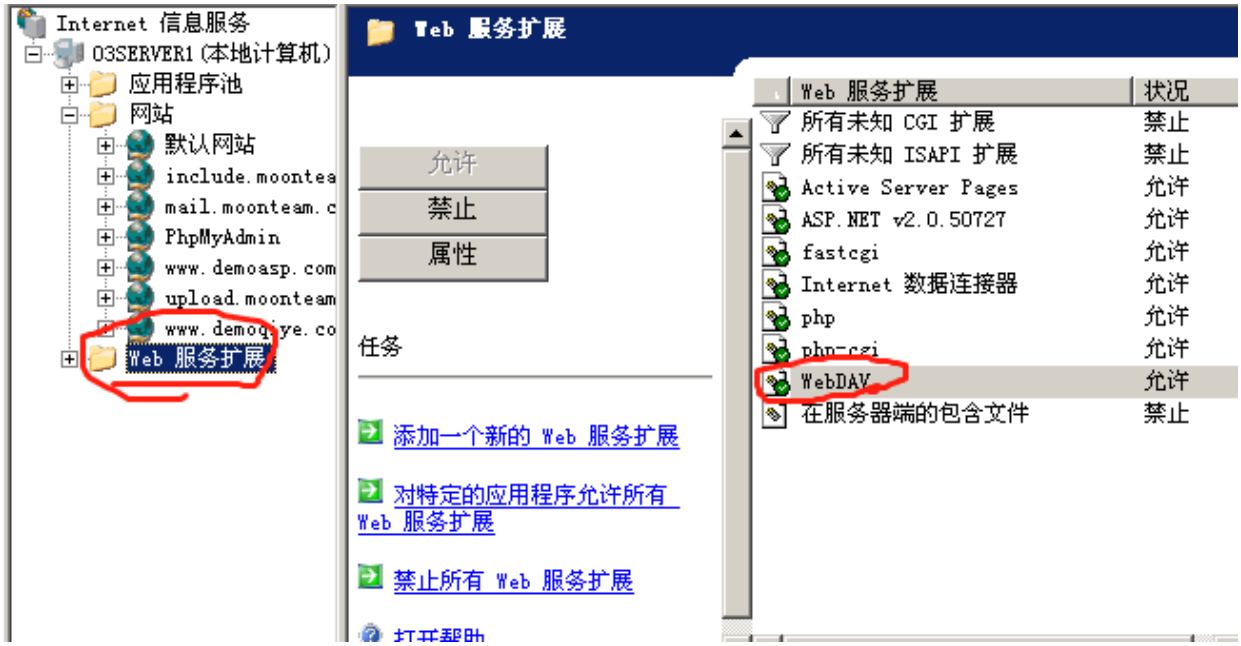
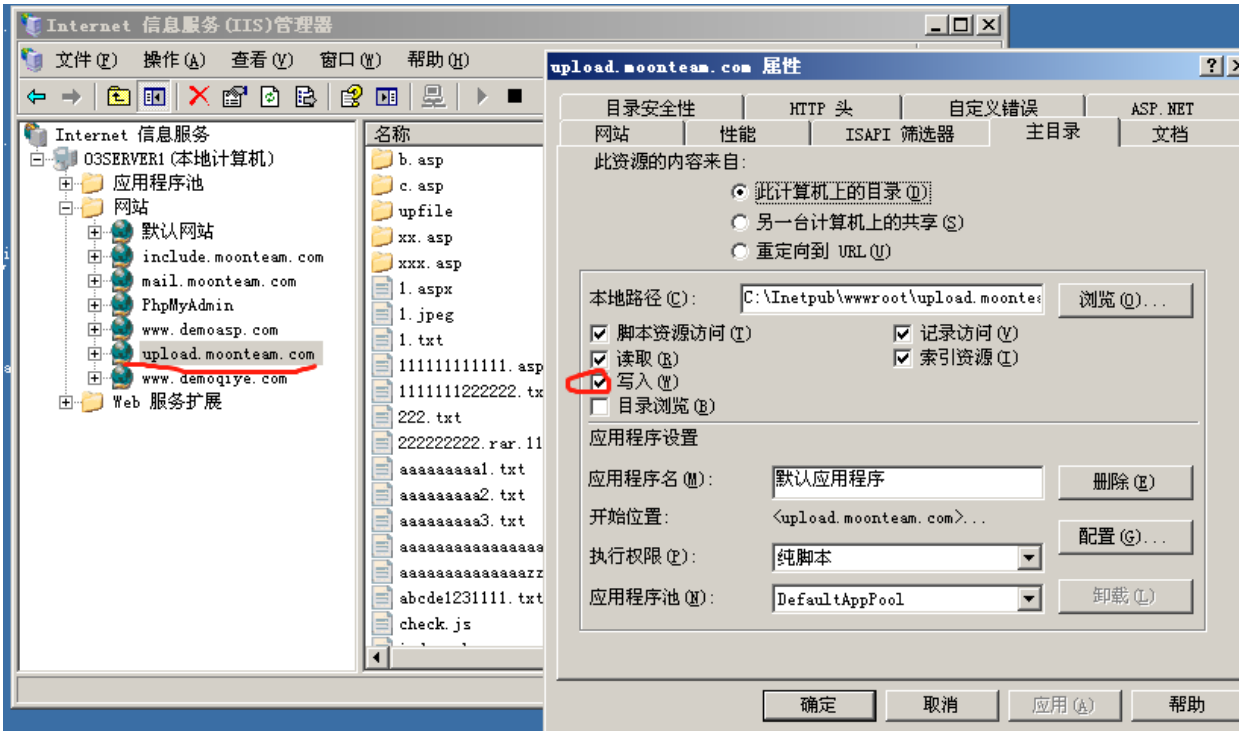
IIS6.0 PUT漏洞任意文件上传

前提条件：

1. 开启Webdav



2. 对应网站开启写权限



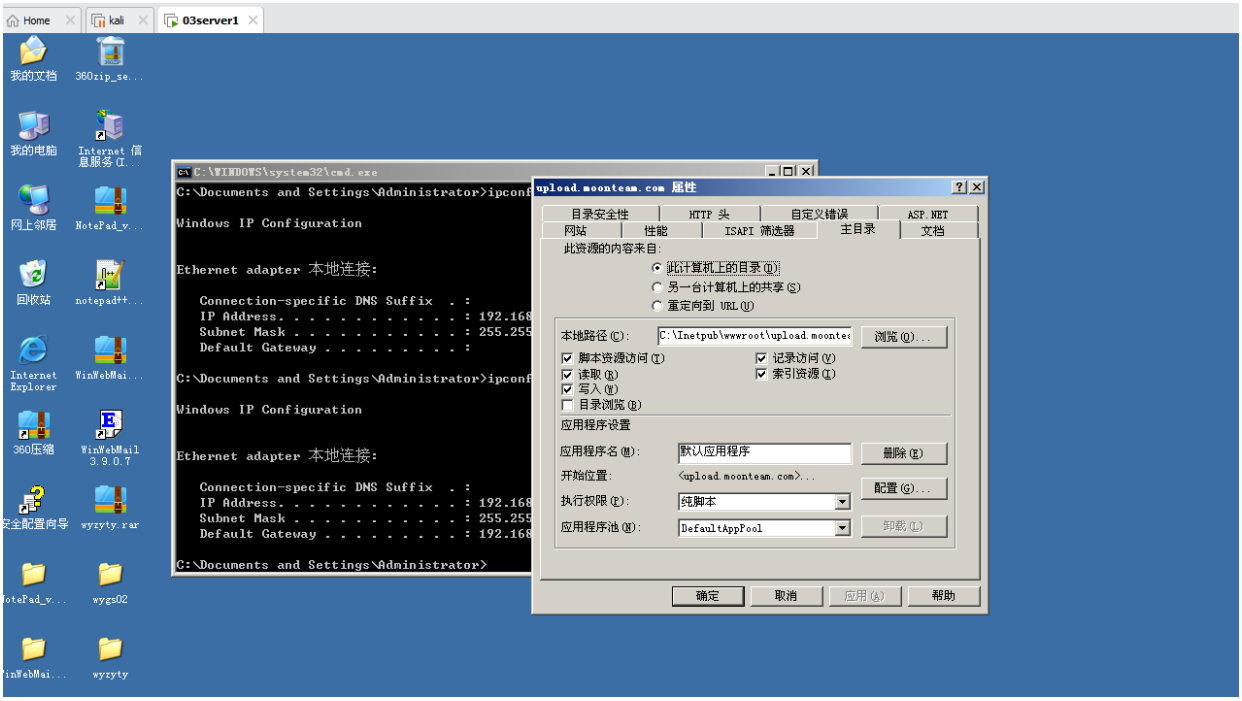
PS: 什么是webdav？ 简单来说就是提供网站并发和其它功能的extensions，需要开启它才能确保网站是可读/可写的而不是read-only。

WebDAV (**Web Distributed Authoring and Versioning**) is a set of extensions to the Hypertext Transfer Protocol (HTTP), which allows user agents to collaboratively author contents *directly* in an HTTP web server by providing facilities for concurrency control and namespace operations, thus allowing Web to be viewed as a *writeable*,

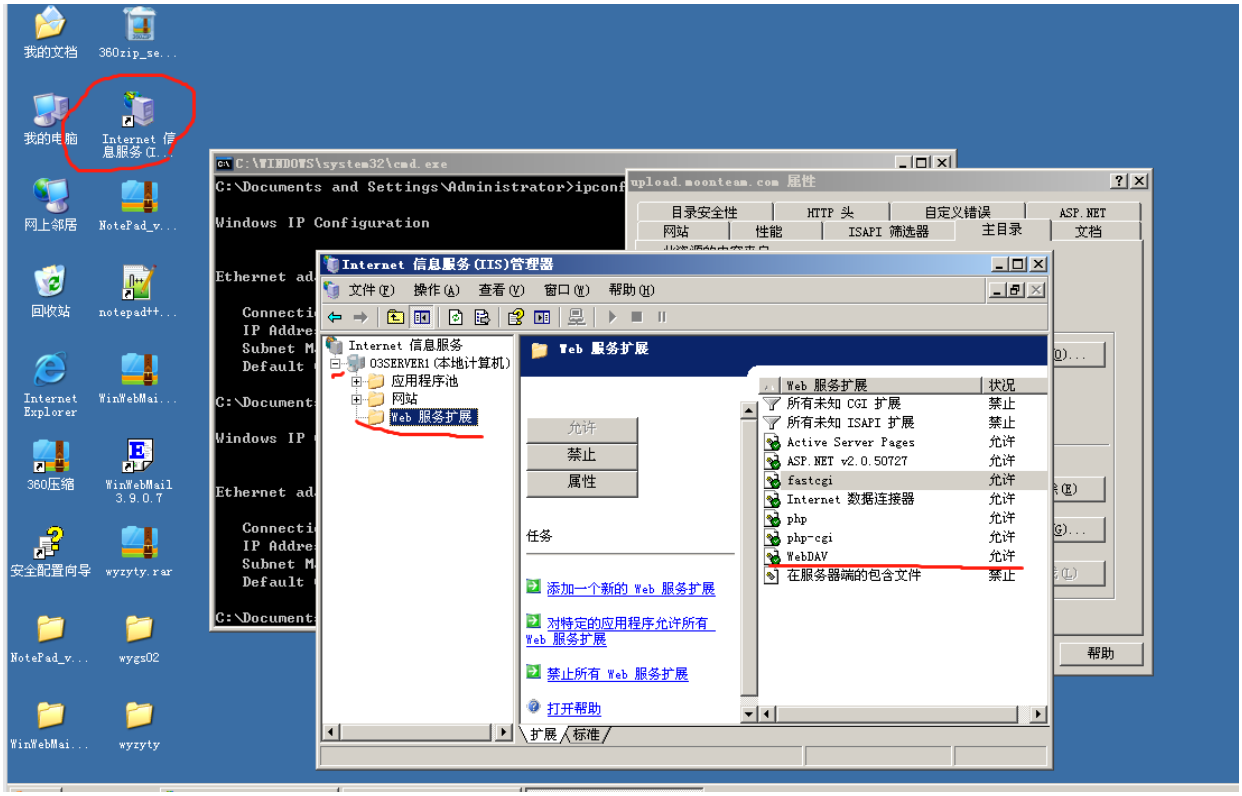
collaborative medium and not just a read-only medium.1(https://en.wikipedia.org/wiki/WebDAV#cite_note-FOOTNOTEWhiteheadGoland1999293-1) WebDAV is defined in RFC 4918 by a working group of the Internet Engineering Task Force (IETF).2(https://en.wikipedia.org/wiki/WebDAV#cite_note-FOOTNOTEWhitehead199834-2)
ref：https://en.wikipedia.org/wiki/WebDAV

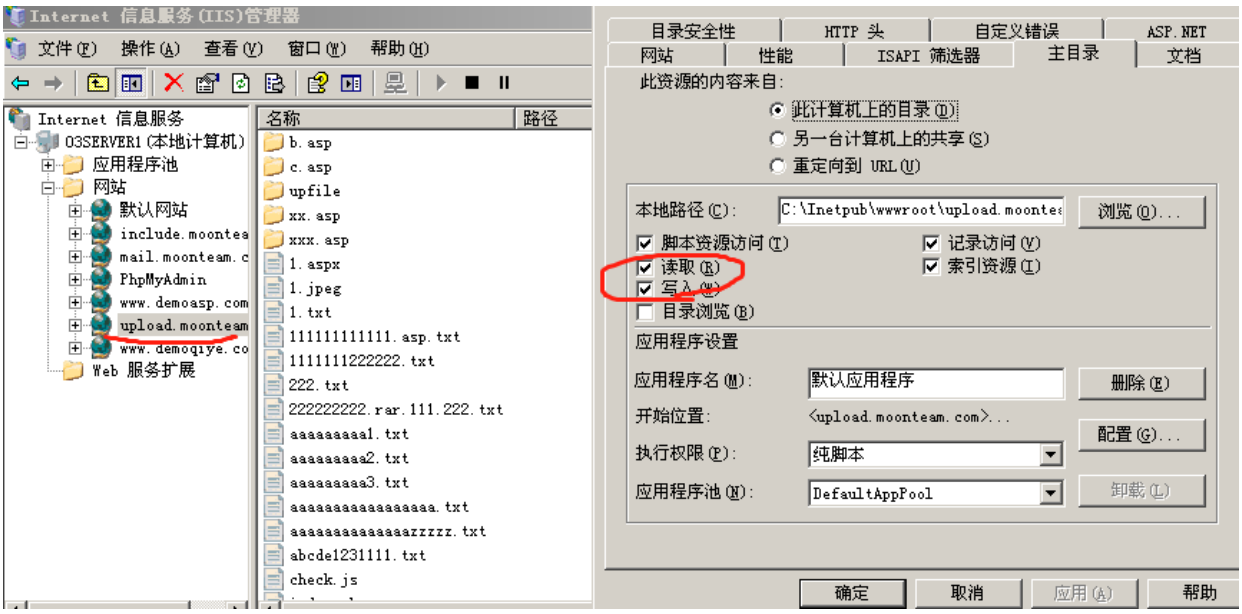
漏洞复现详细过程

1. 下载安装Windows server 2003虚拟机。

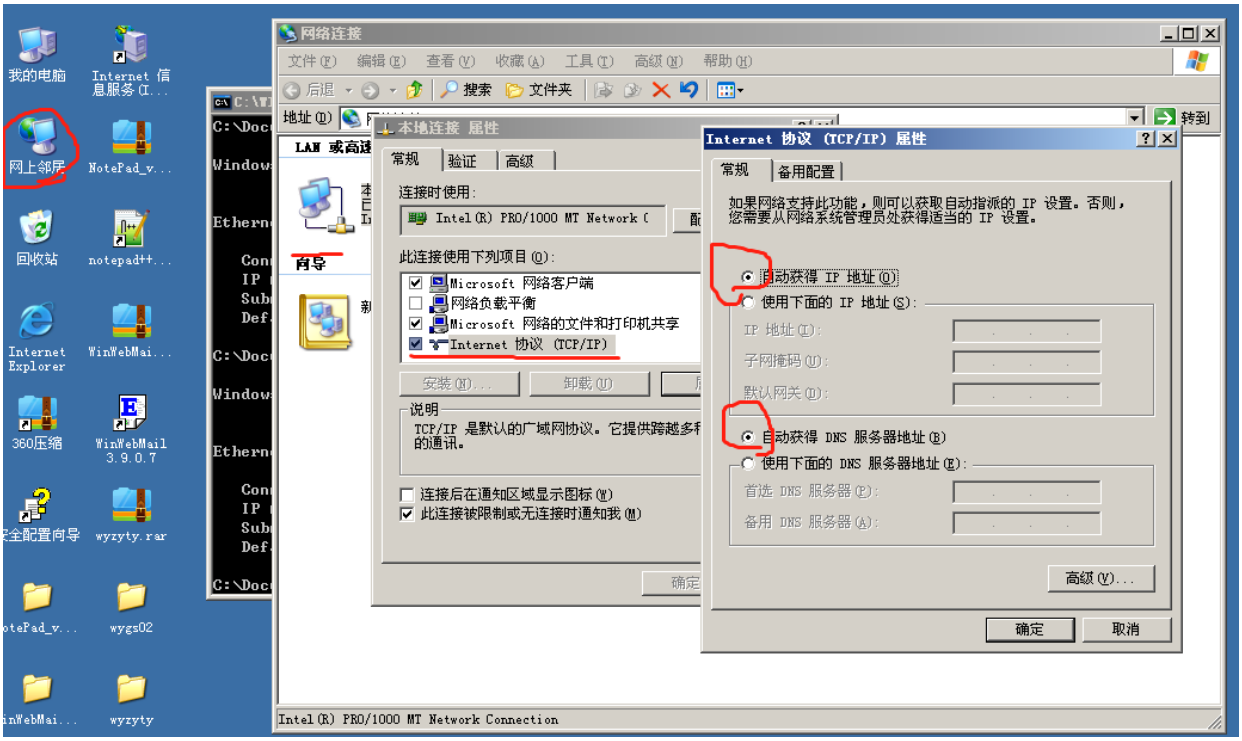


2. 查看是否开启webdav，对应网站是否都开启了读/写功能





3. 查看虚拟机ip（需要和本机在同一subnet，如果绑定了ip务必注意），**本机**修改对应 hosts 。



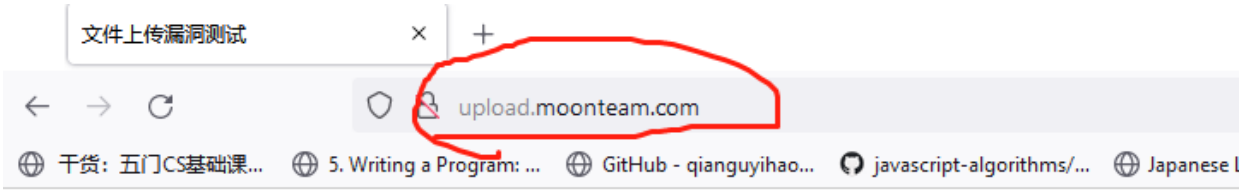

```
Ethernet adapter 本地连接:

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 192.168.50.234
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.50.1

C:\Documents and Settings\Administrator>a
```

hosts - Notepad

File Edit Format View Help

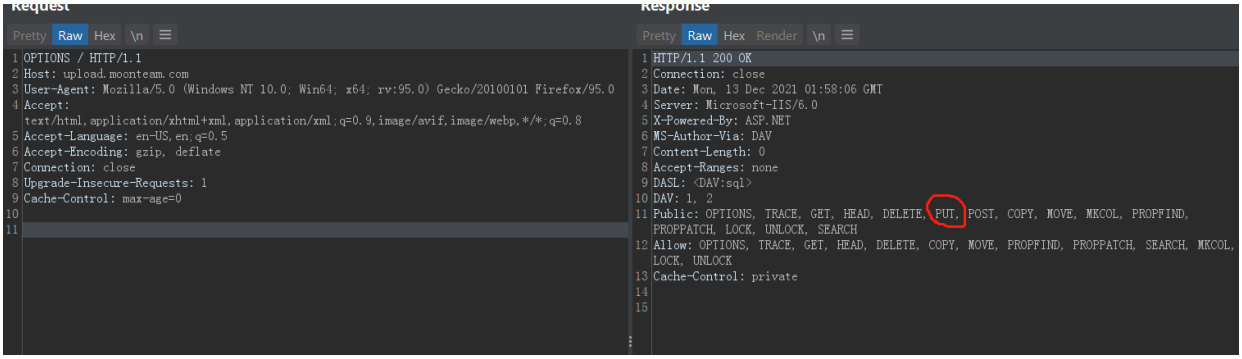
```
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#               127.0.0.1       localhost
#               ::1             localhost
# Added by Docker Desktop
192.168.50.147 host.docker.internal
192.168.50.147 gateway.docker.internal
# To allow the same kube context to work on the host and the container:
127.0.0.1 kubernetes.docker.internal
# End of section
192.168.50.234 upload.moonteam.com
```

4. 都改好后查看能否访问

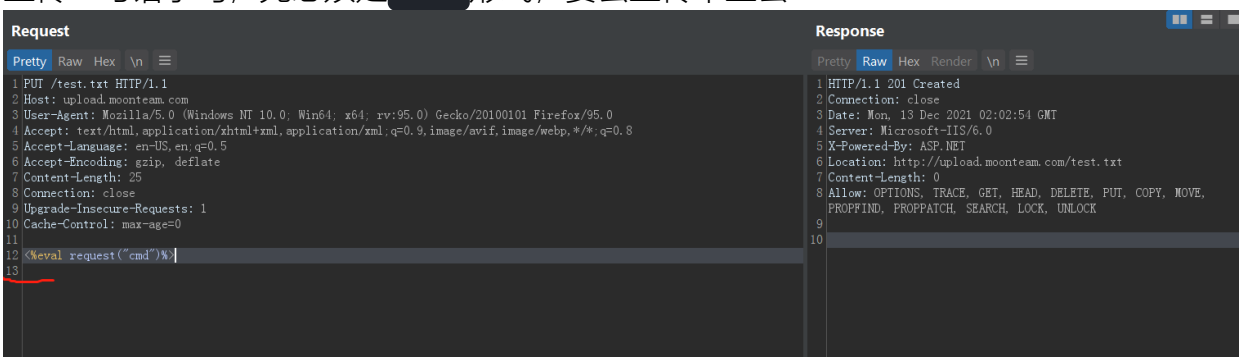


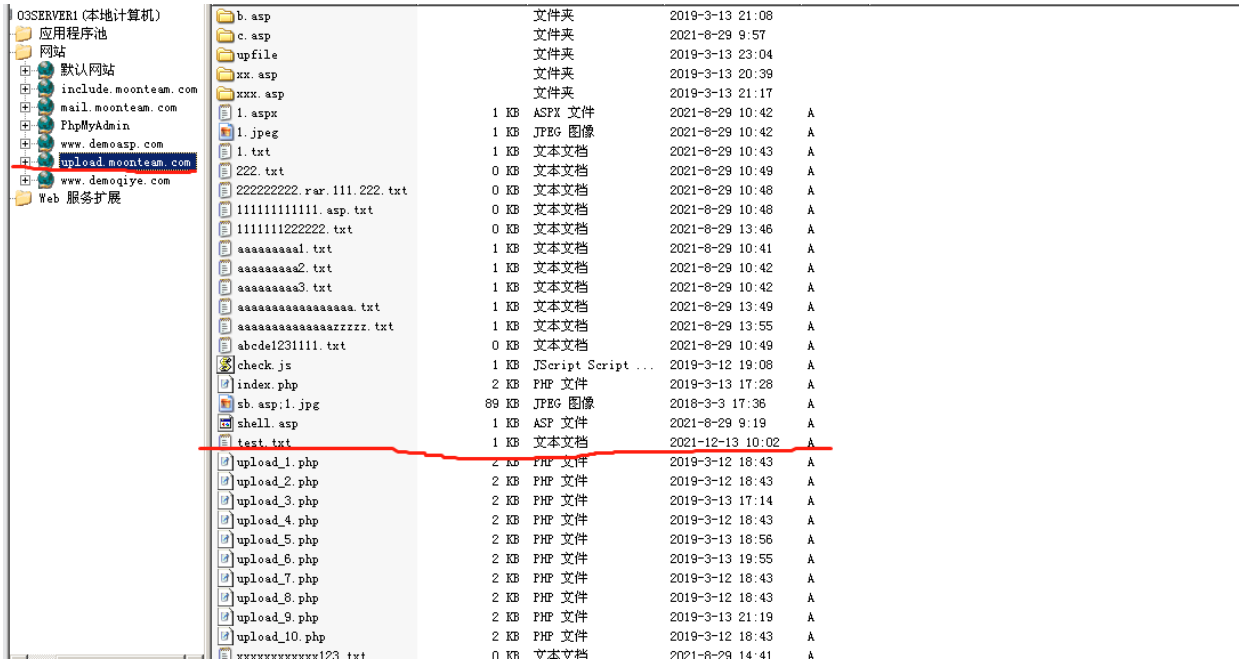
1. 文件名未做任何限制
2. 客户端JS验证绕过突破上传
3. 黑白名单绕过
4. content-type检测
5. 文件头检测突破上传
6. iis6.0解析漏洞
7. 目录解析漏洞
8. 重写解析漏洞
9. %00截断三种场景
10. 系统特性突破上传

5. burp首页抓包，**OPTIONS**看看http request method是否支持PUT。

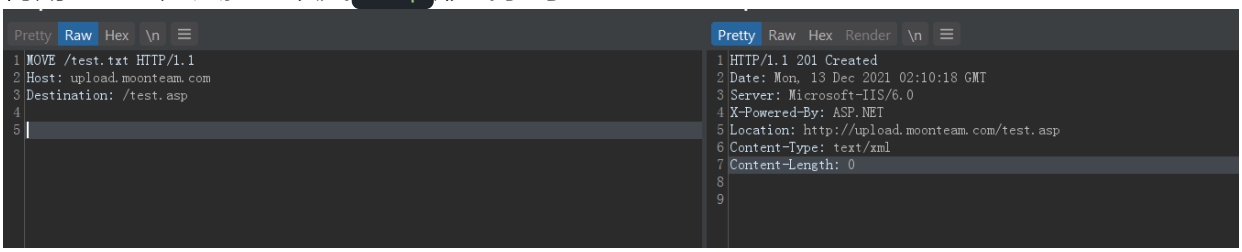


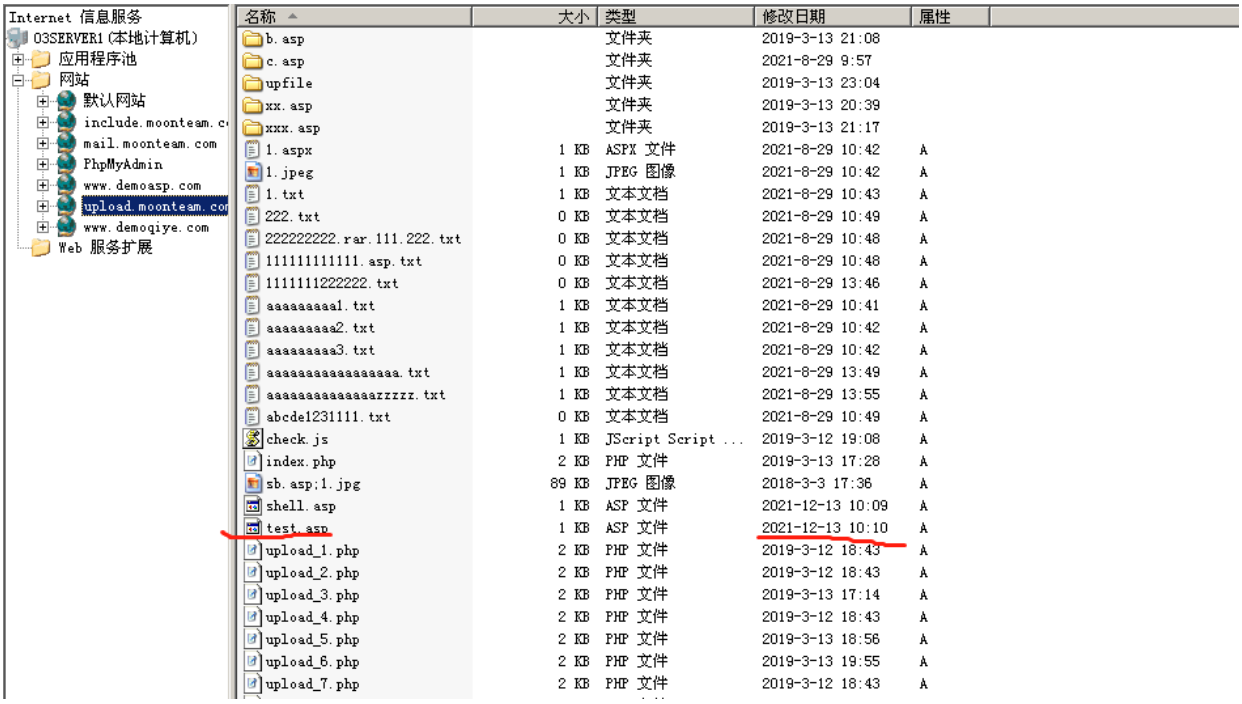
6. 上传一句话小马，先必须是`.txt`形式，要么上传不上去





7. 再用MOVE方法把它改成`.asp`形式小马





8. 访问，可以用菜刀之类的连上这个小马：