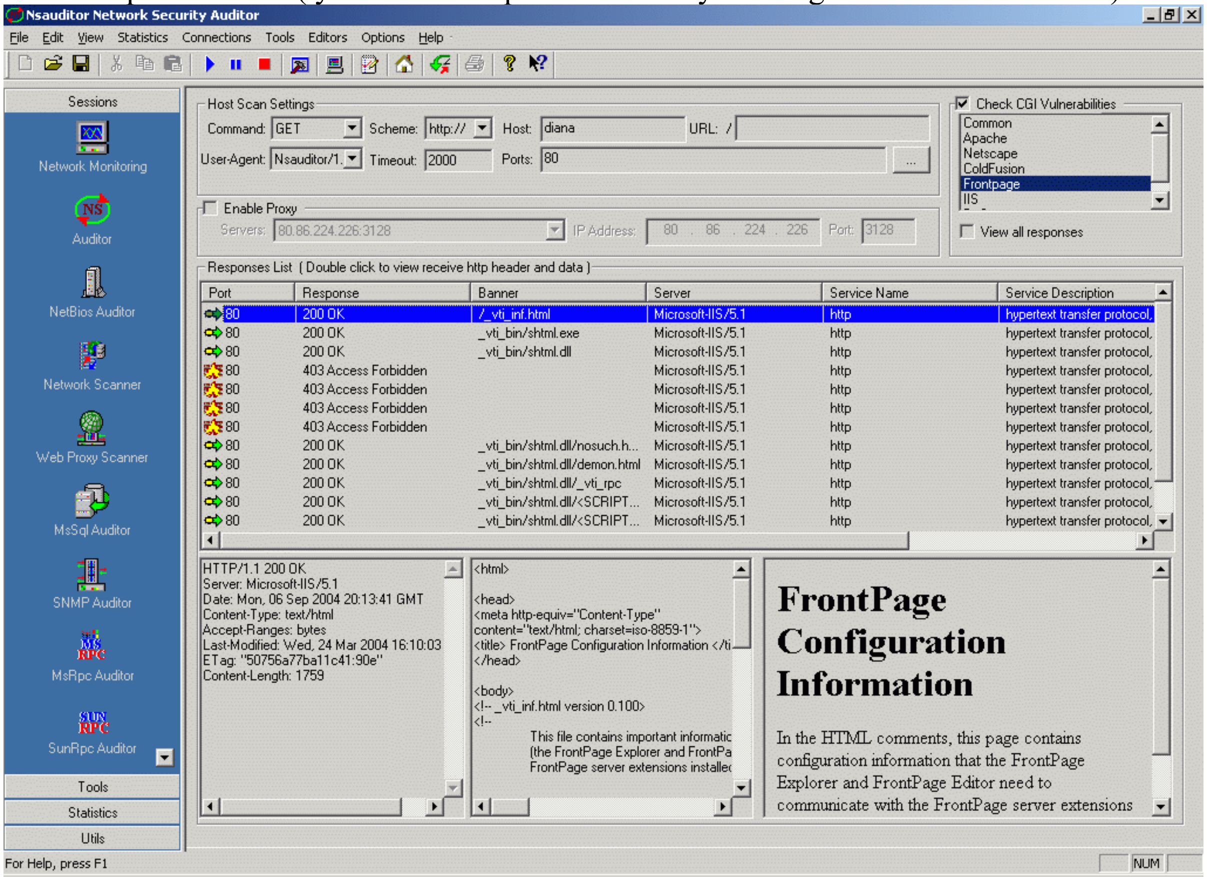
Web Proxy Scanner

Web proxy scanner is a tool to check vulnerabilities of web servers(this scanner can work as a port scanner if **Check CGI Vulnerabilities** is not enabled).
It is evident that CGI probes are sent against web servers. This tool provides an ability to configure the scanner for running CGI probes through that proxy (if **Enable Proxy** is turned on) or without proxy (if **Enable Proxy** is turned off) .
Here is a brief description of each field located in **Host Scan Settings**. The field **Command** contains the command type (GET, PUT,POST, etc.), the field **Scheme** contains the protocol type (http, ftp, gopher), the field **Host** contains the host name (ex. Camelot, www.nsauditor.com), the field **URL** contains the URL, the field **User Agent** contains the name of the client program (Nsauditor/1.0, Mozilla/5.0, Mozilla/4.0) , the field **Timeout** contains the timeout interval to wait for responses, the field **Ports** contains port numbers(you can select port numbers by clicking on the browse button).



Host Scan Settings
Command: GET Scheme: http:// Host: diana URL: /
User-Agent: Nsauditor/1. Timeout: 2000 Ports: 80 ...

☐ Enable Proxy
Servers: 80.86.224.226:3128 IP Address: 80 . 86 . 224 . 226 Port: 3128

☑ Check CGI Vulnerabilities
Common
Apache
Netscape
ColdFusion
Frontpage
IIS

☐ View all responses

Responses List (Double click to view receive http header and data)

Port	Response	Banner	Server	Service Name	Service Description
80	200 OK	/_vti_inf.html	Microsoft-IIS/5.1	http	hypertext transfer protocol,
80	200 OK	_vti_bin/shtml.exe	Microsoft-IIS/5.1	http	hypertext transfer protocol,
80	200 OK	_vti_bin/shtml.dll	Microsoft-IIS/5.1	http	hypertext transfer protocol,
80	403 Access Forbidden		Microsoft-IIS/5.1	http	hypertext transfer protocol,
80	403 Access Forbidden		Microsoft-IIS/5.1	http	hypertext transfer protocol,
80	403 Access Forbidden		Microsoft-IIS/5.1	http	hypertext transfer protocol,
80	403 Access Forbidden		Microsoft-IIS/5.1	http	hypertext transfer protocol,
80	200 OK	_vti_bin/shtml.dll/nosuch.h...	Microsoft-IIS/5.1	http	hypertext transfer protocol,
80	200 OK	_vti_bin/shtml.dll/demon.html	Microsoft-IIS/5.1	http	hypertext transfer protocol,
80	200 OK	_vti_bin/shtml.dll/_vti_rpc	Microsoft-IIS/5.1	http	hypertext transfer protocol,
80	200 OK	_vti_bin/shtml.dll/<SCRIPT...	Microsoft-IIS/5.1	http	hypertext transfer protocol,
80	200 OK	_vti_bin/shtml.dll/<SCRIPT...	Microsoft-IIS/5.1	http	hypertext transfer protocol,

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.1
Date: Mon, 06 Sep 2004 20:13:41 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Wed, 24 Mar 2004 16:10:03
ETag: "50756a77ba11c41:90e"
Content-Length: 1759
```

```
<html>

<head>
<meta http-equiv="Content-Type"
content="text/html; charset=iso-8859-1">
<title> FrontPage Configuration Information </ti
</head>

<body>
<!-- _vti_inf.html version 0.100>
<!--
        This file contains important informatic
        (the FrontPage Explorer and FrontPa
        FrontPage server extensions installec
```

FrontPage Configuration Information

In the HTML comments, this page contains configuration information that the FrontPage Explorer and FrontPage Editor need to communicate with the FrontPage server extensions

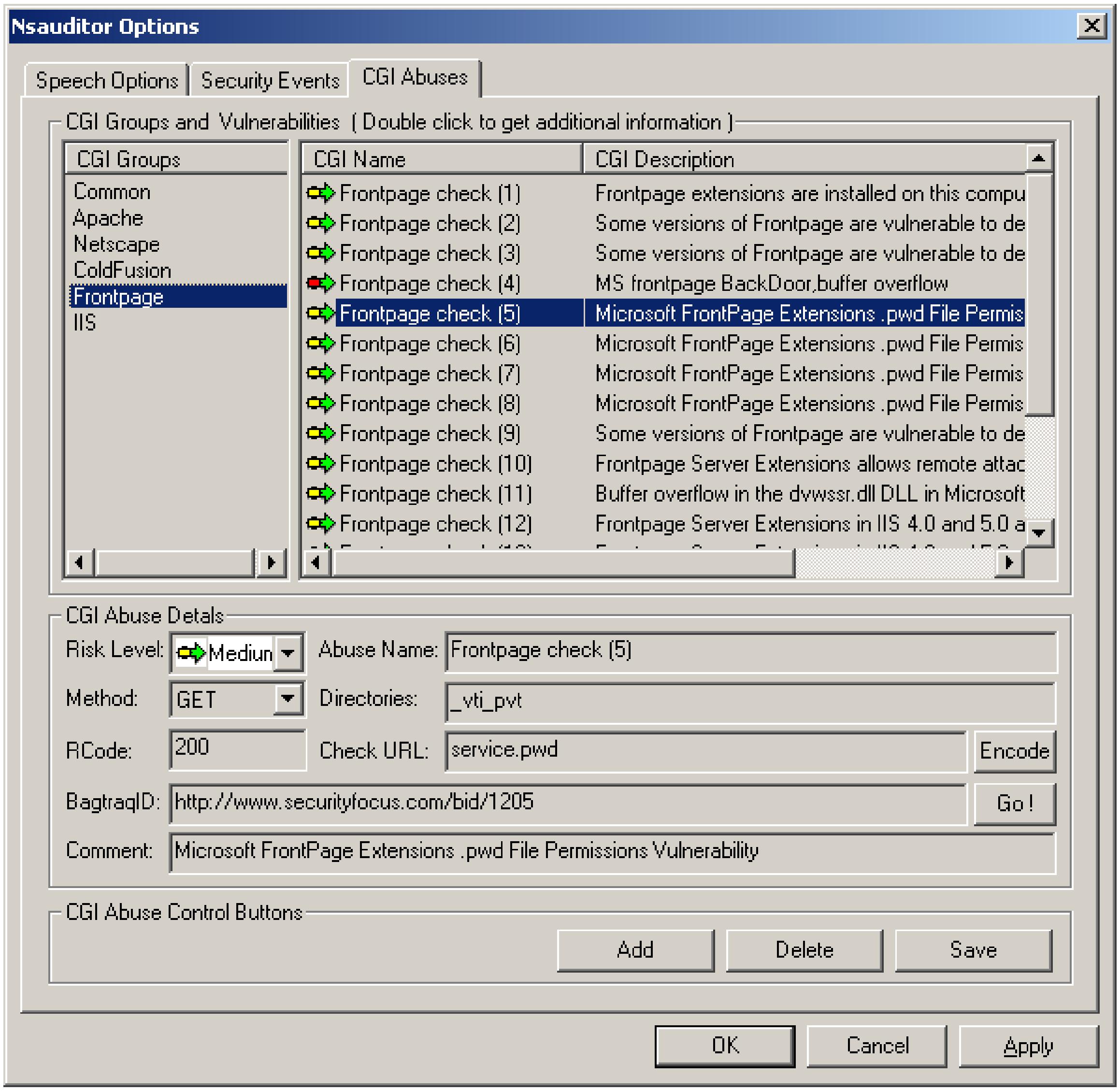
Turning on **Check CGI Vulnerabilities** allows you to select the service(Common, Apache, etc .) for checking vulnerabilities. Note that if the selected service is Front Page or IIS than the operating system of destination host should be Windows. You can use Ping to check the operating system.

To connect through proxy turn on the **Enable Proxy** setting and select one of anonymous proxy servers from the list.

The probe that will be sent to the target host is based on the mentioned parameters. There are some known vulnerability tests for each service.

You can configure these tests using Options/Configuration (CGI Abuses) .

Double clicking on the scan entry you can view the CGI Abuse details. The dialog below shows all the details of the selected row .



CGI Groups and Vulnerabilities (Double click to get additional information)

CGI Groups: Common, Apache, Netscape, ColdFusion, Frontpage, IIS

CGI Name	CGI Description
Frontpage check (1)	Frontpage extensions are installed on this compu
Frontpage check (2)	Some versions of Frontpage are vulnerable to de
Frontpage check (3)	Some versions of Frontpage are vulnerable to de
Frontpage check (4)	MS frontpage BackDoor,buffer overflow
Frontpage check (5)	Microsoft FrontPage Extensions .pwd File Permis
Frontpage check (6)	Microsoft FrontPage Extensions .pwd File Permis
Frontpage check (7)	Microsoft FrontPage Extensions .pwd File Permis
Frontpage check (8)	Microsoft FrontPage Extensions .pwd File Permis
Frontpage check (9)	Some versions of Frontpage are vulnerable to de
Frontpage check (10)	Frontpage Server Extensions allows remote attac
Frontpage check (11)	Buffer overflow in the dvwssr.dll DLL in Microsoft
Frontpage check (12)	Frontpage Server Extensions in IIS 4.0 and 5.0 a

CGI Abuse Detals

Risk Level: Mediun

Abuse Name: Frontpage check (5)

Method: GET

Directories: _vti_pvt

RCode: 200

Check URL: service.pwd

BagtraqID: http://www.securityfocus.com/bid/1205

Comment: Microsoft FrontPage Extensions .pwd File Permissions Vulnerability

CGI Abuse Control Buttons

Selecting the appropriate CGI from the CGI Groups allows you to see all the check probes for the selected CGI including CGI Name and CGI Description. Selecting one of the CGI checks will show the CGI Abuse Details for that check including Risk Level, Abuse Name, Method, Directories, RCode (return code), Directories, Check URL, BagtraqID, Comment.

These well known tests are used to create the probes. You can hide the name of your real user agent by selecting any other from the list(it will seem that the probe is sent not from the real sender Nsauditor).

You can add, delete and save the information in the page by clicking on the **Add**, **Delete**, **Save** buttons accordingly.

If **View All Responses** is turned on the **Responses List** of Network Security Auditor window will contain all responses. Otherwise the list will contain only the responses with open ports. You can double click on the row to view http header, source and data of each response (left, middle , right parts of bottom section).