

Table of Contents

Front page	1
Table of Contents	2
Introduction	3
Vulnerability details	4
Executive Summary	5
Identified Ports and Services	6
Information Gathered	7
Banners identified	8
Overall Summary	9

Introduction

This report is the result of an "online vulnerability assessment scan", performed using the "**SecPoint® Penetrator**".

This document has been compiled and arranged to provide a quick and easy-to-understand report to simplify the task of securing computer systems and IT equipment connected to the Internet.

System vulnerabilities are categorised under one of three headings: High risk, Medium risk or Low risk.

A detailed explanation of each category of vulnerability can be found under the heading of "**Vulnerability Details**".

An **Executive Summary** has been compiled specifically for a management level review. This summary contains both written and graphic details based upon the results of the scanner. These results include such information as "when the scan was performed", "who performed the scan", and the amount of system vulnerabilities found in each category.

The **Executive Summary** also includes a conclusion reporting the "overall security level" of the tested system.

Details and names of vulnerabilities discovered are found under the heading of "**Overall Summary**". This is followed by individual descriptions for fixing each found vulnerability.

Where possible, a **Bugtraq ID** and/or **CVE** is present verifying the existence of the discovered vulnerabilities.

Bugtraq ID is the official **Securityfocus.com** ID; Also known as bugtraq.

CVE is the official **CVE Mitre** list.

Every system vulnerability discovered is supplied with a possible remedy.

Vulnerability details

Vulnerabilities categorised

High Risk Vulnerability Information

When a high risk vulnerability is identified, it means that it is possible for an intruder to penetrate and compromise the system fully and/or gain access to highly sensitive system information. This in turn could lead to theft or loss of private and sensitive data.

Medium Risk Vulnerability Information

When a medium Risk vulnerability is identified, it means that an intruder can gain access to system information that could lead to more specific attacks and possibly a full system compromise. This in turn could lead to theft of loss of private or sensitive data.

Low Risk Vulnerability Information

When a low risk vulnerability is identified, it generally means that an intruder can gain access to system information that can aid and lead to more specific attacks resulting in the theft or loss of private and sensitive data.

Executive Summary

General information

Scan was performed for: SecPoint NL

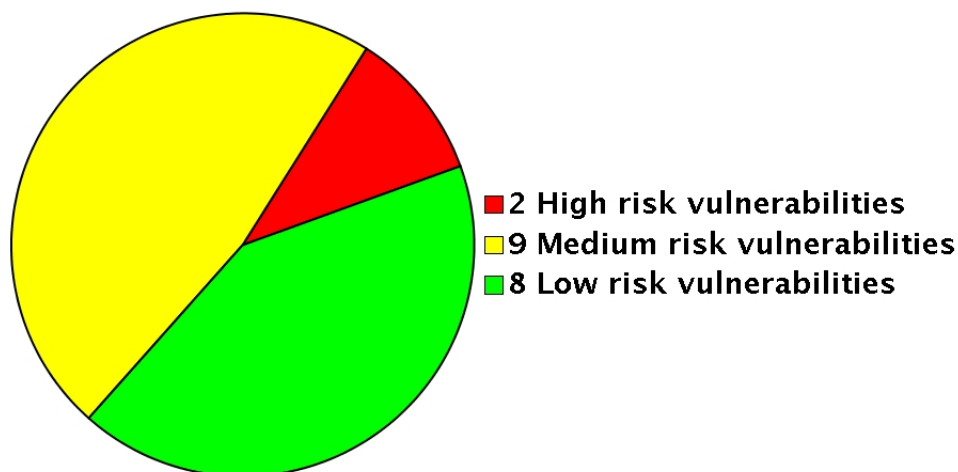
Scan of IP number:	Your IP Address here
Scan was started at:	15:00:31 19 Jul 2006 Central European Time
Scan ended at:	16:14:52 19 Jul 2006 Central European Time
Duration:	01:14:21 Hours
IP Country:	Netherlands
Network handle:	OVG9-RIPE, GVG18-RIPE
Performed by:	SecPoint® Penetrator 5.3.0.0

Overall Security Level: **Cat 1 (Critical level)**

Vulnerabilities

19 potential vulnerabilities identified.

The vulnerabilities divide in the following way:



Conclusion

SecPoint® Penetrator has determined that your system security level is dangerously low. It is possible for intruders to fully penetrate the system which can result in loss of private and sensitive data. It is recommended that you take immediate action to improve the security level.

Identified Ports and Services

The following "Ports and Services" could be identified remotely over the Internet.

Port	Protocol	Service
80	tcp	http

Information Gathered

This is the result of a traceroute from the SecPoint® Penetrator system to the target IP address:

```
1 0x555205d1.adsl.cybercity.dk (85.82.5.209) 1.438 ms 4.519 ms 3.609 ms
2 loop0.mxc1-kd4.ip.cybercity.dk (212.242.3.244) 85.401 ms 91.851 ms 84.065 ms
3 geth3-2.cr1-kd4.ip.cybercity.dk (212.242.7.97) 86.822 ms 85.985 ms 80.943 ms
4 pos4-1.cr2-khk.ip.cybercity.dk (212.242.6.177) 79.264 ms 86.557 ms 86.939 ms
5 ge-2-1-0.ar1.CPH1.gblx.net (67.17.163.233) 90.111 ms 80.229 ms 89.177 ms
6 so1-0-0-2488M.ar1.AMS1.gblx.net (67.17.65.242) 102.137 ms 111.932 ms 98.432 ms
7 64.208.110.70 (64.208.110.70) 99.805 ms 162.092 ms 103.483 ms
8 pos2-0.cr1.ams2.nl.above.net (208.184.231.54) 101.484 ms 98.667 ms 99.983 ms
9 k412.bgp.ams2.nl.above.net.webstekker (82.98.247.76) 99.989 ms 102.725 ms 99.058 ms
10 grnst.com (Your IP addres here) 101.186 ms 97.878 ms 174.234 ms
```

Banners identified

The following Service Banner outputs were readable remotely over the internet.

It is highly recommended to reconfigure these banners with bogus or no information at all.

Http Banner: Microsoft-IIS/6.0

Recommended solution

It is highly recommended to configure this output to return bogus or no information at all. If you have already done that please ignore this warning.

Port: 80/tcp

Overall Summary

Vulnerabilities found:

High risk vulnerabilities

- CFWebstore SQL Injection
- File index.php Command Execution

Medium risk vulnerabilities

- File /WPprofile.cfm Remote SQL Injection Vulnerability
- File /boxoffice/pictures.cfm Remote SQL Injection Vulnerability
- File /wp/WPprofile.cfm Remote SQL Injection Vulnerability
- FrontPage Extensions DoS /_vti_bin/_vti_aut/author.dll
- FrontPage Extensions DoS /_vti_bin/_vti_aut/author.exe
- FrontPage Extensions DoS /_vti_bin/shtml.dll/_vti_rpc
- Frontpage detected /_vti_inf.html
- Instaboard Index.cfm SQL Injection Vulnerability
- Microsoft(R) FrontPage Server Extensions MS-DOS Device Name DoS /_vti_bin/shtml.exe

Low risk vulnerabilities

- ColdFusion Path Disclosure Vulnerability
- Frontpage extensions detected /_vti_bin/_vti_adm/admin.dll
- IIS Identified
- PHP Identified
- Postinfo.html identified
- Remote system answers to PING command
- System Time Revealed via. ICMP TimeStamp
- System time via remote Web Server

CFWebstore SQL Injection

Risk: High

SecPoint ID: 4593

Bugtraq ID: 9854

Port: 80/tcp

Impact

The identified file index.cfm found on the remote web server part of the CFWebstore is subject to a sql injection vulnerability. This can allow an attacker to manipulate the target database and gain administrative privileges and or access sensitive information from the system. The service is also running on 80/tcp, 80/tcp.

Recommended solution

Please upgrade to the latest version of this software from <http://www.cfwebstore.com> and there click on downloads.

Vulnerability output

```
<tr>
  <td id="tablePropsWidth" width="400" colspan="2">
    <font style="COLOR: black
FONT: 8pt/11pt verdana">

    </font>
  </td>
</tr>
<tr>
  <td height>&nbsp;
</td>
</tr>
```

```
<tr>
  <td colspan="2">
    <font style="COLOR: black
FONT: 8pt/11pt verdana">
      Resources:
      <ul>

        <li>Enable Robust Exception Information to provide greater detail about the source of
errors. In the Administrator, click Debugging & Logging > Debugging Settings, and select the
Robust Exception Information option.</li>

        <li>Check the <a href=http://www.macromedia.com/go/proddoc_getdoc target="new">ColdFusion
documentation</a> to verify that you are using the correct syntax.</li>
        <li>Search the <a href=http://www.macromedia.com/support/coldfusion/ target="new">Knowledge
Base</a> to find a solution to your problem.</li>

      </ul>
    <p>
  </td>
</tr>

<tr>
  <td colspan="2">
    <table border="0" cellpadding="0" cellspacing="0">
  <tr>
```

```
<td><font style="COLOR: black
FONT: 8pt/11pt verdana">Browser&nbsp;
&nbsp;
</td>
<td><font style="COLOR: black
FONT: 8pt/11pt verdana"></td>
</
```


</body>

</html>

File /WPprofile.cfm Remote SQL Injection Vulnerability

Risk: Medium

SecPoint ID: 2376

Bugtraq ID: 4135

CVE: CAN-2002-0056

Port: 80/tcp

Impact

The identified file part of the web server software is subject to a SQL injection attack. The file does not properly sanitize user input supplied to the SQL and by that an attacker can modify the SQL statement. This can lead to disclosure of sensitive information. And the error messages by this can disclosure even more sensitive information. The service is also running on 80/tcp.

Recommended solution

Please upgrade to the latest package you are running for the web server and or set the file so that it will filter out arbitrary requests such as: ' | \' and more.

Vulnerability output

```
<tr>
  <td id="tablePropsWidth" width="400" colspan="2">
    <font style="COLOR: black
FONT: 8pt/11pt verdana">

      </font>
    </td>
  </tr>
  <tr>
    <td height>&nbsp;
  </td>
</tr>
```

```
<tr>
  <td colspan="2">
    <font style="COLOR: black
FONT: 8pt/11pt verdana">
      Resources:
      <ul>

        <li>Enable Robust Exception Information to provide greater detail about the source of
errors. In the Administrator, click Debugging & Logging > Debugging Settings, and select the
Robust Exception Information option.</li>

        <li>Check the <a href=http://www.macromedia.com/go/proddoc_getdoc target="new">ColdFusion
documentation</a> to verify that you are using the correct syntax.</li>
        <li>Search the <a href=http://www.macromedia.com/support/coldfusion/ target="new">Knowledge
Base</a> to find a solution to your problem.</li>

      </ul>
      <p>
    </td>
</tr>

<tr>
  <td colspan="2">
    <table border="0" cellpadding="0" cellspacing="0">
```

```
<tr>
  <td><font style="COLOR: black
FONT: 8pt/11pt verdana">Browser&nbsp;
&nbsp;
</td>
  <td><font style="COLOR: black
FONT: 8pt/11pt verdana"></td>
```

File /boxoffice/pictures.cfm Remote SQL Injection Vulnerability

Risk: Medium

SecPoint ID: 2376

Bugtraq ID: 4135

CVE: CAN-2002-0056

Port: 80/tcp

Impact

The identified file part of the web server software is subject to a SQL injection attack. The file does not properly sanitize user input supplied to the SQL and by that an attacker can modify the SQL statement. This can lead to disclosure of sensitive information. And the error messages by this can disclosure even more sensitive information. The service is also running on 80/tcp.

Recommended solution

Please upgrade to the latest package you are running for the web server and or set the file so that it will filter out arbitrary requests such as: ' | \' and more.

Vulnerability output

```
</tr>
<tr>
  <td id="tablePropsWidth" width="400" colspan="2">
    <font style="COLOR: black
FONT: 8pt/11pt verdana">

      </font>
    </td>
</tr>
<tr>
  <td height>&nbsp;
</td>
</tr>
```

```
<tr>
  <td colspan="2">
    <font style="COLOR: black
FONT: 8pt/11pt verdana">
    Resources:
    <ul>
```

```
      <li>Enable Robust Exception Information to provide greater detail about the source of
errors. In the Administrator, click Debugging & Logging > Debugging Settings, and select the
Robust Exception Information option.</li>
```

```
  <li>Check the <a href=http://www.macromedia.com/go/proddoc_getdoc target="new">ColdFusion
documentation</a> to verify that you are using the correct syntax.</li>
```

```
  <li>Search the <a href=http://www.macromedia.com/support/coldfusion/ target="new">Knowledge
Base</a> to find a solution to your problem.</li>
```

```
    </ul>
  <p>
</td>
</tr>
```

```
<tr>
  <td colspan="2">
```

```
<table border="0" cellpadding="0" cellspacing="0">
<tr>
<td><font style="COLOR: black
FONT: 8pt/11pt verdana">Browser&nbsp;
&nbsp;
</td>
<td><font style="COLOR: black
FONT: 8pt/11pt verdana"></td>
```

File /wp/WPprofile.cfm Remote SQL Injection Vulnerability

Risk: Medium

SecPoint ID: 2376

Bugtraq ID: 4135

CVE: CAN-2002-0056

Port: 80/tcp

Impact

The identified file part of the web server software is subject to a SQL injection attack. The file does not properly sanitize user input supplied to the SQL and by that an attacker can modify the SQL statement. This can lead to disclosure of sensitive information. And the error messages by this can disclosure even more sensitive information. The service is also running on 80/tcp.

Recommended solution

Please upgrade to the latest package you are running for the web server and or set the file so that it will filter out arbitrary requests such as: ' | \' and more.

Vulnerability output

```
>
  <tr>
    <td id="tablePropsWidth" width="400" colspan="2">
      <font style="COLOR: black
FONT: 8pt/11pt verdana">

        </font>
      </td>
    </tr>
  <tr>
    <td height>&nbsp;
  </td>
</tr>
```

```
<tr>
  <td colspan="2">
    <font style="COLOR: black
FONT: 8pt/11pt verdana">
    Resources:
    <ul>
```

```
      <li>Enable Robust Exception Information to provide greater detail about the source of
errors. In the Administrator, click Debugging & Logging > Debugging Settings, and select the
Robust Exception Information option.</li>
```

```
  <li>Check the <a href=http://www.macromedia.com/go/proddoc_getdoc target="new">ColdFusion
documentation</a> to verify that you are using the correct syntax.</li>
```

```
  <li>Search the <a href=http://www.macromedia.com/support/coldfusion/ target="new">Knowledge
Base</a> to find a solution to your problem.</li>
```

```
    </ul>
  <p>
</td>
</tr>
```

```
<tr>
  <td colspan="2">
```

```
<table border="0" cellpadding="0" cellspacing="0">
<tr>
<td><font style="COLOR: black
FONT: 8pt/11pt verdana">Browser&nbsp;
&nbsp;
</td>
<td><font style="COLOR: black
FONT: 8pt/11pt verdana"></td>
```

FrontPage Extensions DoS /_vti_bin/_vti_aut/author.dll

Risk: Medium

SecPoint ID: 1416

Bugtraq ID: 2144

CVE: CVE-2001-0096

Port: 80/tcp

Impact

The found file /_vti_bin/_vti_aut/author.dll is part of the FrontPage extensions package. This file is known to contain a vulnerability where remote attackers can crash the system such as a Denial of Service attack.

Recommended solution

WINDOWS

Microsoft(R) has released an advisory on this from

<http://www.microsoft.com/technet/security/bulletin/MS00-100.asp>

Vulnerability output

HTTP/1.1 200 OK

Connection: close

Date: Wed, 19 Jul 2006 13:18:07 GMT

Server: Microsoft-IIS/6.0

MicrosoftOfficeWebServer: 5.0_Pub

X-Powered-By: ASP.NET

FrontPage Extensions DoS /_vti_bin/_vti_aut/author.exe

Risk: Medium

SecPoint ID: 1416

Bugtraq ID: 2144

CVE: CVE-2001-0096

Port: 80/tcp

Impact

The found file /_vti_bin/_vti_aut/author.exe is part of the FrontPage extensions package. This file is known to contain a vulnerability where remote attackers can crash the system such as a Denial of Service attack.

Recommended solution

WINDOWS

Microsoft(R) has released an advisory on this from

<http://www.microsoft.com/technet/security/bulletin/MS00-100.asp>

Vulnerability output

HTTP/1.1 200 OK

Connection: close

Date: Wed, 19 Jul 2006 13:18:08 GMT

Server: Microsoft-IIS/6.0

MicrosoftOfficeWebServer: 5.0_Pub

X-Powered-By: ASP.NET

FrontPage Extensions DoS /_vti_bin/shtml.dll/_vti_rpc

Risk: Medium

SecPoint ID: 1416

Bugtraq ID: 2144

CVE: CVE-2001-0096

Port: 80/tcp

Impact

The found file /_vti_bin/shtml.dll/_vti_rpc is part of the FrontPage extensions package. This file is known to contain a vulnerability where remote attackers can crash the system such as a Denial of Service attack. The service is also running on 80/tcp.

Recommended solution

WINDOWS

Microsoft(R) has released an advisory on this from

<http://www.microsoft.com/technet/security/bulletin/MS00-100.asp>

Vulnerability output

HTTP/1.1 200 OK

Connection: close

Date: Wed, 19 Jul 2006 13:18:07 GMT

Server: Microsoft-IIS/6.0

MicrosoftOfficeWebServer: 5.0_Pub

X-Powered-By: ASP.NET

</head>

<body>

<!-- _vti_inf.html version 0.100>

<!--

This file contains important information used by the FrontPage client (the FrontPage Explorer and FrontPage Editor) to communicate with the FrontPage server extensions installed on this web server.

The values below are automatically set by FrontPage at installation. Normally, you do not need to modify these values, but in case you do, the parameters are as follows:

FPShtmlScriptUrl, FPAuthorScriptUrl, and FPAdminScriptUrl specify the relative urls for the scripts that FrontPage uses for remote authoring. These values should not be changed.

FPVersion identifies the version of the FrontPage Server Extensions installed, and should not be changed.

--><!-- FrontPage Configuration Information

FPVersion="5.0.2.5012"

FPShtmlScriptUrl="_vti_bin/shtml.dll/_vti_rpc"

FPAuthorSc

Instaboard Index.cfm SQL Injection Vulnerability

Risk: Medium

SecPoint ID: 3622

Bugtraq ID: 7338

Port: 80/tcp

Impact

The identified InstaBoard found running on the remote web server is subject to a SQL Injection vulnerability. This can allow an attacker to inject code into the SQL database. This can lead to disclosure of sensitive information. And the error messages by this can disclosure even more sensitive information.

Recommended solution

Please upgrade to the latest version of this software from <http://www.netpleasure.com/instaboard/> and there click on support in the menu to login to the system to download updates.

Vulnerability output

```
</tr>
  <tr>
    <td id="tablePropsWidth" width="400" colspan="2">
      <font style="COLOR: black
FONT: 8pt/11pt verdana">

        </font>
      </td>
    </tr>
    <tr>
      <td height>&nbsp;
</td>
</tr>
```

```
<tr>
  <td colspan="2">
    <font style="COLOR: black
FONT: 8pt/11pt verdana">
      Resources:
      <ul>

        <li>Enable Robust Exception Information to provide greater detail about the source of
errors. In the Administrator, click Debugging & Logging > Debugging Settings, and select the
Robust Exception Information option.</li>

        <li>Check the <a href=http://www.macromedia.com/go/proddoc_getdoc target="new">ColdFusion
documentation</a> to verify that you are using the correct syntax.</li>
        <li>Search the <a href=http://www.macromedia.com/support/coldfusion/ target="new">Knowledge
Base</a> to find a solution to your problem.</li>

      </ul>
      <p>
    </td>
</tr>

<tr>
  <td colspan="2">
    <table border="0" cellpadding="0" cellspacing="0">
```

```
<tr>
  <td><font style="COLOR: black
FONT: 8pt/11pt verdana">Browser&nbsp;
&nbsp;
</td>
  <td><font style="COLOR: black
FONT: 8pt/11pt verdana"></td>
```

Microsoft(R) FrontPage Server Extensions MS-DOS Device Name DoS /_vti_bin/shtml.exe

Risk: Medium

SecPoint ID: 1414

Bugtraq ID: 1608

CVE: CAN-2000-0710

Port: 80/tcp

Impact

There exist a Denial of Service via the identified file /_vti_bin/shtml.exe when requesting MS-DOS devices.

Recommended solution

WINDOWS

Please upgrade to the latest version of the FrontPage Server Extensions Services if needed from <http://msdn.microsoft.com/workshop/languages/fp/2000/winfpse.asp>

Vulnerability output

HTTP/1.1 200 OK

Connection: close

Date: Wed, 19 Jul 2006 13:53:58 GMT

Server: Microsoft-IIS/6.0

MicrosoftOfficeWebServer: 5.0_Pub

X-Powered-By: ASP.NET

ColdFusion Path Disclosure Vulnerability

Risk: Low

SecPoint ID: 2501

Bugtraq ID: 4542

CVE: CAN-2002-0576

Port: 80/tcp

Impact

The identified ColdFusion service running is subject to a path disclosure vulnerability. An attacker can use this information to base other attacks on.

Recommended solution

Please remove the entire /cfdocs from the system. NOTE* This will not affect your online services since it is just contains example files. And or Please upgrade to the latest version of Allaire ColdFusion from <http://www.allaire.com> NOTE* Always make a backup before deleting files.

Vulnerability output

```
splay = "none"
```

```
    }  
  }  
}  
</script>
```

```
</head>
```

```
<body>
```

```
<font style="COLOR: black  
FONT: 16pt/18pt verdana">
```

```
The web site you are accessing has experienced an unexpected error.<br>  
Please contact the website administrator.
```

```
</font>
```

```
<br><br>
```

```
<table border="1" cellpadding="3" bordercolor="#000808" bgcolor="#e7e7e7">
```

```
<tr>
  <td bgcolor="#000066">
    <font style="COLOR: white
FONT: 11pt/13pt verdana" color="white">
      The following information is meant for the website developer for debugging purposes.
    </font>
  </td>
</tr>
<tr>
<tr>
  <td bgcolor="#4646EE">
    <font style="COLOR: white
FONT: 11pt/13pt verdana" color="white">
      Error Occurred While Processing Request
    </font>
  </td>
</tr>
<tr>
<tr>
  <td>
    <font style="COLOR: black
FONT: 8pt/11pt verdana">
```

```
<table width="500" cellpadding="0" cellspacing="0" border="0">
<tr>
  <td id="tableProps2" align="left" valign="middle" width="500">
    <h1 id="textSection1" style="COLOR: black
FONT: 13pt/15pt verdana">
      Access is denied
    </h1>
  </td>
</tr>
<tr>
```

Frontpage extensions detected /_vti_bin/_vti_adm/admin.dll

Risk: Low

SecPoint ID: 151

Port: 80/tcp

Impact

The following file /_vti_bin/_vti_adm/admin.dll has been found on the target system. This file gives information the idea that frontpage extensions are running on the host. The attacker can use this information to base other attacks on. And this file can contain a vulnerability found in the future.

Recommended solution

Please block all incoming requests on the web server software for the file
/_vti_bin/_vti_adm/admin.dll

Vulnerability output

HTTP/1.1 200 OK

Connection: close

Date: Wed, 19 Jul 2006 13:18:22 GMT

Server: Microsoft-IIS/6.0

MicrosoftOfficeWebServer: 5.0_Pub

X-Powered-By: ASP.NET

PHP Identified

Risk: Low

SecPoint ID: 500

Port: 80/tcp

Impact

It is possible via the banner from the web server software to detect some presence of PHP. PHP has a known history of several security vulnerabilities. Attackers can use this information to do PHP specified attacks.

Recommended solution

To reconfigure the PHP version banner edit /php-4.0/main/php_version.h and in /php-4.0/sapi/apache/mod_php4.c and look for PHP/ and remove that. Now recompile PHP.
RECOMMENDED SOLUTION: Immediately upgrade to the latest version of php from <http://www.php.net> .

Vulnerability output

```
HTTP/1.1 404 OK
Content-Length: 1635
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: PHP/5.1.2
X-Powered-By: ASP.NET
Date: Wed, 19 Jul 2006 13:16:25 GMT
Connection: close
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd">
<HTML><HEAD><TITLE>The page cannot be found</TITLE>
<META HTTP-EQUIV="Content-Type" Content="text/html
charset=Windows-1252">
<STYLE type="text/css">
  BODY { font: 8pt/12pt verdana }
  H1 { font: 13pt/15pt verdana }
  H2 { font: 8pt/12pt verdana }
  A:link { color: red }
```

```
A:visited { color: maroon }
</STYLE>
</HEAD><BODY><TABLE width=500 border=0 cellpadding=10><TR><TD>

<h1>The page cannot be found</h1>
The page you are looking for might have been removed, had its name changed, or is temporarily
unavailable.
<hr>
<p>Please try the following:</p>
<ul>
<li>Make sure that the Web site address displayed in the address bar of your browser is spelled
and formatted correctly.</li>
<li>If you reached this page by clicking a link, contact
the Web site administrator to alert them that the link is incorrectly formatted.
</li>
<li>Click the <a href="javascript:history.back(1)">Back</a> button to try another link.</li>
</ul>
<h2>HTTP Error 404 - File or directory not found.<br>Internet Information Services (IIS)</h2>
<hr>
<p>Technical Information (for support personnel)</p>
<ul>
<li>Go to <a href="http://go.microsoft.com/fwlink/?linkid=8180">Microsoft Product Support
Services</a> and perform a title search for the words <b>HTTP</b> and <b>404</b>.</li>
<li>Open <b>IIS Help</b>, which is accessible in IIS Manager (inetmgr),
and search for topics titled <b>Web Site Setup</b>, <b>Common Administrative Tasks</b>, and
<b>About Custom Error Messages</b>.</li>
</ul>

</TD></TR></TABLE></BODY></HTML>
```



```
<body>
```

```
<!-- postinfo.html version 0.100>
```

```
<!--
```

This file allows users to post files to their web with the Web Publishing Wizard or FrontPad, using the same username and password they would use if they were authoring with the FrontPage Explorer and Editor.

The values below are automatically set by FrontPage at installation time. Normally, you do not need to modify these values, but in case you do, the parameters are as follows:

BaseUrl is the URL for your web server.

DefaultPage is the name of the default (home) page name for your web.

XferType specifies that the FrontPage server extensions have been installed on this web. This value should not be changed.

FPShtmlScriptUrl, FPAuthorScriptUrl, and FPAdminScriptUrl specify the relative urls for the scripts that FrontPage uses for remote authoring. These values should not be ch

