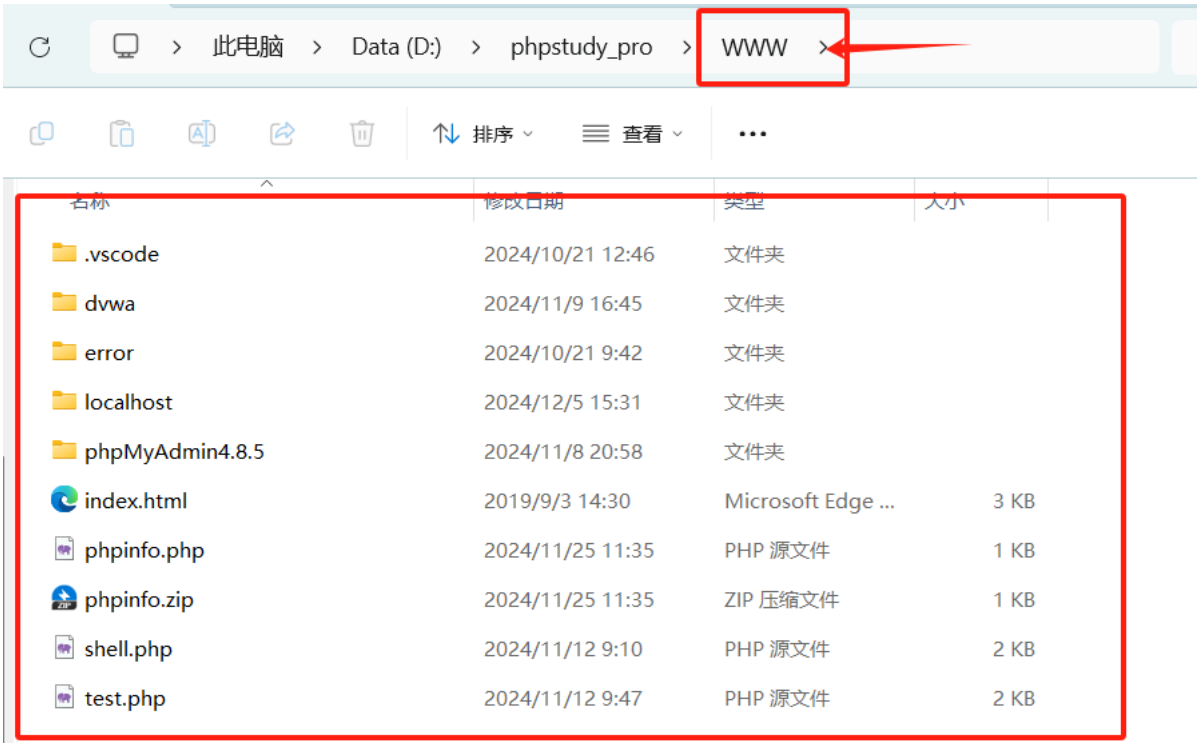
IP和域名

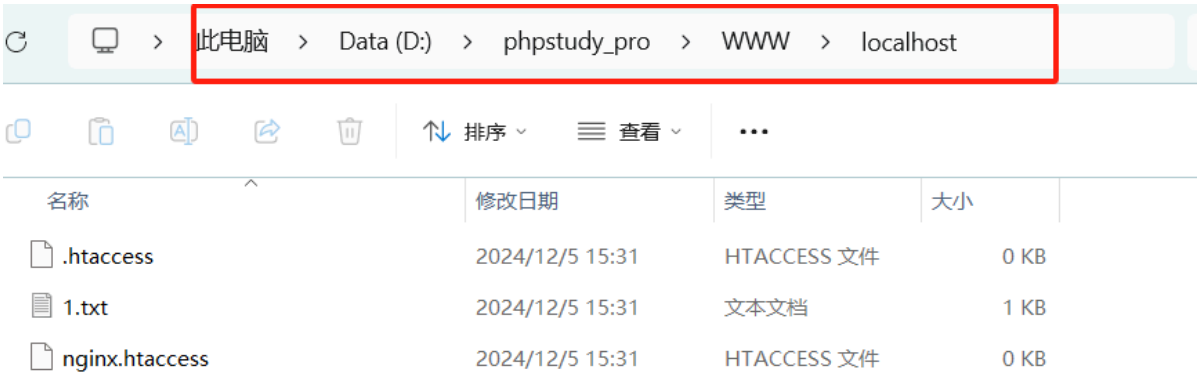
这里就是说通过IP访问和域名访问得到的目录是不一样的

我们在访问本地网站

访问本地网站10.4.14.21 打开的目录是



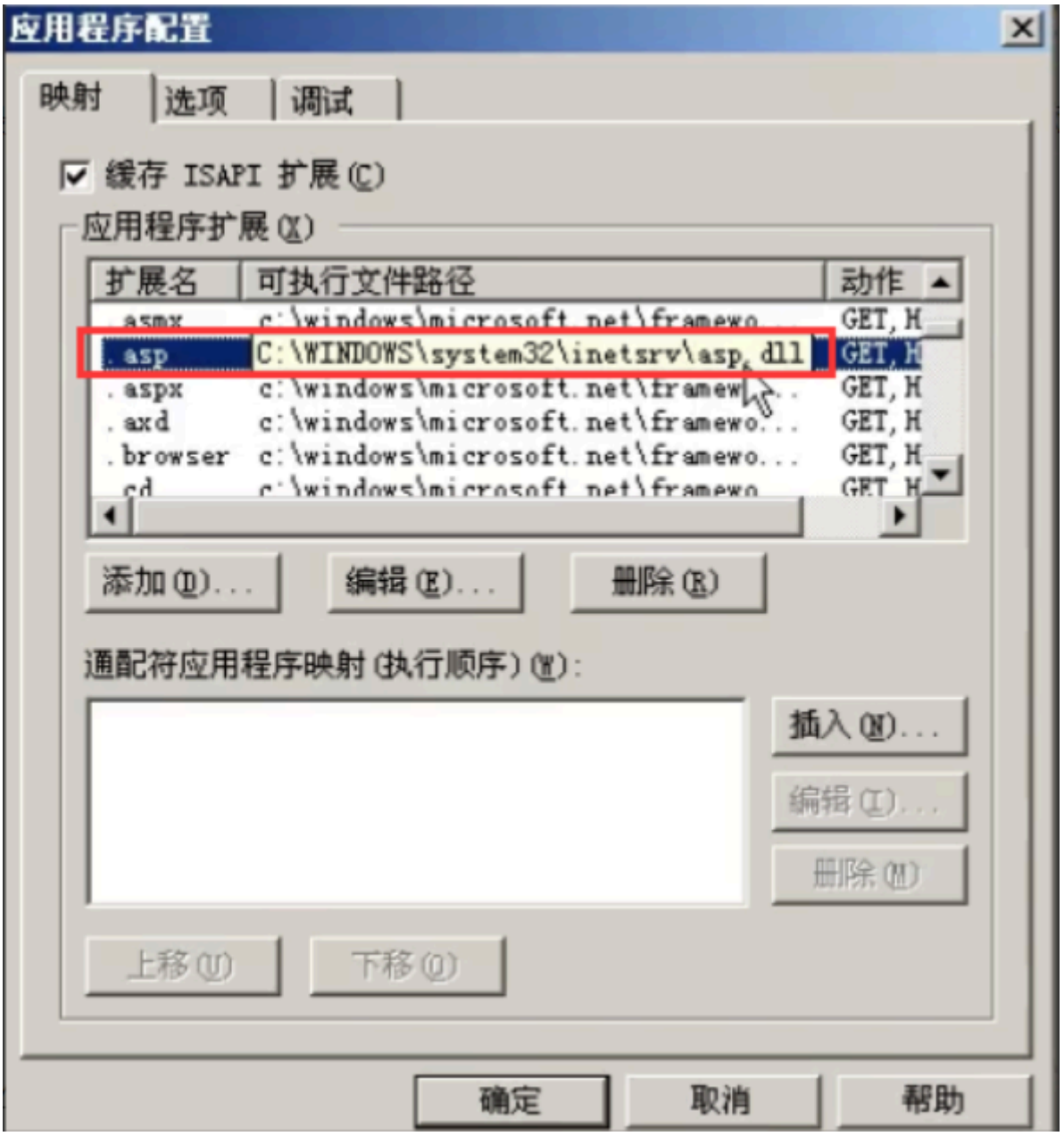
访问域名test.com,访问的目录是WWW/localhost



这就是IP访问和域名访问的区别，有些网站就是这样的设置的，把网站源码放在域名目录下

常见文件后缀解析对应安全

如果网站中间件是ASP，网站解析asp后缀名文件，原因是在应用程序扩展里，asp扩展名对应了asp.dll可执行文件。



这样的话我们可以自定义一个拓展名，如果其他后缀名文件也对应asp.dll可执行文件的话，那么网站默认也会以解析asp文件的方式解析该文件。这样就会造成漏洞。

在视频中的实验是 将拓展名xiaodi8,解析为asp.dll。在网站目录下创建新文件x.xiaodi8。写入asp一句话木马，浏览器访问，用菜刀连接，拿到shell权限

基于中间件的靶场使用

在vulhub靶场中学习