目标站我就不发了！  
习惯性的用工具扫描可以利用的信息！  
得到  
   
  
有默认后台！有editor目录！但是木有找到有用的东西！  
木有办法！只能去旁站碰碰运气了！  
找到了一个net的站！试了试fckeditor  
[http://www.xxx.net/fckeditor/editor/filemanager//upload/test.html](http://www.xxx.net/fckeditor/editor/filemanager/upload/test.html)  
人品还不错！直接上传了一个一句话！倒也木有过滤！  
我传了个大马上去！

|  |  |  |
| --- | --- | --- |
| Scripting.FileSystemObject | √ | 文 件 操 作 组 件 |
| wscript.shell | × | 命令行执行组件,显示'×'时用 执行Cmd二 此功能执行 |
| ADOX.Catalog | √ | ACCESS 建 库 组 件 |
| JRO.JetEngine | √ | ACCESS 压 缩 组 件 |
| Scripting.Dictionary | √ | 数据流 上 传 辅助 组件 |
| Adodb.connection | √ | 数据库 连接 组件 |
| Adodb.Stream | √ | 数据流 上传 组件 |
| SoftArtisans.FileUp | × | SA-FileUp 文件 上传 组件 |
| LyfUpload.UploadFile | × | 刘云峰 文件 上传 组件 |
| Persits.Upload.1 | × | ASPUpload 文件 上传 组件 |
| JMail.SmtpMail | √ | JMail 邮件 收发 组件 |
| CDONTS.NewMail | × | 虚拟SMTP 发信 组件 |
| SmtpMail.SmtpMail.1 | × | SmtpMail 发信 组件 |
| Microsoft.XMLHTTP | √ | 数据 传输 组件 |
| wscript.shell.1 | × | 如果wsh被禁，可以改用这个组件 |
| WSCRIPT.NETWORK | × | 查看服务器信息的组件，有时可以用来提权 |
| shell.application | × | shell.application 操作，无FSO时操作文件以及执行命令 |
| shell.application.1 | × | shell.application 的别名，无FSO时操作文件以及执行命令 |
| Shell.Users | √ | 删除了net.exe net1.exe的情况下添加用户的组件 |

呵呵！组件全删了！木有办法！传了个aspx马！传完我就纠结了！服务器出错！该程序不可用！我纠结郁闷！  
经过一晚上的郁闷！第二天我登录我的大马！发现网站已经正常！看了下用户组的信息！

|  |  |
| --- | --- |
| AccountType | 512 |
| Caption | KJWX-HOST\0436dj |
| Description | AutoHost创建的用于建匿名访问 Internet 信息服务的帐户 |
| Disabled | False |
| Domain | KJWX-HOST |
| FullName | Internet 来宾和FTP帐户  //重点 |
| InstallDate |  |
| LocalAccount | True |
| Lockout | False |
| Name | 0436dj |
| PasswordChangeable | False |
| PasswordExpires | False |
| PasswordRequired | True |
| SID | S-1-5-21-420698832-2239331177-446498532-1691 |
| SIDType | 1 |
| Status | OK |

呵呵！iis的账号是ftp账号！我喜欢！  
   
  
呵呵！拿到ftp！拿我需要的东西！呵呵！  
  
检测至此结束！木有进行服务器提权！懒得提了！拿了木有用！不抓鸡！不嗅探！纯属路过！纠结！看到却步我就纠结