

# Microsoft IIS 6 parsing directory “x.asp” Vulnerability

By: Pouya Daneshmand

[whh\\_iran@yahoo.com](mailto:whh_iran@yahoo.com)  
<http://securitylab.ir/blog/>

First release date: 2010-06-19  
English rewrite date: 2011-01-25

### Introduction:

Using this vulnerability you can bypass some Security filters, for example a file with ".jpg" or ".rar" extension can be executed as an asp (Active Server Page) file.

### Vulnerable:

It just works for asp files and works on Windows 2003 / IIS 6 (As I tested...).  
The test failed on IIS 5.1 and IIS 7.

### Description:

- 1) Create a Folder with '.asp' extension. (Figure #1)
- 2) Insert your ASP code in a file with any extension (like .jpg,.rar,.txt) in the folder you have created. (Figure #2)
- 3) Open the file with your browser and you will see it's executed as an asp file! (Figure #3)

Note: The Extension of file does not matter at all!

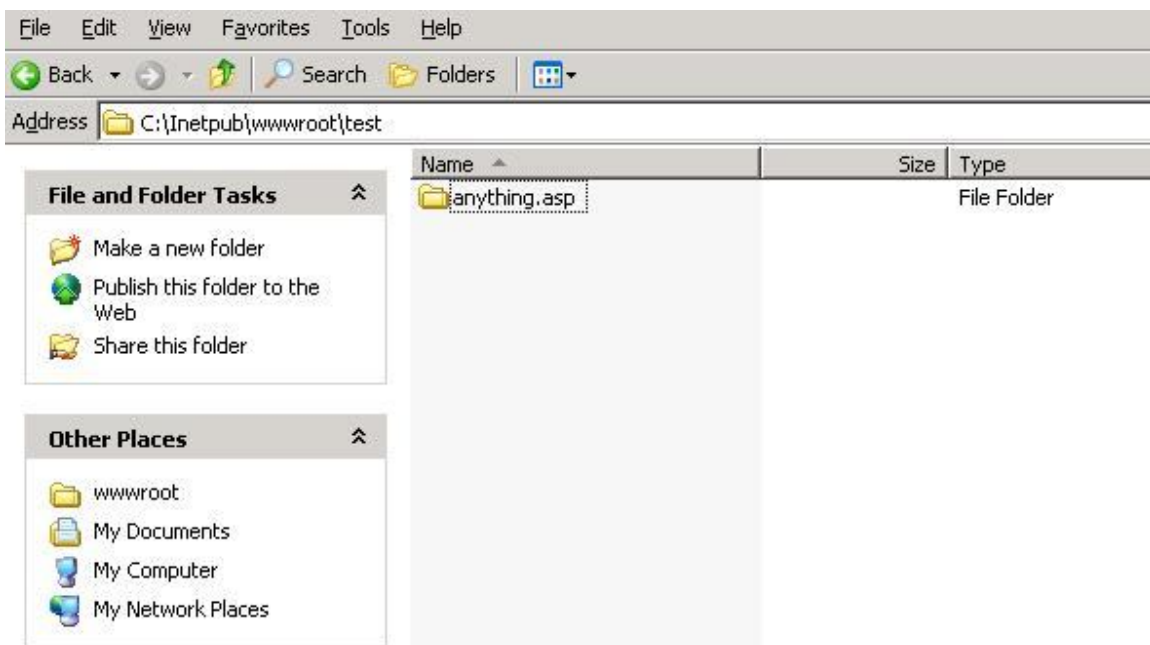


Figure 1: Create folder

## Microsoft IIS 6 parsing directory "x.asp" Vulnerability

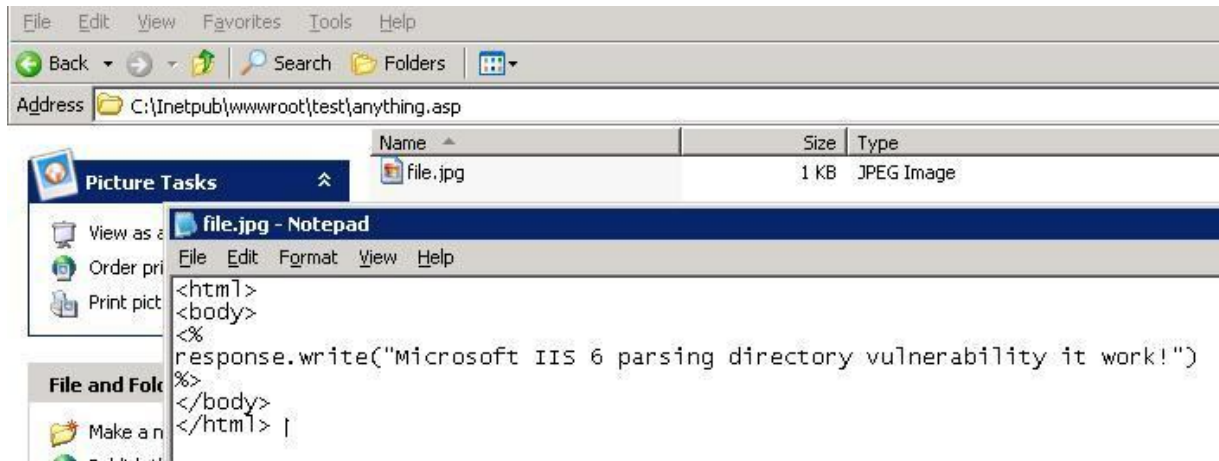


Figure 2: Create .jpg file



Microsoft IIS 6 parsing directory vulnerability it work!

Figure 3: Run file.jpg

**Solution:**

There is no patch to fix this security vulnerability yet, the best thing I can say is to DISABLE ASP FILES FROM YOUR "web server extensions"! Or Remove "execute" permission from the upload directories.

**PS:**

This vulnerability was reported for first time at 2010-06-19 in Persian (<http://sebug.net/vulndb/19820/>)