# 1. Getting Started

## 1.1. Default Policies

N-Stalker Web Application Security Scanner provides a default list of scan policies that can be used to initiate quick scan sessions or even serve as template to generate custom user policies.

### 1.1.1. Development & QA

This is the list of default policies for Development & QA Life-cycle:

| | |
|---|---|
| **Custom Design Error Only** | This policy will search for Custom Design Errors on the application such as XSS and SQL injection, Buffer Overflow, Parameters Tampering issues and Cookie vulnerabilities. |
| **Common OWASP Top10 Check** | This policy will search for Common Top10 security issues described by OWASP (Open Web Application Security Project) focused on development. The assessment includes XSS and SQL injection, Buffer Overflow, Parameter Tampering, Cookie vulnerability, Insecure data handling, confidentiality issues, File & Directory issues and much more. |
| **Information Exposure Analysis (Confidential Check Only)** | This is a policy focused on Confidentiality issues. It will search for insecure data handling, information leakage through meta tags, html comments and scripts, Cookie and File exposure. |

### 1.1.2. Infrastructure & Deploy

This is the list of default policies for Infrastructure & Deploy:

| | |
|---|---|
| **Complete Web Server Pen-test** | This policy will assess Web Server infrastructure for security vulnerabilities. It will complement the assessment with the traditional N-Stealth's 35,000 attack signature database for 3rd party software. Also searches for Backup, Password and configuration files misplaced in the server's root directory. |
| **Web Server Technology Assessment Only** | This policy is focused on assessing the Web Server technology only, searching for vulnerable platform version. |
| **SANS/FBI Top10 and Backup Assessment** | This policy will assess Web Server against SANS/FBI Top10 common web security vulnerabilities. N-Stalker will also search for backup files misplaced on server's root directory. |

### 1.1.3. Audit & Pen-test

This is the list of default policies for Infrastructure & Deploy:

| | |
|---|---|
| **Complete Pen-test** | This is the most complete security assessment |


All Rights reserved ZMT Comunicações e Tecnologia Ltda.

| | |
|---|---|
| **Assessment** | policy. It will search for custom development vulnerabilities such as XSS and SQL injection, Buffer Overflow, Parameter Tampering, File & Directory issues, Confidentiality issues, Cookie vulnerabilities and will also include an infrastructure check of N-Stealth's 35,000 attack signature database. |
| **Confidential SSL Web Application Assessment** | This policy will assess Web Application that is supposed to run securely over SSL. It will search for confidentiality issues, insecure data handling and web server SSL weakness. |
| **Privacy Act Compliance Policy** | This policy will assess Web Application for privacy issues. It will search for insecure personal data handling, SSL infrastructure weakness, presence of a privacy policy on every web form and file exposures. |

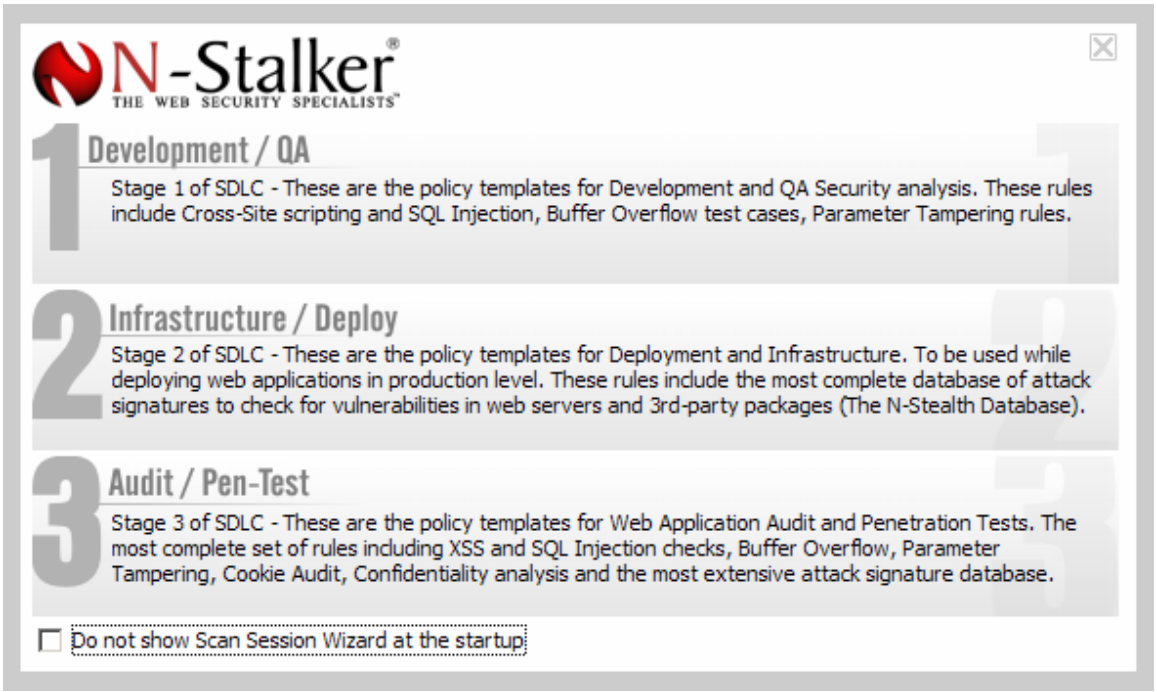
## 1.2. Starting Wizard-based scan

N-Stalker Web Application Security Scanner provides a Wizard interface to enable quick set up of scan sessions. By default, the Scan Wizard will appear during initialization. You may modify this behavior by enabling the option "Do not show Scan Session Wizard at the startup".

Scan Wizard can be invoked at any time by selecting option "Scan Wizard" onto N-Stalker's toolbar.

### 1.2.1. Choose Policy Profile

Once the Scan Wizard is opened, you will be required to choose a policy profile from N-Stalker Web Security Development Life-Cycle (see section 1.3.1):





All Rights reserved ZMT Comunicações e Tecnologia Ltda.

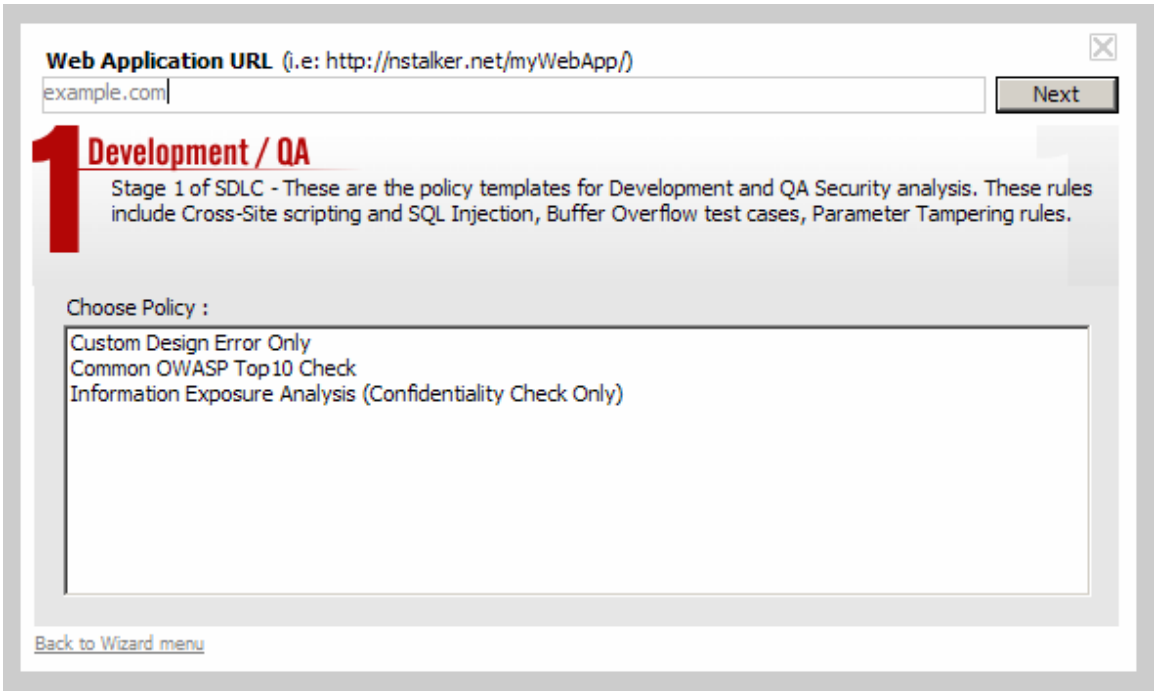
| | |
|---|---|
| **Development & QA** | This option will allow you to choose from Development & QA Policies available to scan with.<br><br>This option is available on the following editions(*):<br>• **QA Edition**<br>• **Enterprise Edition** |
| **Infrastructure & Deploy** | This option will allow you to choose from Infrastructure & Deploy Policies available to scan with.<br><br>This option is available on the following editions(*):<br>• **Infrastructure Edition**<br>• **Enterprise Edition** |
| **Audit & Pen-Test** | This option will allow you to choose from Audit & Pen-test available to scan with.<br><br>This option is available on the following editions(*):<br>• **Enterprise Edition** |

(*) Policy Profiles depend on N-Stalker Web Application Security Scanner Edition and may not be available on your licensed edition.

To understand more about N-Stalker Web Application Security Scanner Policy Profiles, please see Chapter 3.

### 1.2.2. Choose Target

Before choosing the appropriate scan policy you must select the target Web Application (URL) to scan. Enter the URL in the "Web Application URL" field:



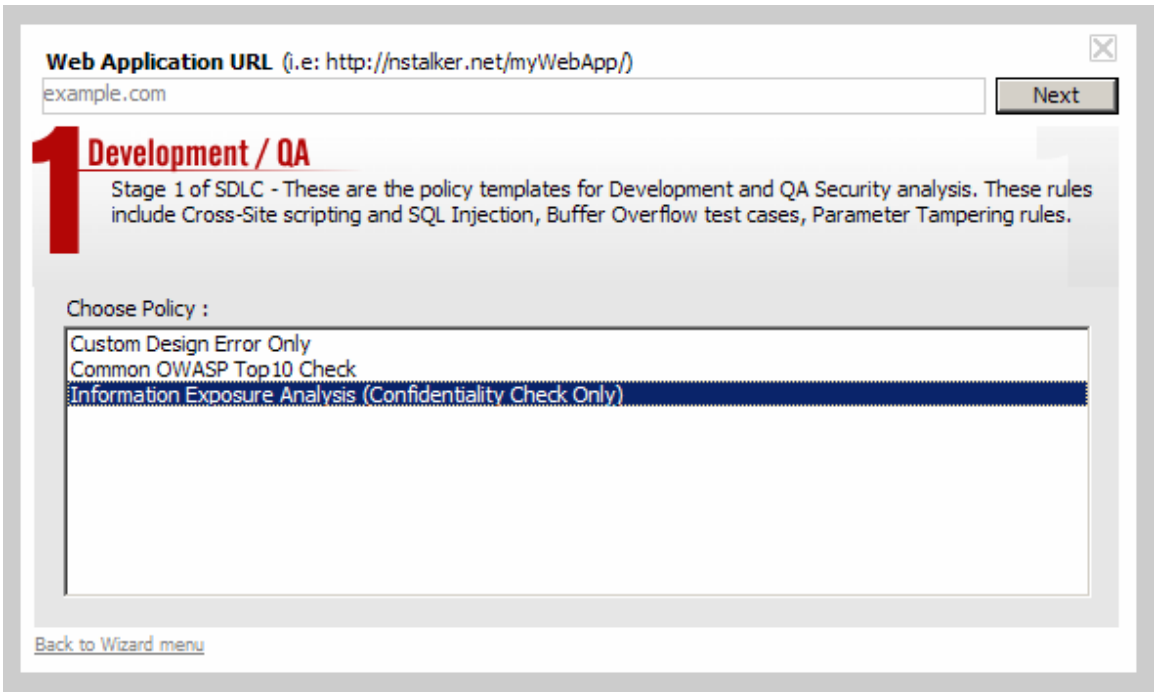

You may specify the following URL formats:


All Rights reserved ZMT Comunicações e Tecnologia Ltda.

- www.example.com
- http://www.example.com
- https://www.example.com
- http://www.example.com:8080/
  (connect to TCP port 8080)
- http://www.example.com/sample/
  (scan will be restricted to “sample” directory)

### 1.2.3. Choose Scan Policy

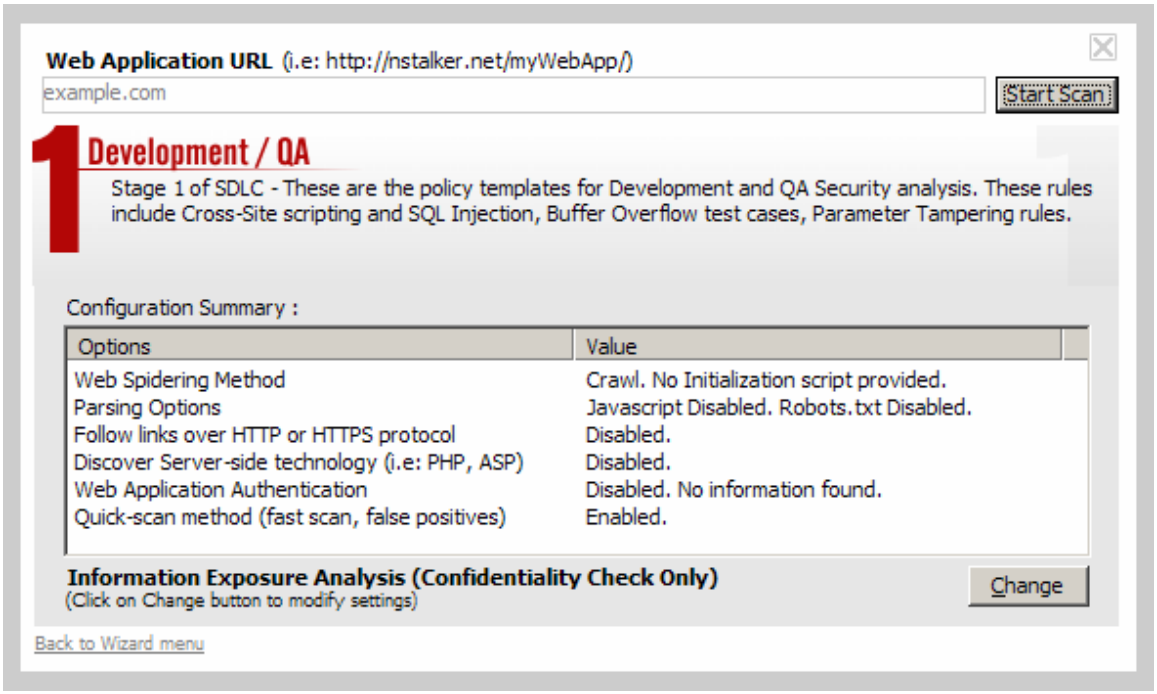
Once target URL is chosen, you must provide the scan policy to be used. To select it, double click on the policy of your choice (alternatively, you may also click on the policy of your choice and press “Next” button):




### 1.2.4. Customizing Scan Options

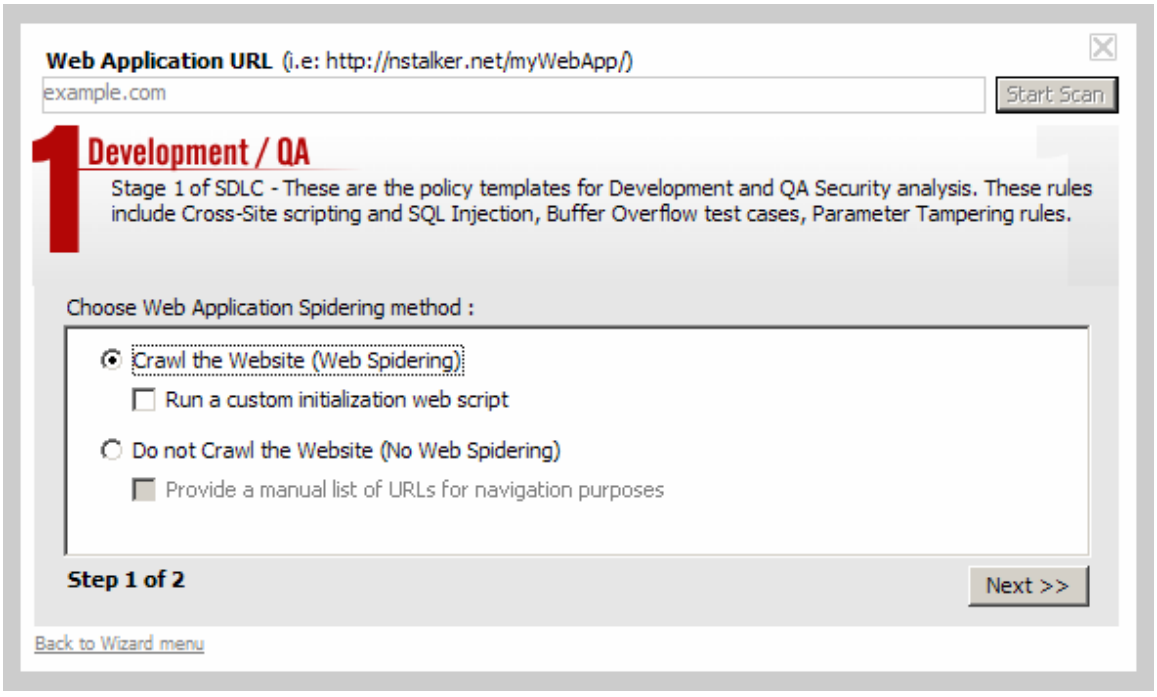
When target URL and scan policy are chosen, you will be prompted with a configuration summary. This is the list of options that can be customized to enhance N-Stalker capabilities:


All Rights reserved ZMT Comunicações e Tecnologia Ltda.




To modify settings, click on "Change" button. You will browse through a wizard interface that will allow you to change a set of host-based options before initiating scan. Options that can be modified include:

- **Step 1 - Web Spidering Options**




Allows you to modify Web Spider method:

✓ **Crawl Website**


All Rights reserved ZMT Comunicações e Tecnologia Ltda.

N-Stalker will follow Web Application hyperlinks and retrieve every possible resource found.

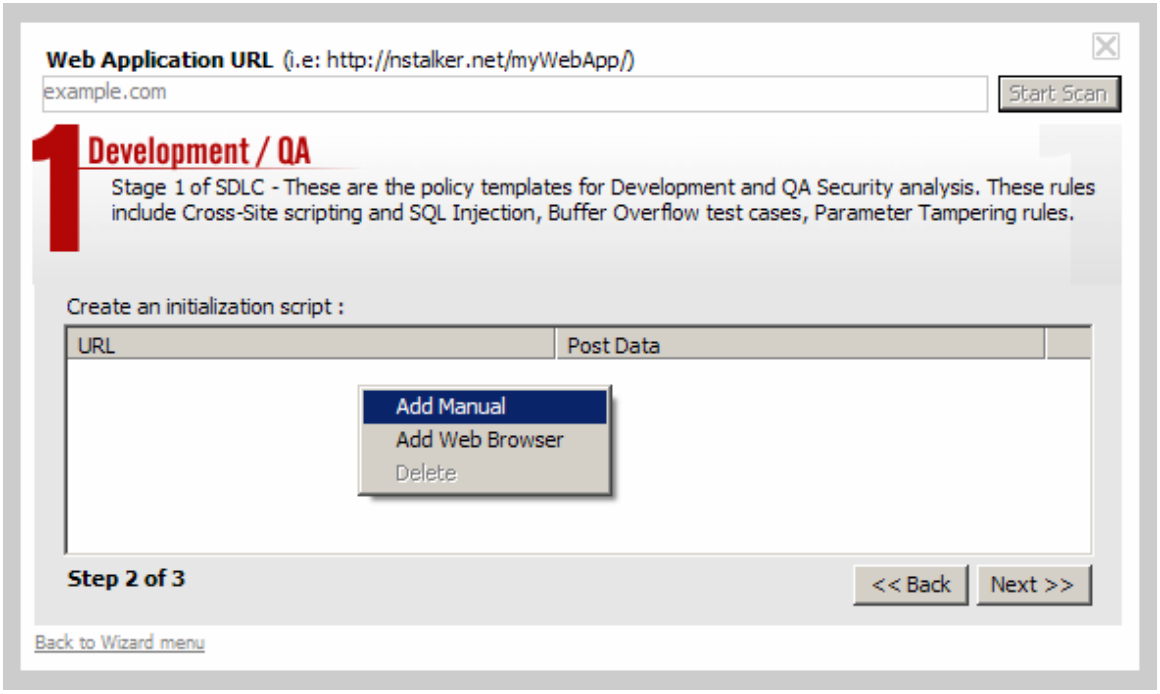
An initialization script can be recorded if you need to "teach" N-Stalker to go through a particular area of your Web Application. Just enable "Run a custom initialization web script".

✓ **Do not Crawl through Website**

N-Stalker will navigate through your web application but will neither follow hyperlinks nor retrieve web resources.

You may provide a manual list of URLs to be navigated. It may be recorded as either script or set of URLs. Just enable "Provide a manual list of URLs for navigation purposes".

- **Step 2 – Recording a web script**



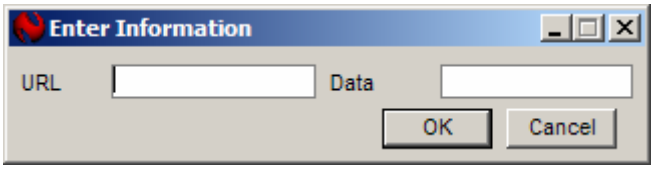

When you select to either "Run a custom initialization web script" or "Provide a manual list of URLs for navigation purposes", N-Stalker will allow you to record a web script. There are two options to add resources to the script (right-click on the list to obtain the menu):

✓ **Add Manual**

When manually adding resources, you must provide the URL to navigate and, if necessary, the Data to be submitted to this particular resource.

When Data is provided, N-Stalker will submit it using "POST" method, otherwise N-Stalker will use the Spider Method provided (default: "GET").


All Rights reserved ZMT Comunicações e Tecnologia Ltda.



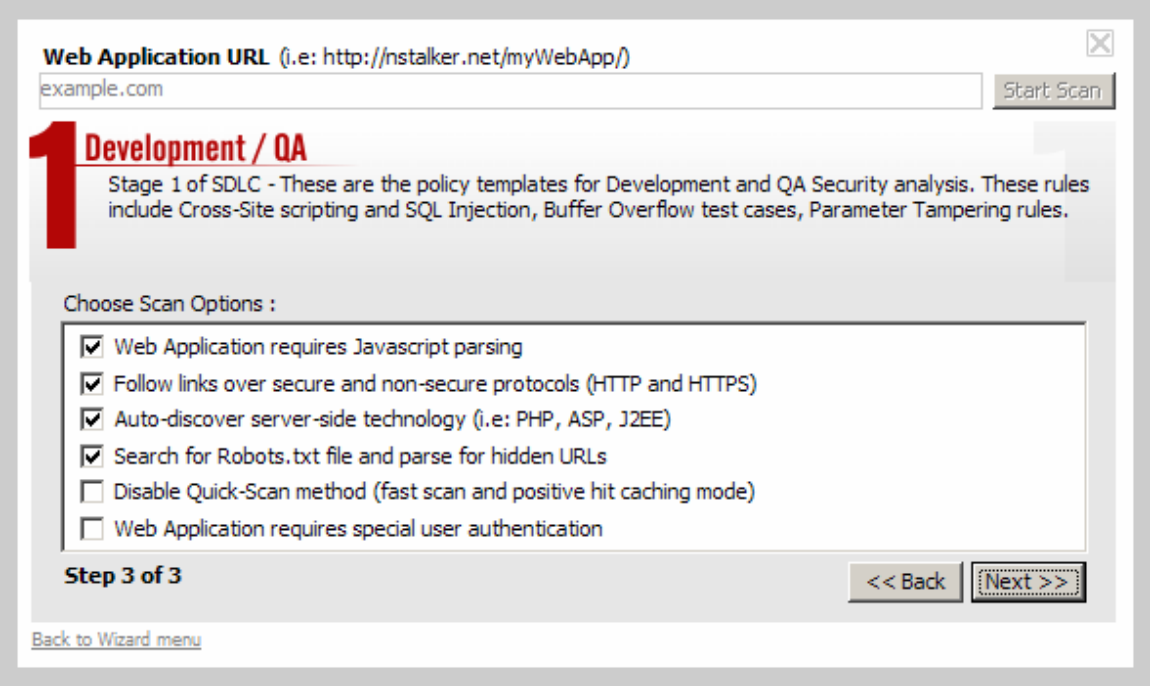

✓ **Add Web Browser**

If you choose to add resources via Web Browser, just navigate using N-Stalker browser interface. As you browse through different resources, a list of URLs and data information will be captured in the list below. If necessary, click on resource to modify it. If you need to delete it, right-click on resource and press "Delete" option.

Once navigation is done, choose "Yes" to add captured resources to N-Stalker permanently.


- **Step 3 – Choose Multiple Options**


All Rights reserved ZMT Comunicações e Tecnologia Ltda.




This interface will allow you to choose multiple options that may enhance N-Stalker scanning experience. Here is a brief description of each item:

- ✓ **Web Application requires Javascript parsing**

  When enabled, N-Stalker will parse javascript to extract possible URL resources.

- ✓ **Follows links over secure and non-secure protocol**

  When enabled, N-Stalker will follow either HTTP or HTTPS links, as long as destination URL is the same.

- ✓ **Auto-discover server-side technology**

  When enabled, N-Stalker will probe Web Application for common server-side development technologies, including PHP, J2EE, ASP (.NET), Cold Fusion, etc. Once detected, N-Stalker will create a special profile for each technology discovered.

- ✓ **Search for Robots.txt file and parse for hidden URLs**

  When enabled, N-Stalker will search for robots.txt file and it will try to extract hidden URLs to be inspected.

- ✓ **Disable Quick-Scan method**

  When enabled, N-Stalker will disable Quick-Scan method. That means it will exhaustively try every possible attack combination against an URL, extending the total scan time.

  **Tip:** Use this option carefully as it may cause false positives depending on the Web Application technology.

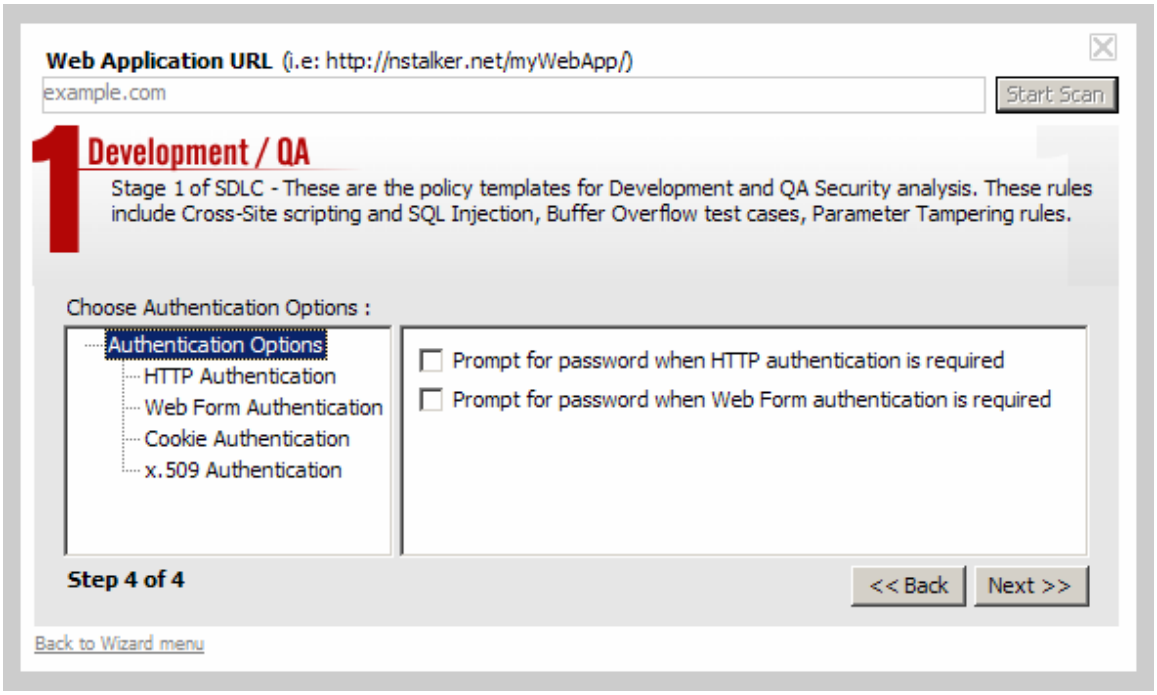

All Rights reserved ZMT Comunicações e Tecnologia Ltda.

✓ **Web Application requires special user authentication**

When enabled, N-Stalker will provide access to authentication configuration interface (step 4), allowing you to specify either HTTP, Web Form, x.509 certificate or Cookie authentication.

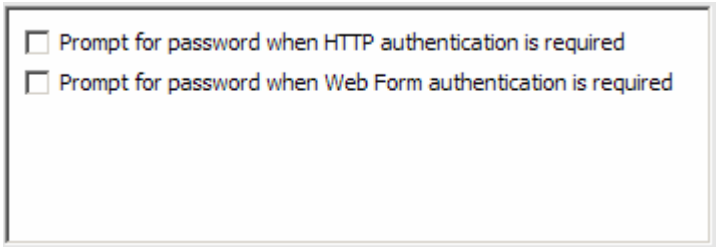
- **Step 4 – Authentication Options**

The Authentication Options interface allow you to configure how N-Stalker will interact with Web Application to get authenticated through existent access controls.




✓ **Authentication Options**

These options allow specifying if you should be prompted for manual authentication whenever N-Stalker found it is required in the Web Application.



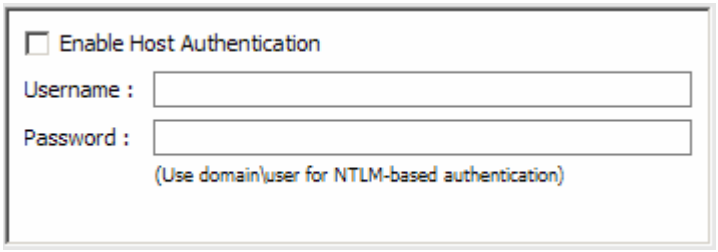

| | |
|---|---|
| **Prompt for password when HTTP** | When enabled, N-Stalker will manually prompt for user and password whenever a HTTP |


All Rights reserved ZMT Comunicações e Tecnologia Ltda.

| | |
|---|---|
| **authentication is required** | authentication is required. |
| **Prompt for password when Web Form authentication is required** | When enabled, N-Stalker will manually prompt for user and password whenever a web form authentication is required. |

✓ **HTTP Authentication**

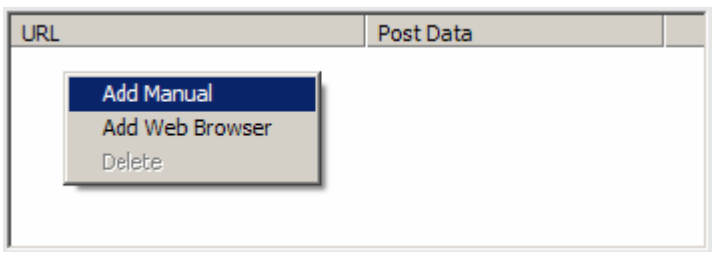
These options allow you to specify HTTP (Host) authentication (generally required by a 401 status code message).




| | |
|---|---|
| **Enable Host Authentication** | When host (HTTP) authentication is required, you must enable this option. |
| **Username** | Enter username for HTTP authentication. You may use MS Windows™ NTLM or Kerberos format. |
| **Password** | Enter password for HTTP authentication. |

✓ **Web Form Authentication**

These options allow you to record a web script for Web Form authentication. Similar to web script recorder tool (see Step 2), you may navigate through a web browser interface or manually provide a set of URL scripts to authenticate.




| | |
|---|---|
| **Add Manual** | This option allows you to manually specify an URL action to authenticate against the target Web Application. |
| **Add Web Browser** | This option allows you to record a |

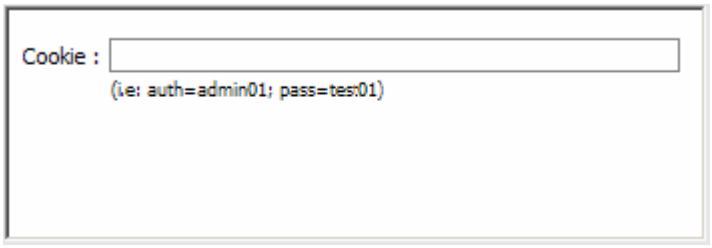

All Rights reserved ZMT Comunicações e Tecnologia Ltda.

| | |
|---|---|
| | web authentication script using a Web Browser interface. Once is done, you may also enter logout procedure to be filtered from spider mechanism. |
| **Delete** | Allows you to delete resources. |

**Tip:** When using Web Browser interface, you will be asked to record a logout script procedure. By doing so, you will avoid N-Stalker to mistakenly execute logout action and get itself out of Web Application authenticated context.

### ✓ Cookie Authentication

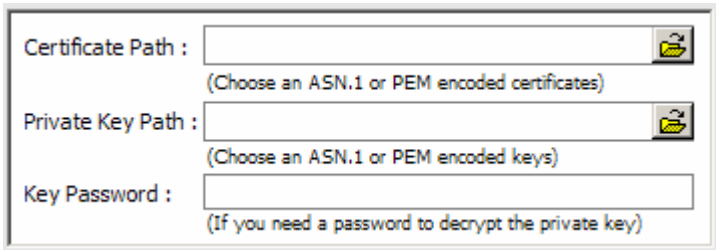
This option allows you to provide a cookie-based authentication to be used against target Web Application.




| | |
|---|---|
| **Cookie** | This option allows you to provide a cookie value to be transmitted on every communication with target Web Application. |

### ✓ x.509 Authentication

If Web Application requires a client-side certificate for authentication purposes, you may provide x.509 information through this interface.




| | |
|---|---|
| **Certificate Path** | This option allows you to provide the x.509 Certificate file path in ASN.1 or PEM encoded format. |
| **Private Key Path** | This option allows you to provide the Private key file path in ASN.1 or PEM encoded format. |


All Rights reserved ZMT Comunicações e Tecnologia Ltda.

| | |
|---|---|
| **Key Password** | This option allows you to provide a password string to decrypt Private key if necessary. |

### 1.2.5. Initiating Scan Session

Once satisfied with Configuration options, you may press “Start Scan” to initiate Scan Session. The N-Stalker Policy Editor component will be minimized and you will be taken to the N-Stalker Web Application Security Scanner Engine.

## 1.3. Running Scan Engine

### 1.3.1. Initiating Scan Session

N-Stalker Web Application Security Scanner Engine interface is responsible to run security tests against target Web Application. Once you have chosen the correct options and scan policy, you will be required to initiate scan session by clicking on “Play” button (green color) on the left side of Engine’s toolbar.

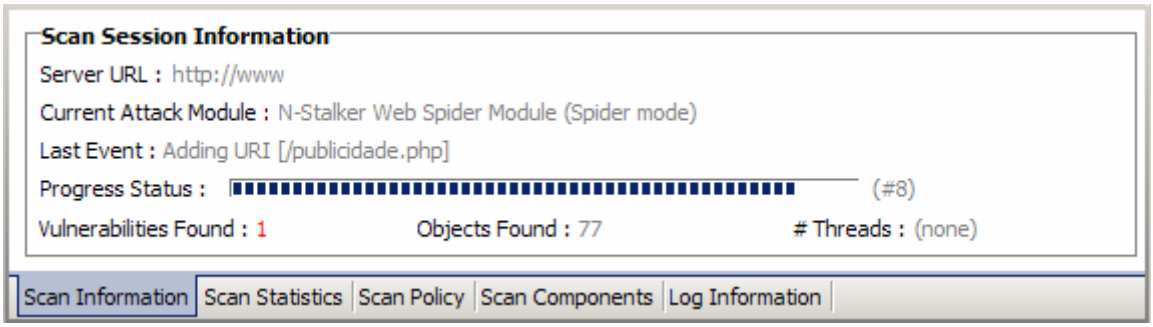

N-Stalker Web Application Security Scanner’s toolbar has the following available controls:

| | |
|---|---|
| **Play (Button)** | This button will initiate Scanner Engine’s activities in their very beginning. It may also be used to resume suspended sessions. |
| **Stop (Button)** | This button will stop Scanner Engine’s activities and quit current scan session. A quit dialog will be displayed for additional instructions. |
| **Pause (Button)** | This button will suspend temporarily Scanner Engine’s activities. Session may be resumed by pressing “Play” button. |
| **Forward (Button)** | This button will skip current scan module or activity. N-Stalker Scanner Engine may require an additional time to stop current activity which will cause a status message to be displayed in the application’s status panel (bottom). |

### 1.3.2. Understanding Scan Engine Interface

#### 1.3.2.1. Scan Information

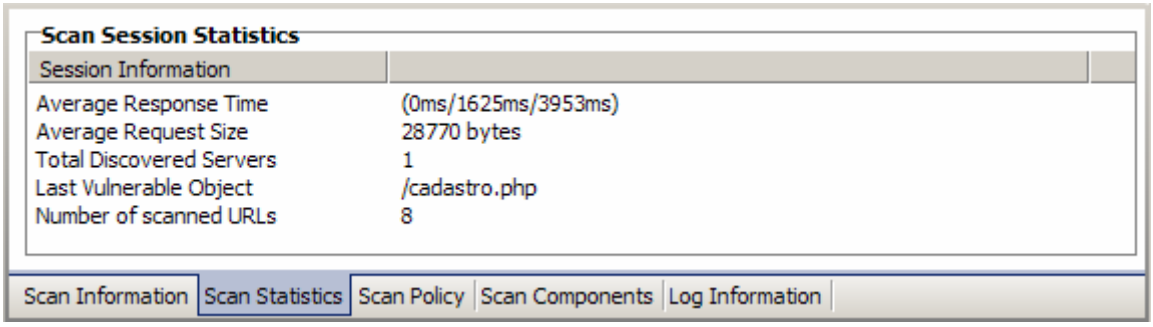

All Rights reserved ZMT Comunicações e Tecnologia Ltda.




Scan Session Information provides details on current attacks being executed, progress status, number of vulnerabilities and objects already found. See more details below:

| | |
|---|---|
| **Server URL** | URL of target Web Application being scanned. |
| **Current Attack Module** | The name of the current attack module being executed. |
| **Last Event** | Last relevant event discovered by N-Stalker. |
| **Progress Status** | Progress status of the current attack module. |
| **Vulnerabilities Found** | Number of vulnerabilities found. |
| **Objects Found** | Number of objects (including scripts, comments, e-mails, cookies, etc) found. |
| **Threads** | Number of parallel threads currently in execution. |

### 1.3.2.2. Scan Statistics



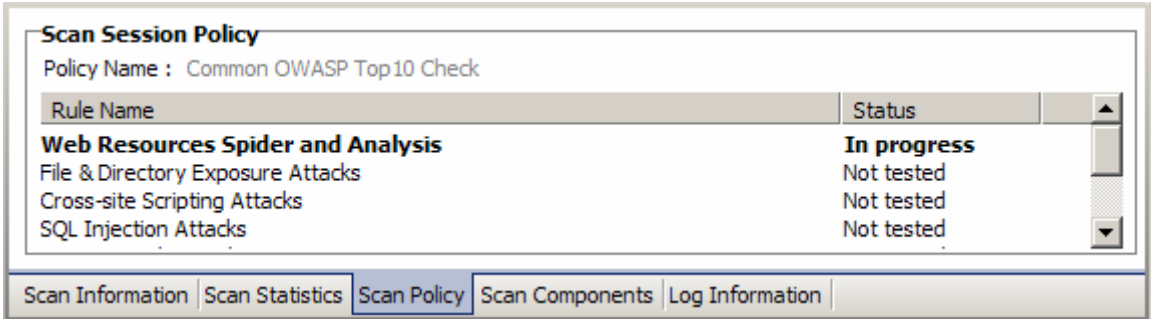

Scan Session Statistics provides details on various engine statistics, including time response, response size, number of servers discovered and URLs scanned.

| | |
|---|---|
| **Average Response Time** | Minimum, average and maximum response time obtained while scanning target URL. |
| **Average Response Size** | Average size (in bytes) of response obtained while scanning target URL. |
| **Total Discovered Servers** | Number of distinct Web servers found while scanning target URL. |
| **Last Vulnerable Object** | The URI of the last object found to carry a vulnerability. |
| **Number of scanned URLs** | Number of URLs already scanned. |


All Rights reserved ZMT Comunicações e Tecnologia Ltda.

| | |
|---|---|

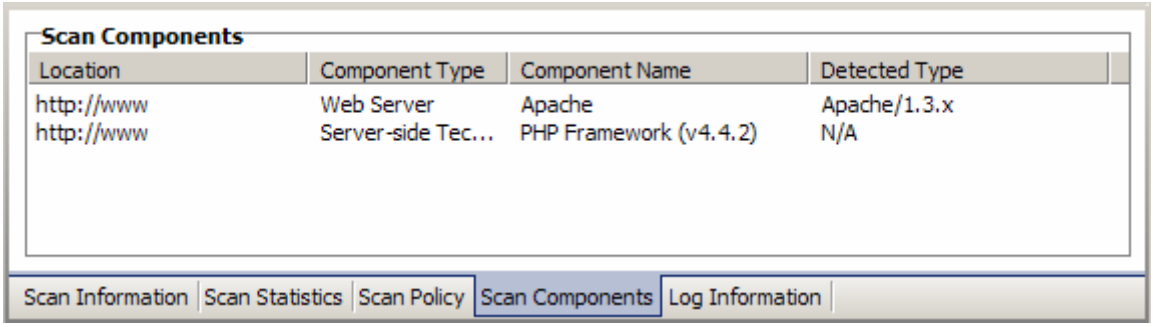
### 1.3.2.3. Scan Policy




Scan Session Policy provides details on the status of different security check rules that form the entire Scan Policy.

| | |
|---|---|
| **Policy Name** | Name of the Scan Policy being used. |
| **Rule Table** | Rule table provides the name of the rule and its current status:<br>• **In progress:** currently in execution<br>• **Not tested:** scheduled to be executed<br>• **OK:** already tested |

### 1.3.2.4. Scan Components



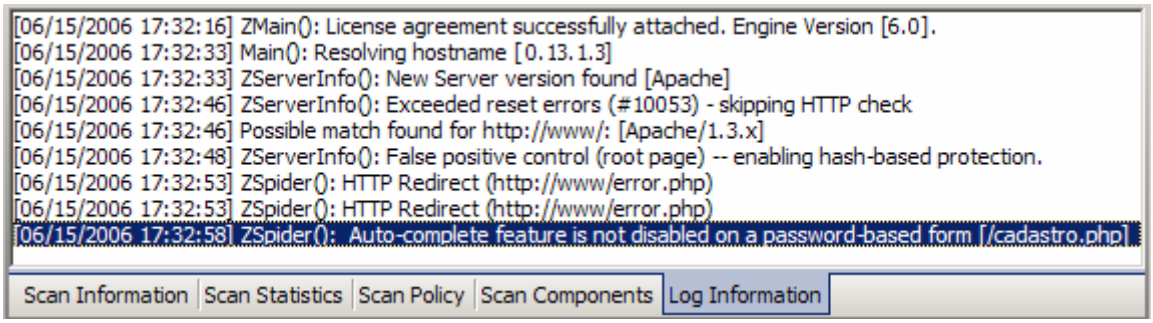

Scan Components provide details on the web components fingerprinted and detected in the Web Application.

| | |
|---|---|
| **Location** | URL of the detected component. |
| **Component Type** | Type of detected component. Most common components are Web Server and Server Side Technology. |
| **Component Name** | Name of detected component. |
| **Detected Type** | Type of detected component when fingerprinted. This currently applies only for |


All Rights reserved ZMT Comunicações e Tecnologia Ltda.

| | |
|---|---|
| | Web Servers. |

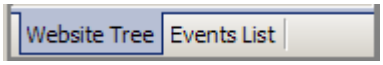
### 1.3.2.5. Log Information




Log Information provides details on various events executed by N-Stalker, including error messages, redirections, results of security checks and license information. It is useful also for debugging purposes.

## 1.3.3. Inspecting Website Tree

The Website Tree interface is a panel located in the left side of N-Stalker Scanner Engine. It is meant to provide details on URI resources found during Engine's activities – being it crawling or navigating.

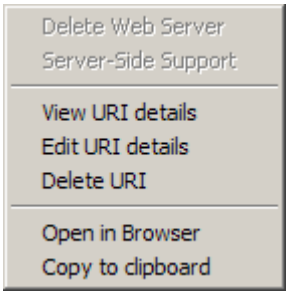



### 1.3.3.1. Website Tree Options

Website Tree Options allow you to view and modify URI details, delete URI and modify server-side configuration. There are two ways to invoke them:

- **Select a URI resource and right-click on it**

These are the options for URI resource context menu:

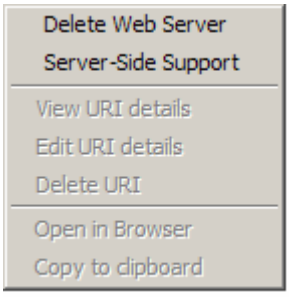



| | |
|---|---|
| **View URI details** | This option will open "View URI details" window, showing request and response detail, exploit terminal (for manual tests), browser view and hex view. |
| **Edit URI details** | This option allows you to change |


All Rights reserved ZMT Comunicações e Tecnologia Ltda.

| | |
|---|---|
| | some aspects of URI, including URI string itself, Post data and Session Information. |
| **Delete URI** | This option will remove URI from Website Tree. |
| **Open in Browser** | This option will open the URI in your default web browser. |
| **Copy to clipboard** | This option will copy the entire URL into the clipboard. |

- **Select a server (URL) and right-click on it**

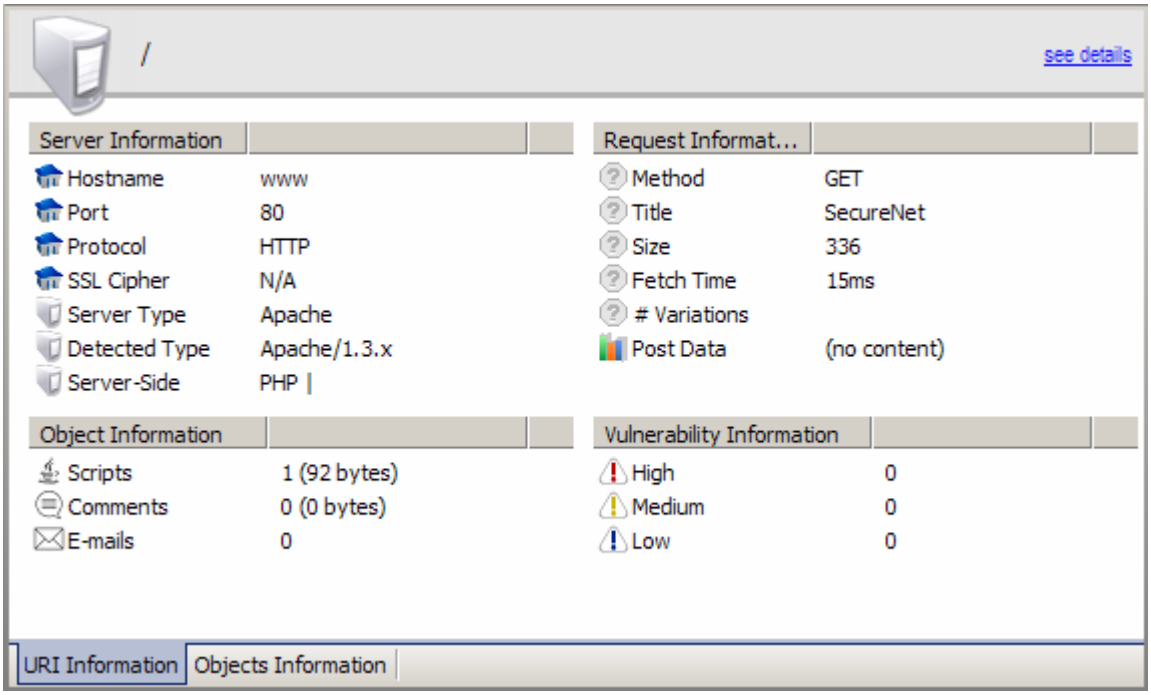



| | |
|---|---|
| **Delete Web Server** | This option will remove a secondary web server and child nodes from Website tree. It does not apply to primary server (target's URL). |
| **Server-Side Support** | This option allows you to modify server-side support configuration for a particular web server, including fingerprinted results such as PHP, ASP and J2EE support. |

### 1.3.3.2. URI Information

When an URI resource is selected in Website Tree, its details will be displayed in the "URI Information" tab, located on the bottom right side of Engine's interface.


All Rights reserved ZMT Comunicações e Tecnologia Ltda.




| | |
|---|---|
| **Hostname** | Hostname of the Web server where URI resource has been found. |
| **Port** | TCP Port of the Web server where URI resource has been found. |
| **Protocol** | Transportation protocol, being it either **HTTP** (plain text web protocol) or **HTTPS** (encrypted web protocol). |
| **SSL Cipher** | When transported over HTTPS, it should display the encryption cipher being used. |
| **Server Type** | Type and version of web server as it is announced. |
| **Detected Type** | Type and version of web server detected after being fingerprinted by N-Stalker. |
| **Server-Side** | Type of server-side technologies supported by the server, such as PHP, ASP (.NET), J2EE, etc. |
| **Method** | HTTP Method used to retrieve the URI resource. |
| **Title** | HTML Title of the retrieved URI resource. |
| **Size** | Size (in bytes) of URI resource. |
| **Fetch Time** | Time taken to receive the resource from Web server. |
| **# Variations** | Number of URI variations. Variations can be compared by evaluating strings after question mark character (“?”). |
| **Post Data** | When HTTP POST method is used, this field will display the data being transmitted to the server. |
| **Scripts** | Number of HTML scripts parsed from URI resource and its size in bytes. |
| **Comments** | Number of HTML comments parsed from URI resource and its size in bytes. |
| **E-mails** | Number of e-mail addresses found in URI resource. |

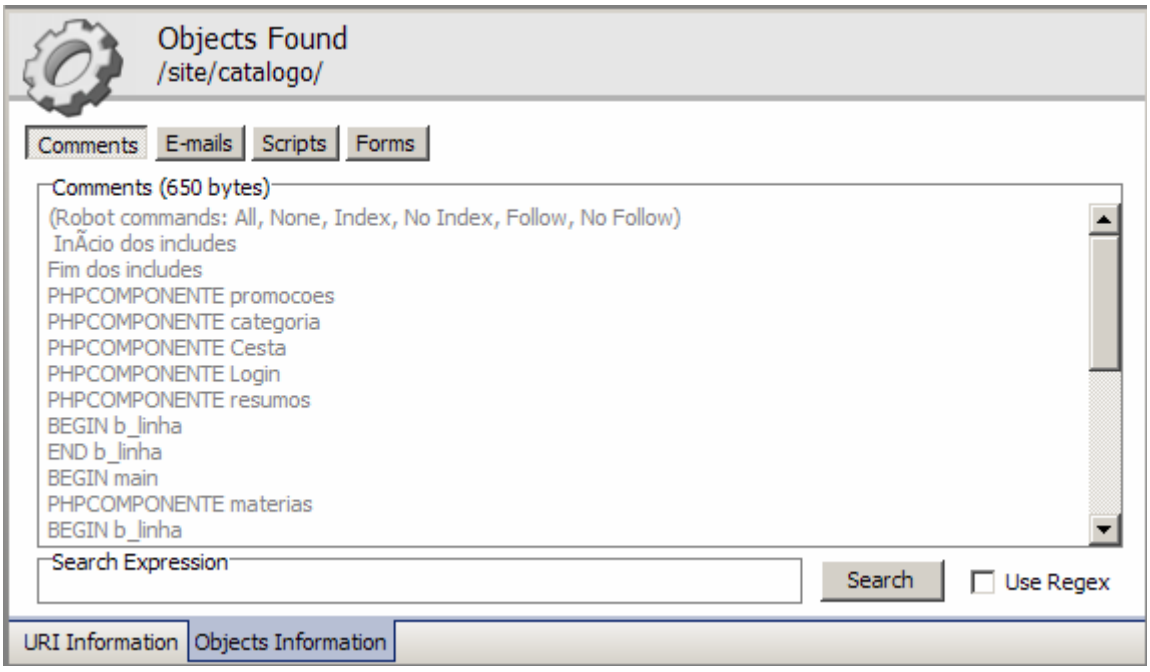

All Rights reserved ZMT Comunicações e Tecnologia Ltda.

| | |
|---|---|
| **High** | Number of high level vulnerabilities found in URI resource. |
| **Medium** | Number of medium level vulnerabilities found in URI resource. |
| **Low** | Number of low level vulnerabilities found in URI resource. |
| **See Details** | Click on this hyperlink to open "View URI details" window and obtain more details about this request (see section 4.3.3.4). |

### 1.3.3.3. Objects Information

"Objects Information tab" is a section where you may find every details and aspects of a particular URI resource, including HTML comments and Scripts being found, E-mails addresses and Web Forms.

- **Comments**

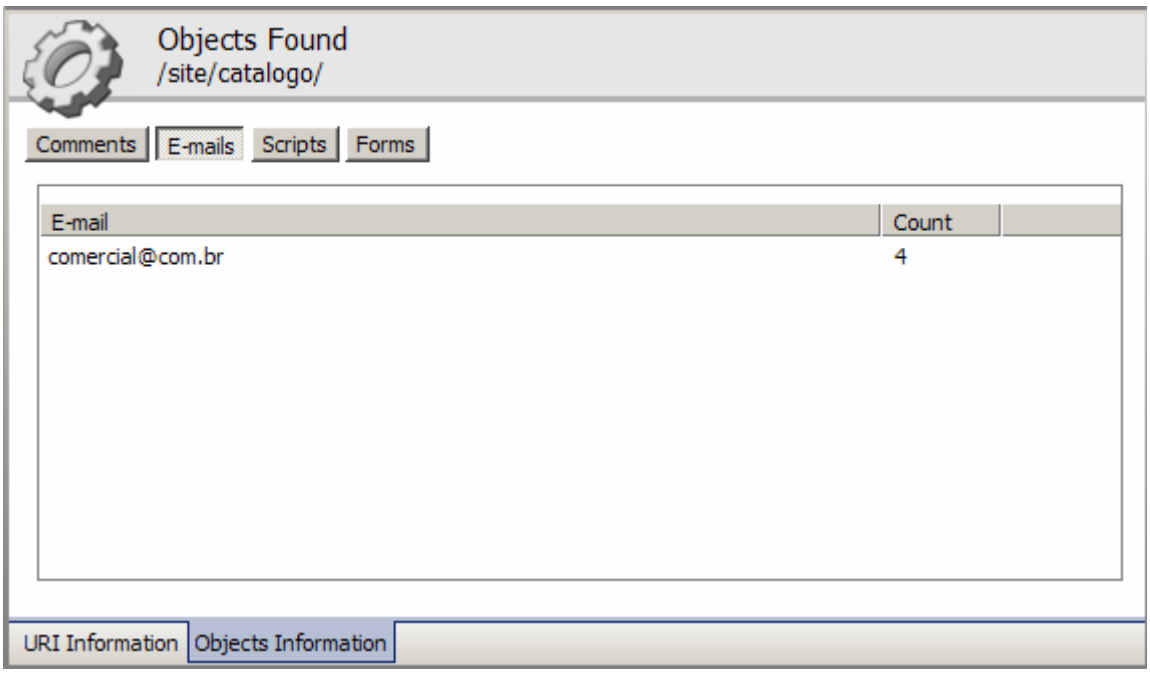



| | |
|---|---|
| **Comments** | This field will display all HTML comments being extracted from URI resource and the total size of it in bytes. |
| **Search Expression** | You may provide here custom keywords to be searched among HTML comments strings. |
| **Search (Button)** | Once search expression is filled, press this button to start searching for it among HTML comments. |
| **Use Regex** | If you wish to provide regular expression keywords for search |


All Rights reserved ZMT Comunicações e Tecnologia Ltda.

| | |
|---|---|
| | purposes, enable this option first. |

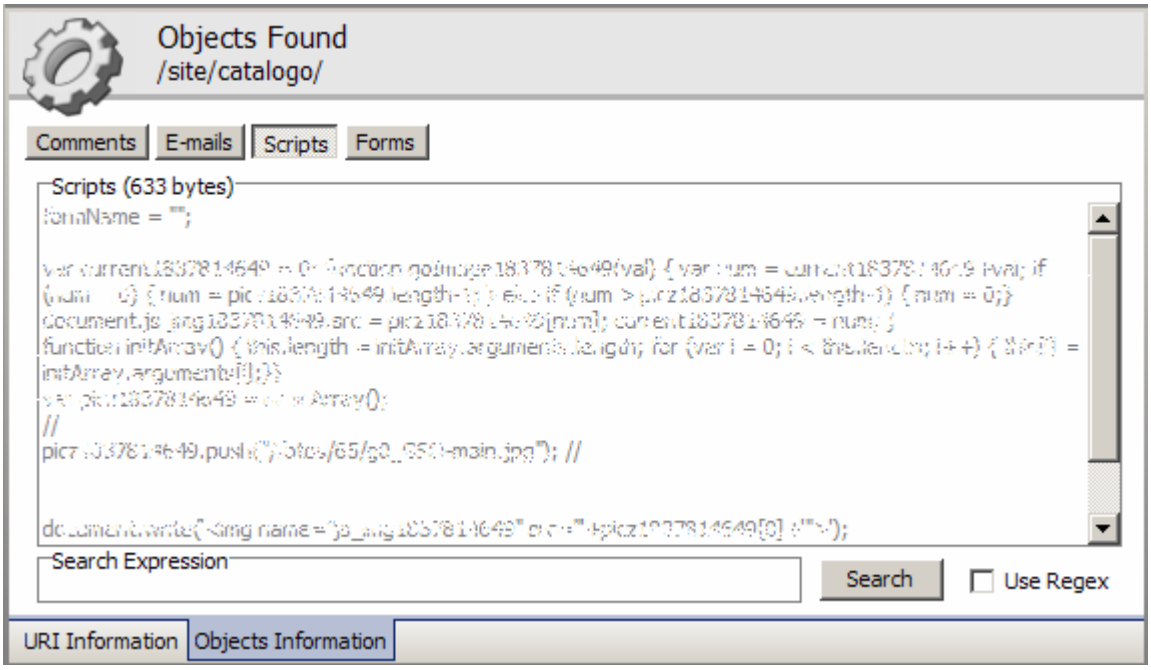
- **E-mails**




| | |
|---|---|
| **E-mail** | This field will display all e-mail addresses being found in the URI resource. |
| **Count** | This field provides the number of times this e-mail address has been exposed along with the Web Application. |

- **Scripts**

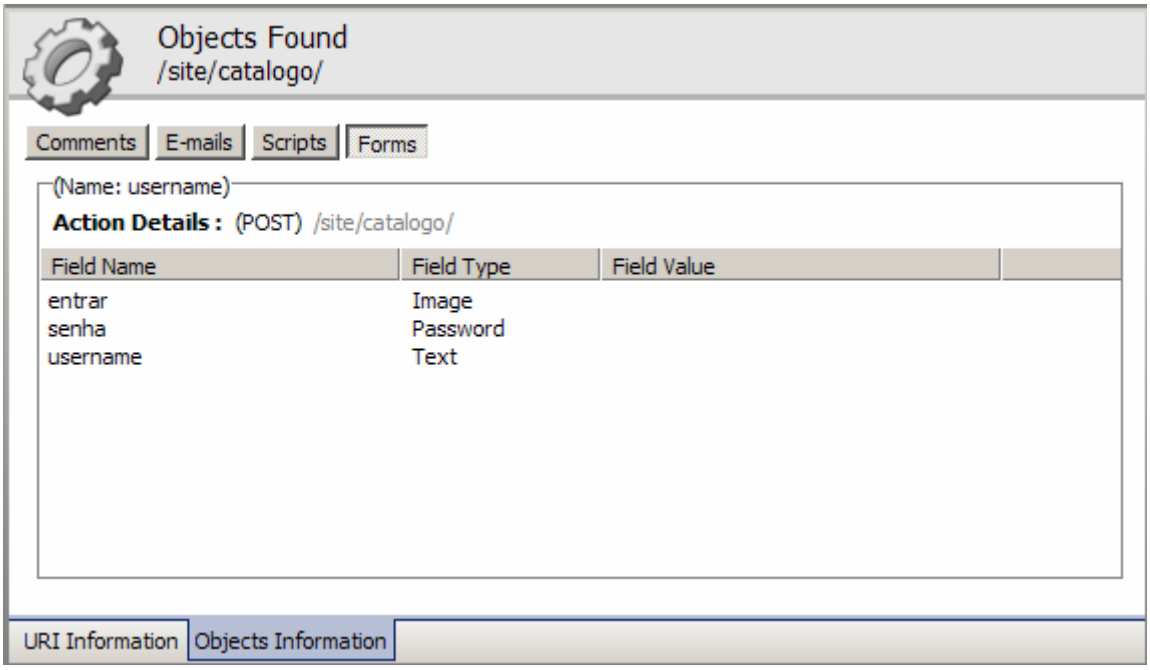

All Rights reserved ZMT Comunicações e Tecnologia Ltda.




| | |
|---|---|
| **Scripts** | This field will display all HTML scripts being extracted from URI resource and the total size of it in bytes. |
| **Search Expression** | You may provide here custom keywords to be searched among HTML scripts strings. |
| **Search (Button)** | Once search expression is filled, press this button to start searching for it among HTML scripts. |
| **Use Regex** | If you wish to provide regular expression keywords for search purposes, enable this option first. |

- **Forms**


All Rights reserved ZMT Comunicações e Tecnologia Ltda.




| | |
|---|---|
| **Name** | This field will display the name of the Web Form. If no name is provided, N-Stalker will assume the first form field found. |
| **Action Details** | This field will display HTTP method to be used and URL action to send information to. |
| **Field Name** | Name of the field as extracted from URI resource. |
| **Field Type** | Type of the field, being it **Text**, **Numeric**, **Image**, **Hidden** and **Password**. |
| **Field Value** | Value content of Form field, if any, is found. |

### 1.3.3.4. Viewing URI details

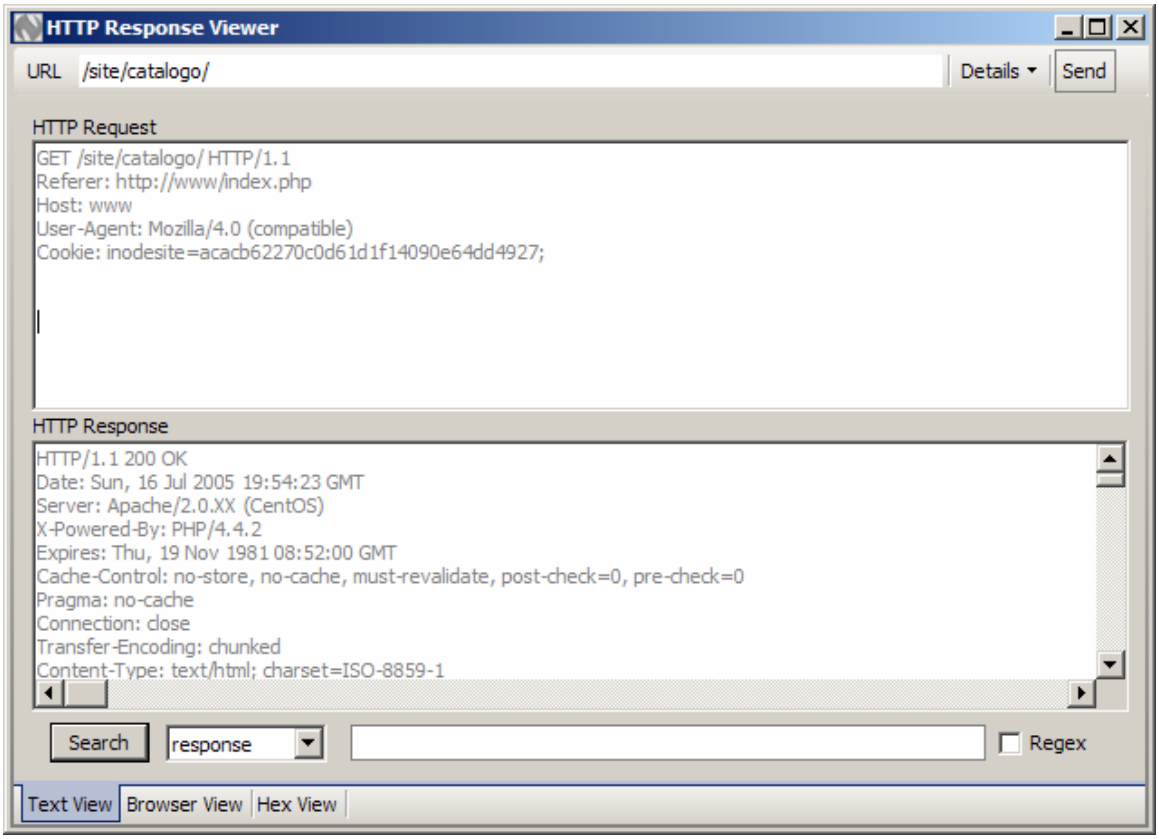
You may invoke "View URI details" by either clicking on "See details" hyperlink in the "URI Information" tab (see section 4.3.3.3) or right-clicking over a resource on Website Tree and choosing "View URI details" in the context menu (see section 4.3.3.1).

There are three (3) different views that can be used to learn more details about a particular URI resource and even interact with it.

- **Text View**

  Text View allows you to visualize raw request and response from N-Stalker communication to target's Web Server. It also allows you to search custom keywords or regular expressions among request and response strings.


All Rights reserved ZMT Comunicações e Tecnologia Ltda.




| | |
|---|---|
| **HTTP Request** | This field will display the raw request string being used by N-Stalker to send to Web server. |
| **HTTP Response** | This field will display the raw response string received from the Web server as result of the request. |
| **Search (Button)** | Search button can be used to trigger the search of custom keywords among request or response strings. Use the blank field to provide the desired keywords. |
| **Request / Response (combo box)** | This combo box is used to switch from Request or Response when searching for custom keywords . |
| **Regex** | You may provide regular expression keywords to be searched. Enable this option to do so. |

- **Using Text View as Exploit Terminal**

  You may use Text View as an Exploit Terminal, modifying certain aspects of the request and have it sent back to the server in real–time.



All Rights reserved ZMT Comunicações e Tecnologia Ltda.

Just modify URL field or click on "Details" option and provide "Post Content" information to submit information to the web server. When done, press "Send" button.

- **Browser View**

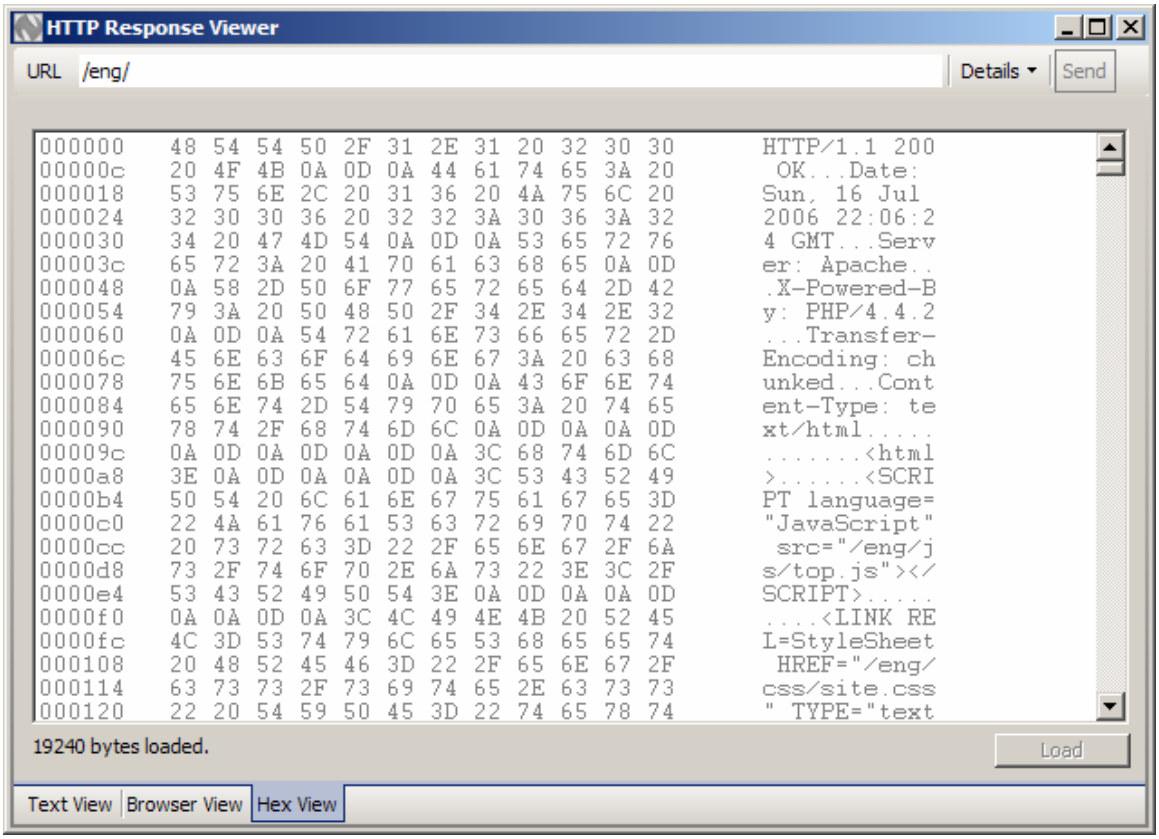
Browser View allows you to visualize the response sent by Web Server as if it was requested from a standard Web Server.


| | |
|---|---|
| **Request On-line Resource** | Use this option to force a N-Stalker Web Browser interface to request fresh content directly from Web Server. |
| **Use always on-line browser** | If you prefer to always visualize fresh content directly from Web server, just enable this option. |

- **Hex View**

Hex View allows you to visualize the entire request separated in a table with its hexadecimal equivalent symbol.

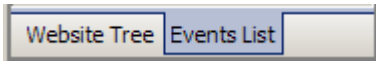

All Rights reserved ZMT Comunicações e Tecnologia Ltda.




| | |
|---|---|
| **Load** | Click on "Load" button to display request in hexadecimal table. |

### 1.3.4. Inspecting Events List

"Events List" interface is a panel located in the left side of N-Stalker Scanner Engine. It is meant to provide details of vulnerabilities and objects found during Engine's activities.

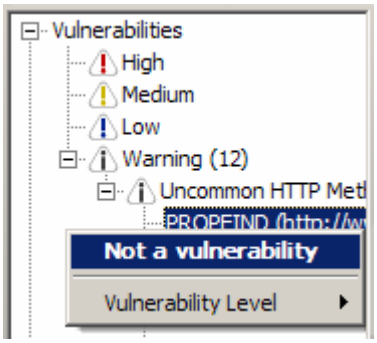



#### 1.3.4.1. Vulnerabilities

When inspecting the list of vulnerabilities found by Scanner Engine, you either visualize or modify its details:

- **Modifying Vulnerability Details**


All Rights reserved ZMT Comunicações e Tecnologia Ltda.

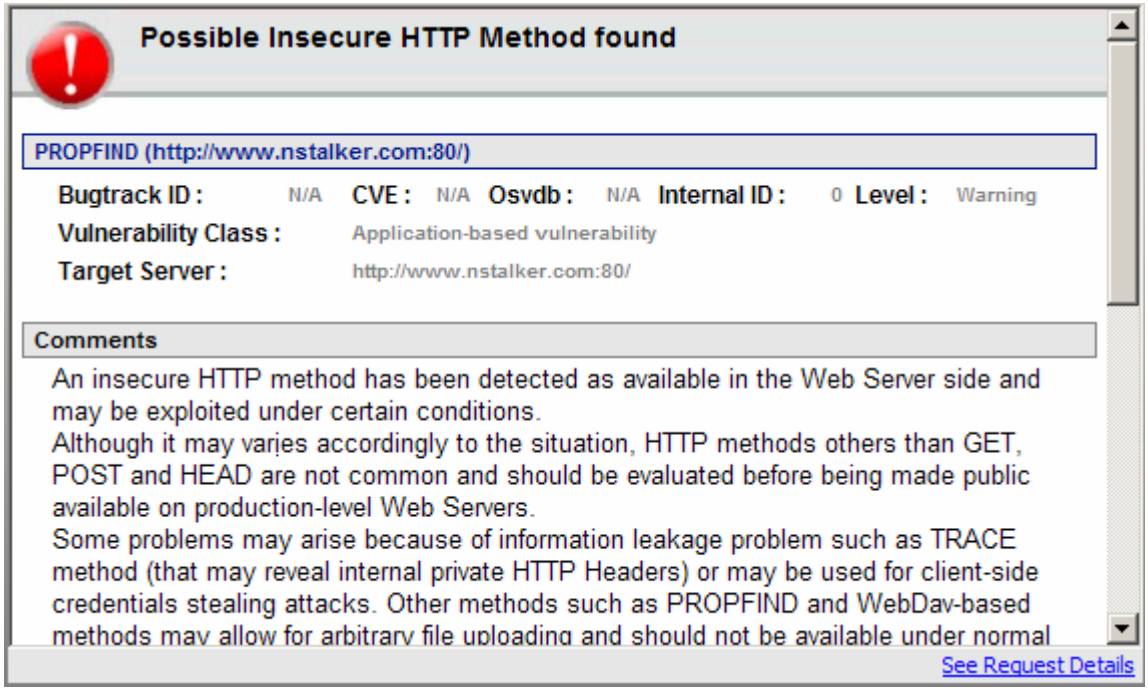



If you do not agree with the default critical level classification, you may modify it by right-clicking on a vulnerability and choosing the preferred level from "Vulnerability Level" option.

If a particular event is not considered a vulnerability under your perspective, it may be removed by also right-clicking on a vulnerability and choosing "Not a vulnerability" option.

- **Visualizing Vulnerability Details**

To visualize details of a particular vulnerability, click on it. Information will be displayed in the panel located in the bottom right side of Engine's interface.



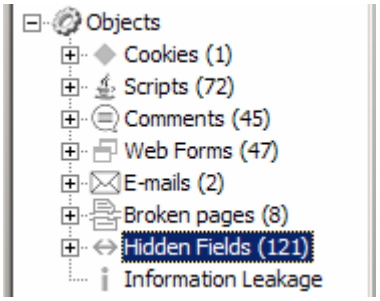

To visualize more information about a particular vulnerability, click on "See Request Details" to trigger the "View URI details" window. From that point onwards, you will be able to investigate request and response information on three distinct views (Text, Browser and Hex – see section 4.3.3.4).

If no information is available an error message ("No Information available") will appear at the bottom of the panel:


All Rights reserved ZMT Comunicações e Tecnologia Ltda.

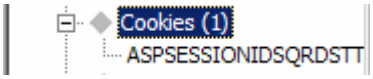

### 1.3.4.2. Objects

During scanning session, you will be allowed to inspect various different web objects found by the Scanner Engine. Ranging from Cookies to exposed meta tag information, you may search custom keywords and regular expressions similar to "Object Information" tab from Website Tree (section 4.3.3.3).

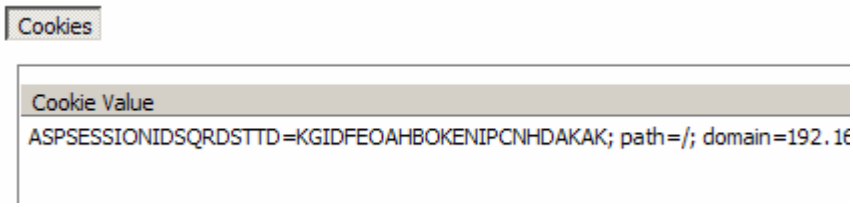



These are the list of objects and available functionalities:

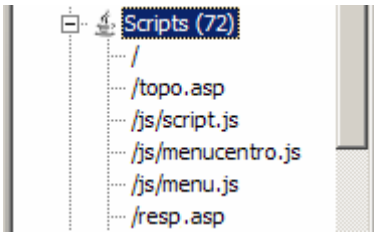
- **Cookies**




This item will display a sortable list of cookies found during Scan Engine's activities.



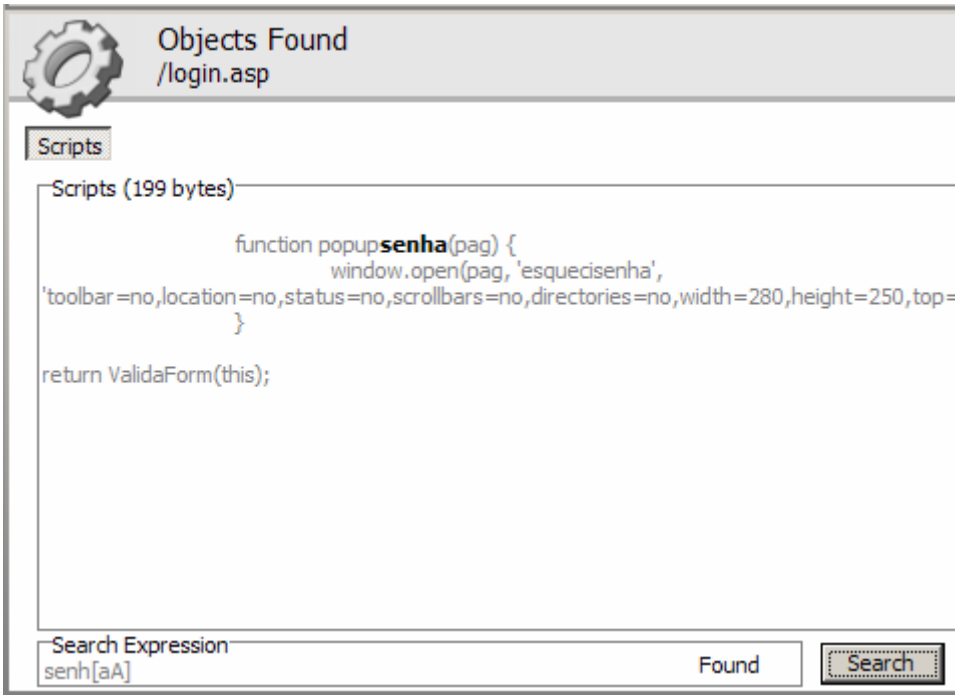

- **Scripts**



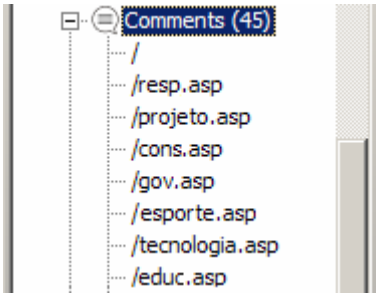


All Rights reserved ZMT Comunicações e Tecnologia Ltda.

This item will provide a list of URI resources containing HTML scripts. By clicking on a particular resource, you will have the ability to list its contents and search custom keywords or regular expressions.

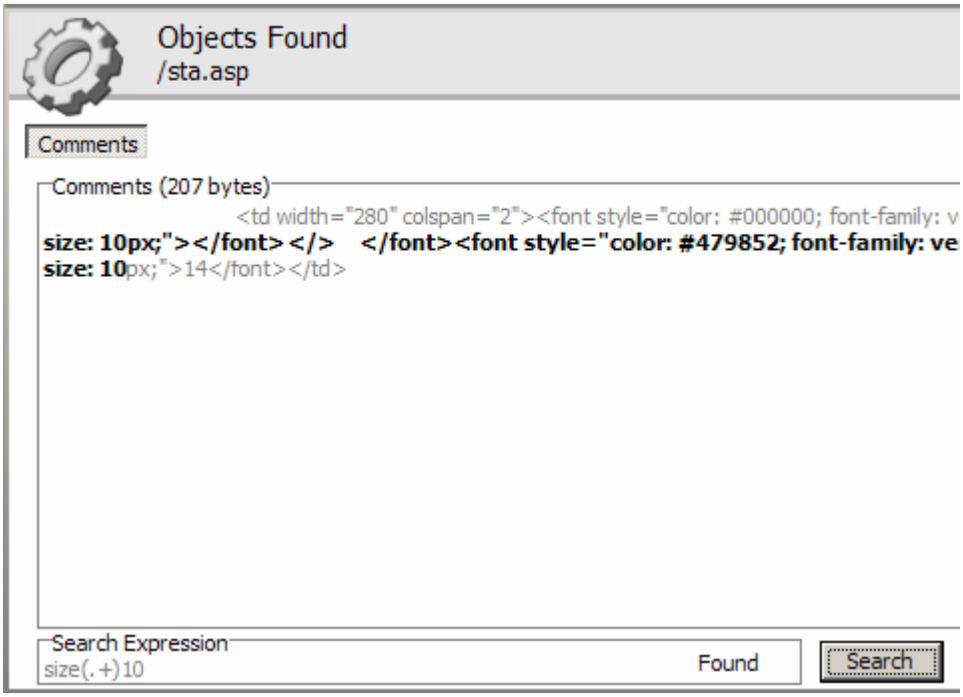



- **Comments**

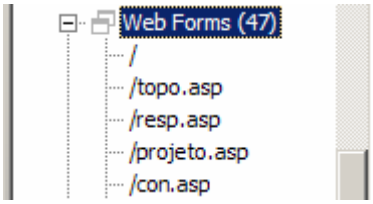



This item will provide you with a list of URI resources containing HTML comments. By clicking on a particular resource, you will have the ability to list its contents and search custom keywords or regular expressions.

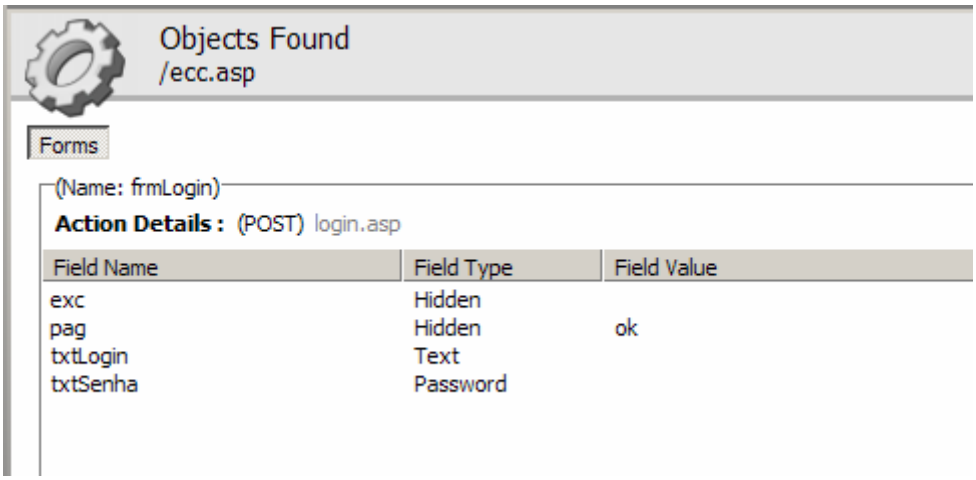

All Rights reserved ZMT Comunicações e Tecnologia Ltda.




- **Web Forms**



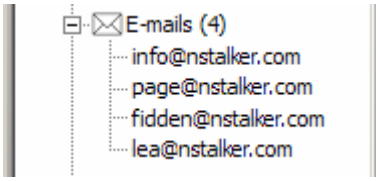

This item will provide you with a list of URI resources containing Web Forms. By clicking on a particular resource, you will obtain details about web form, input fields, HTTP method and action.





All Rights reserved ZMT Comunicações e Tecnologia Ltda.

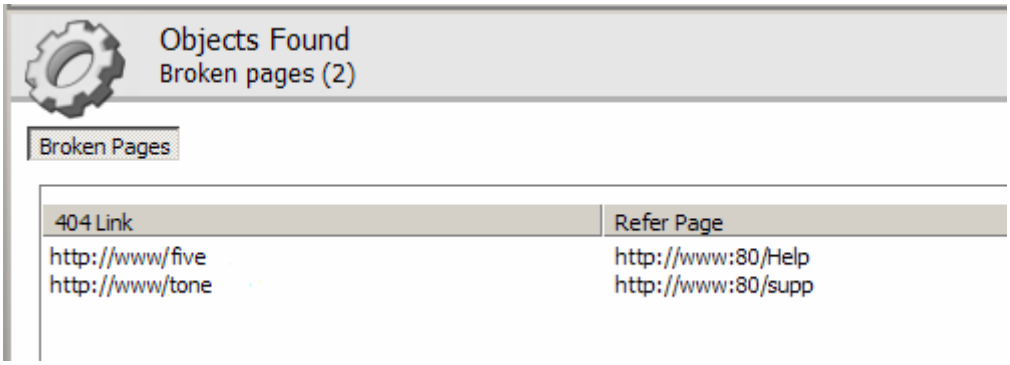
- **E-mails**



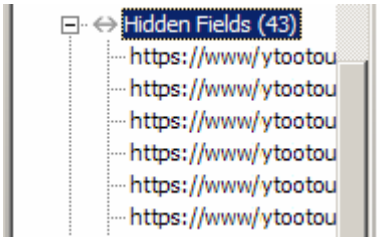

This item will provide you with the list of e-mails extracted during Scanner Engine's activities. By clicking on a particular e-mail address, you may learn how many times it was exposed in the Web Application.

- **Broken Pages**


This item will provide you with the list of broken pages found during Scanner Engine's activities. URLs are listed along with the refer page.

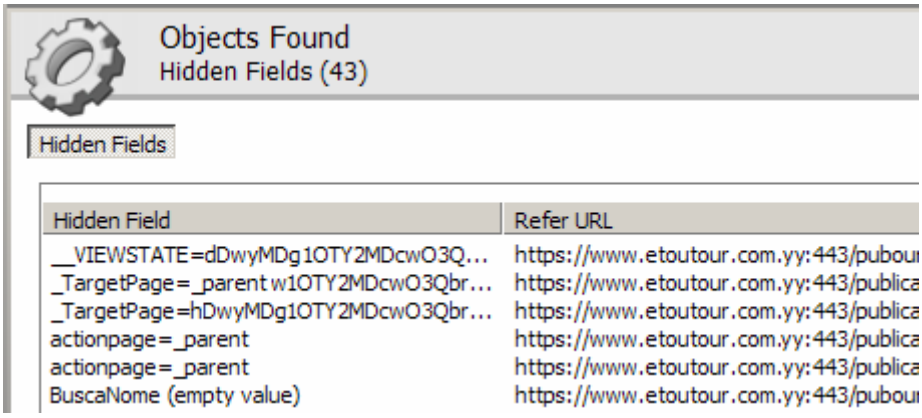



- **Hidden Fields**

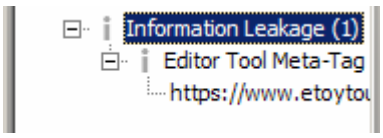



This item will provide you with the list of hidden fields from Web Forms found during Scanner Engine's activities. You may inspect the name and value of hidden fields as well as the URL of its original location.

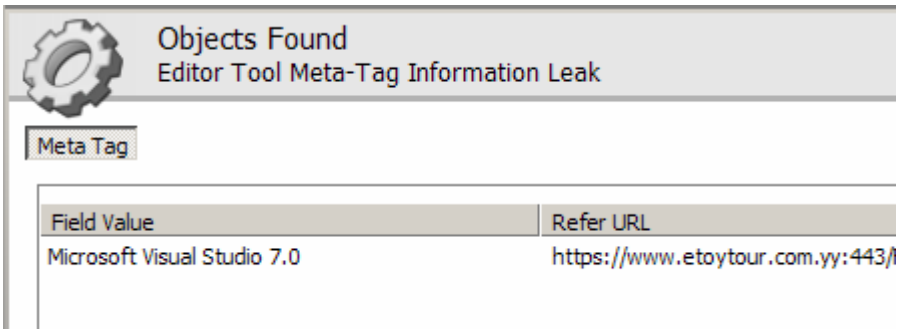

All Rights reserved ZMT Comunicações e Tecnologia Ltda.




- **Information Leakage**

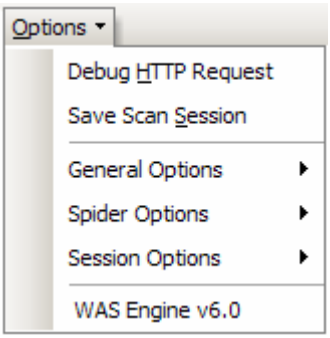



This item will provide you with the list of all meta-tags that may possibly represent an information leakage. You may inspect tag values and obtain the original URL where resource was found.




### 1.3.5. Managing Scan Engine Options

During scanning session, user is allowed to modify settings, provide new resources and inspect resources found. These all can be done by clicking on “Options” menu in the right side of Engine’s toolbar.

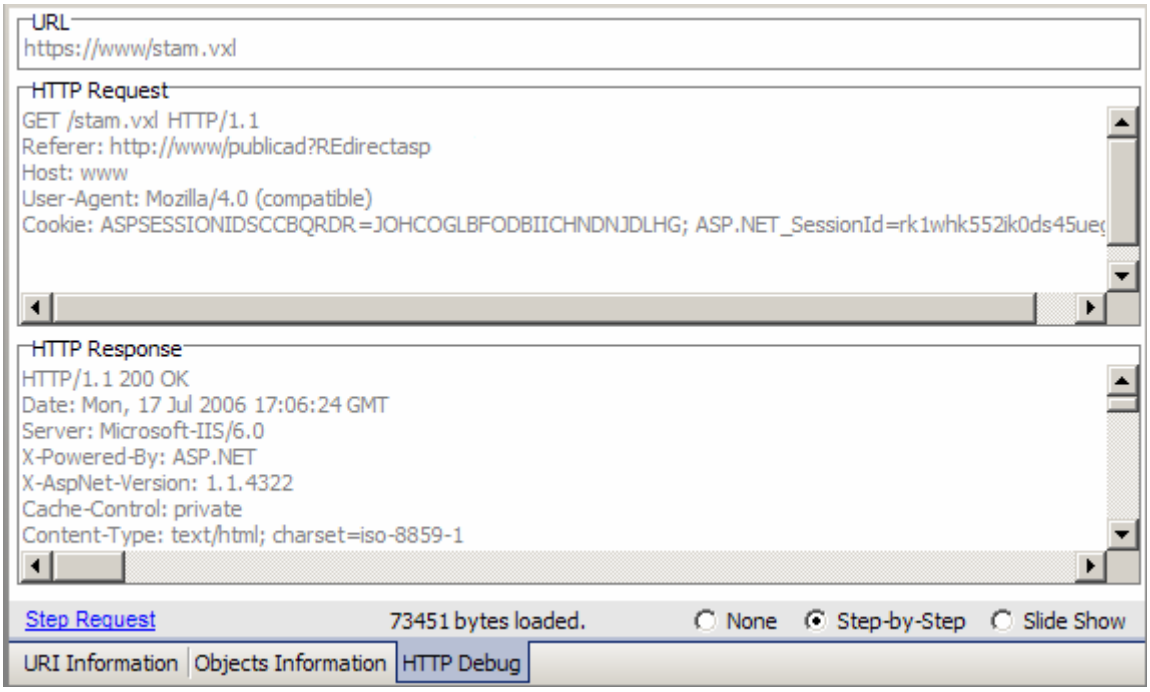




All Rights reserved ZMT Comunicações e Tecnologia Ltda.

### 1.3.5.1. Debugging Scan Engine Transactions

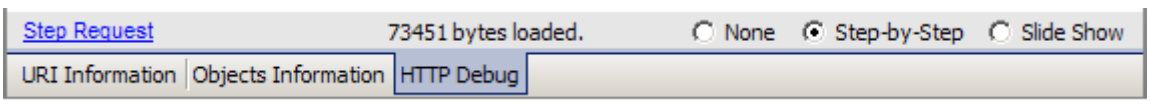
When crawling for web resources (spider mode), N-Stalker Scanner Engine can be intercepted for debugging purposes. This is especially interesting when a particular request must be modified before being sent to the web server or even if you just want to watch navigation to observe resource details.




Among displayed properties, there are:

| | |
|---|---|
| **URL** | The Correspondent URL part of the debugged HTTP request (read-only). |
| **HTTP Request** | Raw HTTP request that will be sent to the server (read-write). It can be modified before being submitted. |
| **HTTP Response** | The Correspondent Raw HTTP response of the debugged HTTP request (read-only). |

To enable it, you should go to “Options” menu (in Engine’s toolbar) and click on “Debug HTTP request”. Next available request will be intercepted and an additional panel will be displayed in the tab list located in the bottom right side (next to “URI Information”).




There are three HTTP Debug modes available and they can be selected by clicking on the appropriate radio button:

- **None**


All Rights reserved ZMT Comunicações e Tecnologia Ltda.

"None" mode means HTTP Debug enabled, however, no data will be displayed to the user. This is interesting when you need to speed up debug process until you reach a particular position for a full debug mode.

- **Step-by-Step**

  "Step-by-Step" mode will enable a manual debug, which means every request and response must be triggered by clicking on "Step Request" hyperlink located in the bottom left side of HTTP Debug panel.

  It is ideal for modifying HTTP requests before they are sent out by the N-Stalker Scanner Engine.

- **Slide Show**

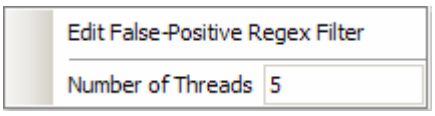
  "Slide Show" mode allows you to visualize every request and its correspondent response without manual interference. You may set the delay in seconds between each response and request.

### 1.3.5.2. Save Scan Session

While running a Scan Session, there is an option to stop current activities and save the entire session state. Once session is saved, you may continue the scan on a later time. To initiate it, go to "Options" in Engine's toolbar and choose "Save Scan Session".

When requested, Scanner Engine will suspend all activities and quit the current session. The same behavior may be simulated if you press "Stop" button located in Engine's toolbar.

### 1.3.5.3. General Engine Option



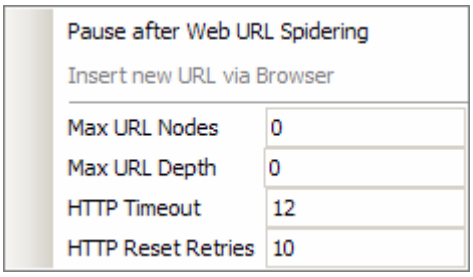

"General Engine Option" controls the behavior of N-Stalker Web Application Security Scanner Engine. There are two available options under this menu:

| | |
|---|---|
| **Edit False-Positive Regex Filter** | This option allows you to edit current False-Positive Regex filters being used by Scanner Engine. When set, Engine will compare every HTTP response against these filters to determine if it is a negative response and should be dropped out (see section 2.5.5 for more details). |
| **Number of Threads** | When multithreaded checks are available, N-Stalker will use this configuration field to determine number of simultaneous threads it will launch. Higher numbers means quicker scanning performance, however, it depends on machine's hardware capabilities. |


All Rights reserved ZMT Comunicações e Tecnologia Ltda.

**Tip:** Do not increase number of threads if you are not sure about your own machine's performance. High number of threads may interfere with Scanner Engine's performance and may cause incorrect scan results.

### 1.3.5.4. Spider Options



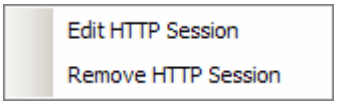

"Spider Options" controls the behavior of N-Stalker Web Application Scanner Engine Spider module. There are multiple options under this menu:

| | |
|---|---|
| **Pause after Web URL Spidering** | This option allows you to pause Scanner Engine just after the spidering phase. This is especially interesting when you need to review the Website Tree content, modify settings, add or remove URI resources. |
| **Insert new URL via Browser** | If you need to provide additional URLs to Scanner Engine's queue for inspection purposes, you may use this option. A Web Browser interface will be opened and every action will be captured. This option will become disabled after Spidering Phase. |
| **Max URL Nodes** | This option allows you to control the total number of URL nodes (resources) Scanner Engine might request. If set to zero (0) or blank, there will be no restrictions. |
| **Max URL Depth** | This option allows you to control the directory depth of Scanner Engine. Example: /test/example.asp would be 1 (one) and /test/next/example.asp would be 2 (two). If set to zero (0) or blank, there will be no restrictions. |
| **HTTP Timeout** | This option allows you to establish a value (in seconds) for HTTP timeout. This setting will be reflected during the entire Scanner Engine session (to every HTTP connection). |
| **HTTP Reset Retries** | This option allows you to establish the number of retries once a TCP reset is received during the HTTP connection. |

**Tip:** For performance optimization, we do not recommend to set HTTP Reset Retries to a high number (8-10 would be the recommended setting).

### 1.3.5.5. Session Options


All Rights reserved ZMT Comunicações e Tecnologia Ltda.



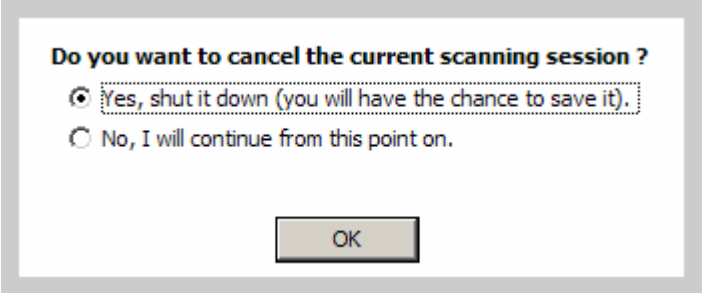

"Session Options" controls the behavior of Web sessions managed by N-Stalker Web Application Security Scanner Engine. There are two available options under this menu:

| | |
|---|---|
| **Edit HTTP Session** | This option allows you to edit content of all web sessions being currently managed by N-Stalker's Scanner Engine. |
| **Remove HTTP Session** | This option will reset the entire web session space, including authentication tokens (if available). |

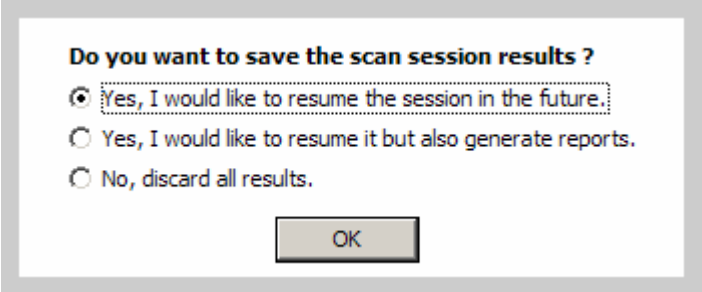
### 1.3.6. Terminating Scan Engine Session

There are two ways to terminate Scan Engine Session activities. You may press "Stop" Button (located in the Engine's toolbar) or choosing "Save Scan Session" located in the "Options" menu (also in the Engine's toolbar).

When stopping Engine's activities, you will be prompted to confirm the operation:




Choose "Yes" to confirm it or "No" to cancel the request and resume the Scanner Engine session. If you choose "Yes", the following options will become available:




- **Yes, I would like to resume the session in the future**

  N-Stalker will save the entire current session and will allow you to resume it on a later time. No results will be available to generate reports until you resume it again.

- **Yes, I would like to resume it but also generate reports**


All Rights reserved ZMT Comunicações e Tecnologia Ltda.

N-Stalker will save the entire current session and will allow you to resume it on a later time. Current scanner results will be also available to generate partial reports using the "N-Stalker Report Manager".

- **No, discard all results**

  No results will be available, neither for resuming to them later nor for report generation.

## 1.4. Resuming Scan Sessions

Once a scan session is saved to be resumed later, you must recover it from "N-Stalker Policy Editor". Here are the instructions:

1. Open N-Stalker Policy Editor (NstalkerScanner.exe);


2. Go to the "Web Security Audit Policies" tree located in the left side panel of Policy Editor and find the "Saved Sessions" node;



All Rights reserved ZMT Comunicações e Tecnologia Ltda.

3. Expand “Saved Sessions” node;


4. Right-click on the target saved session to enable context menu;


5. From this point, there are two options:

| | |
|---|---|
| **Start Scan Session** | Click here to resume saved scan session. It will begin from the previous saved state. |
| **Delete Scan Session** | Click here to delete the entire saved scan session and its content cache. |

## 1.5. Overview of N-Stalker Reports

Once you have completed a Web Application Security evaluation, you may create reports based on your own needs.

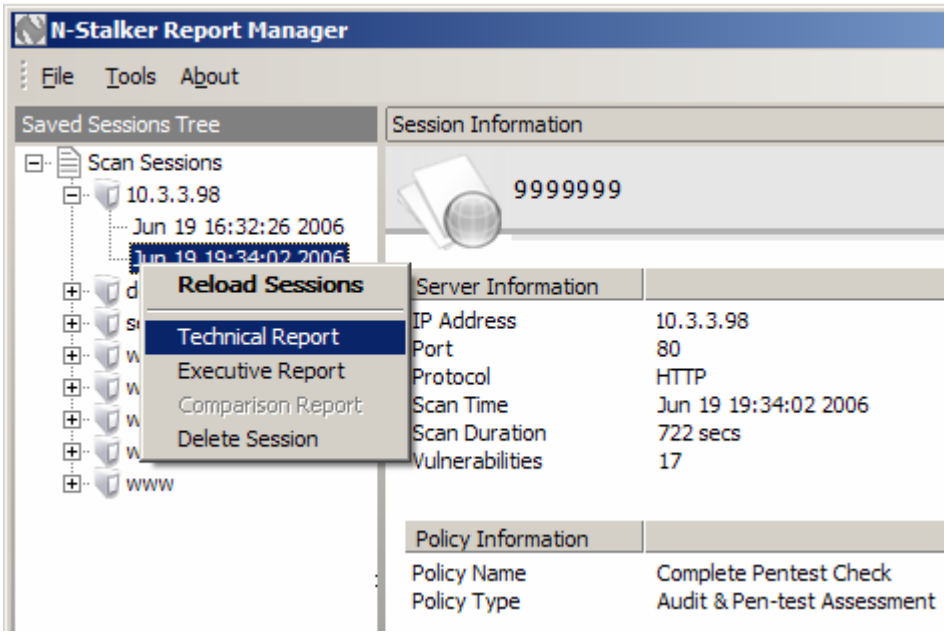

All Rights reserved ZMT Comunicações e Tecnologia Ltda.

In this version, N-Stalker Web Application Security Scanner provides you with the ability to create three different report profiles, customizing the level of information you may need. These reports can be generated on HTML, RTF and PDF formats, according to your specification.

In this section, we will provide you with a brief analysis of each particular report profile. For customization and format options please see Chapter 6.

### 1.5.1. Technical Report

This is the most detailed report made available in the N-Stalker Web Application Security Scanner. It provides user not only with a summary of scanned resources and vulnerabilities found but also with website tree view, objects found and detailed information about vulnerabilities.




These are the most common available sections:

- **Scan Summary**
- **Web Application Information**
- **Published Directories**
- **Website Tree**
- **Cookies Report**
- **E-mails Report**
- **Information Leakage Report**
- **Hidden Files Report**
- **Broken Pages Report**
- **Web Forms Report**
- **Web Server Exposure Vulnerabilities**
- **Custom Design Errors Vulnerabilities**
- **Web Signature Attacks Vulnerabilities**
- **Confidentiality Exposure Vulnerabilities**
- **Cookie Exposure Vulnerabilities**
- **File & Directory Exposure Vulnerabilities**

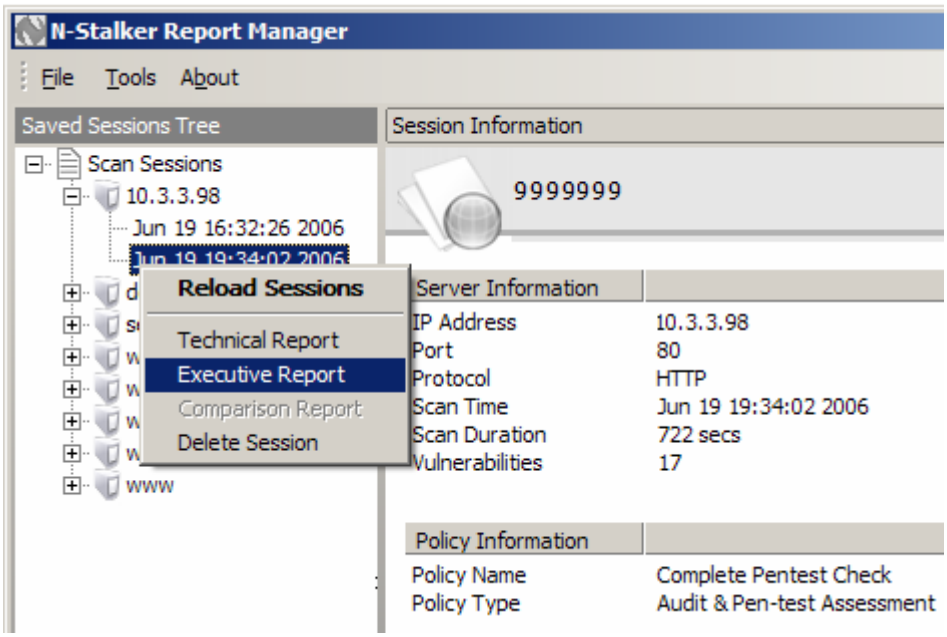

All Rights reserved ZMT Comunicações e Tecnologia Ltda.

- **Content Inspection Report**

If necessary, N-Stalker Reports may include technical details about each HTTP Request and Response (entire content).

### 1.5.2. Executive Report

This is an executive view of a N-Stalker Scan Session. It provides a summary of scanned resources and vulnerabilities information. It is recommended to managers, IT executives, auditors or for those requiring to get a glance at the Web Application current security status.

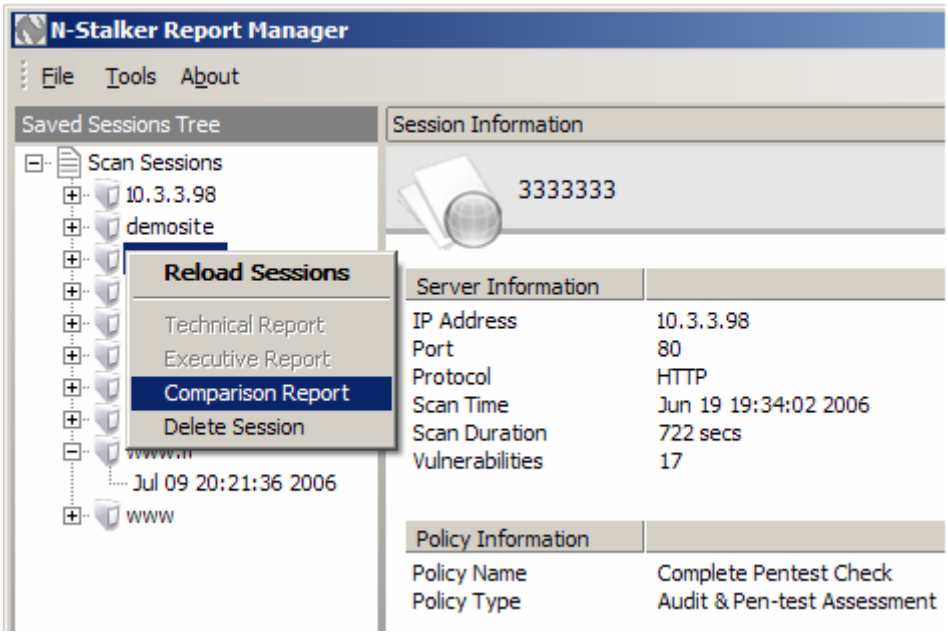



### 1.5.3. Comparison Report

Comparison Report is an executive summary that compares results of one particular Web Application target from a specified period range.

No doubt it is a very important differential for IT managers, auditors and senior administrators wishing to compare previous scan results to identify possible vulnerability trends. It is ideal for Patch and Change management control.


All Rights reserved ZMT Comunicações e Tecnologia Ltda.





All Rights reserved ZMT Comunicações e Tecnologia Ltda.