Below is a sample from a Cisco Press book:

IP: 172.16.22.199 Name: CorpWebSrvr1

Port	Service	Description
80	HTTP (Web)	Host appears to be running Microsoft Internet Information Server 5.0. Attempts to penetrate included the following: 1) msadc exploit, 2) codebrw.asp exploit, 3) showcode.asp exploit, 4) cgi exploits, 5) webhits.dll / webhits.htw exploits, 6) $data exploit, 7) ASP dot bug exploit, 8) ISM.dll buffer truncation exploit, 9) .idc and .ida exploits, 10) +htr exploits, 11) adsamples exploit, 12) /iisadmnpasswd, 13) dictionary password cracking, 14) brute force password cracking, and 15) SQL injection.
443	HTTPS (Secure Web)	A 1024-bit digital certificate is used that will expire December 15, 2005. The certificate is encrypted using RSA Sha1 encryption and is signed by VeriSign.

Vulnerability Analysis

Vulnerability: Unicode Directory Traversal

Risk: High

Description: A flaw in IIS allows for a malicious hacker to execute code on a target system. During testing, the following was entered into the URL string in a Microsoft Internet Explorer web browser:

http://www.hackmynetwork.com/scripts/..%co%af%../..%co%af%../..

%co%af%../

..%co%af%../..%co%af%../..%co%af%../..%co%af%../..%co%af%..

/winnt/system32/

cmd.exe?/c+dir+c:

This resulted in getting a complete directory listing of the target server. You can use this same syntax to execute code on a target system. Attackers can use this exploit to steal confidential information, launch another attack, or perform DoS attacks on the target network.

Vulnerability: IIS Sample Codebrws.asp

Risk: Medium

The codebrws.asp sample file is shipped with Microsoft IIS server and can be used to remotely read arbitrary files. This might reveal sensitive information or code that can be used for further exploits.