事情，借助本文就不需要浪费太多时间来探究问题出在哪里了。

那么言归正传，当apache服务器在上传点处没有限制用户上传.htaccess文件的时候，并开启了.htaccess功能的时候就会出现漏洞。在上传处对shell文件做了一定上传限制却没有限制上传.htaccess文件的时候，恶意攻击者可以先上传一个.htaccess文件，写配置规定将当前目录中的文件的解析方式。这样就可以绕过一些针对文件上传漏洞的防护。具体的操作可以看看另一篇文章《upload-labs pass02-04》。觉得写得不错别忘了双击么么哒！！！