

### 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				
5 ,	the application such as XSS and SOL injection				
	the application such as ASS and SQL injection,				
	Buffer Overflow, Parameters Tampering issues and				
	Cookie vulnerabilities.				
Common OWASP Top10	This policy will search for Common Top10 security				
Check	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	This is a policy focused on Confidentiality issues. It				
Analysis	will search for insecure data handling, information				
(Confidential Check Only)	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 3 <sup>rd</sup> 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:



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):





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

(\*) 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:



- 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):

ample.com		Next
Develop	nent / QA	
Stage 1 include C	of SDLC - These are the policy templates for Dev ross-Site scripting and SQL Injection, Buffer Ove	elopment and QA Security analysis. These rule erflow test cases, Parameter Tampering rules.
Choose Policy Custom Desid	: n Frror Only	
Common OW	ASP Top 10 Check	
Information I	xposure Analysis (Confidentiality Check Only)	

### 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:



ample.com	Start	Sc
Development / QA		
Stage 1 of SDLC - These are the policy template include Cross-Site scripting and SQL Injection, B	es for Development and QA Security analysis. These r Buffer Overflow test cases, Parameter Tampering rule	ule: s.
Configuration Summary :	Value	_
Web Spidering Method Parsing Options Follow links over HTTP or HTTPS protocol Discover Server-side technology (i.e: PHP, ASP) Web Application Authentication Ouick-scan method (fast scan, false positives)	Crawl. No Initialization script provided. Javascript Disabled. Robots.txt Disabled. Disabled. Disabled. Disabled. Disabled. No information found. Enabled.	
<b>C</b>		

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

imple.com				Start Sca
Development / O	A			
Stage 1 of SDLC - 1 include Cross-Site s	hese are the policy temp cripting and SQL Injectio	lates for Developme n, Buffer Overflow t	ent and QA Security test cases, Paramet	analysis. These rule. er Tampering rules.
•				
Choose Web Application	Spidering method :			
Crawl the Websit	e (Web Spidering)			
Run a custom	initialization web script			
Run a custom O Do not Crawl the	initialization web script Website (No Web Spider	ing)		
C Do not Crawl the	initialization web script Website (No Web Spider nual list of URLs for navig	<b>ing)</b> ation purposes		
Run a custom     Do not Crawl the     Provide a mai	initialization web script Website (No Web Spider nual list of URLs for navig	<b>ing)</b> ation purposes		
Run a custom O Do not Crawl the Provide a mai Step 1 of 2	initialization web script Website (No Web Spider hual list of URLs for navig	ing) ation purposes		Next >>

Allows you to modify Web Spider method:

✓ Crawl Website

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

eb Application OKL	(i.e. mep///istaiker megnyw	201000	
ample.com			Start Sca
Development / (	A		
Stage 1 of SDLC - include Cross-Site	These are the policy template scripting and SQL Injection, B	s for Development and QA Security anal uffer Overflow test cases, Parameter Ta	ysis. These rules ampering rules.
Create an initialization :	script :		
URL		Post Data	
URL	Add Manual Add Web Browse Delete	Post Data	
URL Step 2 of 3	Add Manual Add Web Browse Delete	Post Data	k Next >>

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").



🙌 Enter Inforn	nation		_ 🗆 🗙
URL	Data	ОК	Cancel

### ✓ 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.

🙌 N-Stalker W	eb Capture Ini	terface					_ [	IX
Address http://	//www.nstalker.	com/				0	ptions 👻 Naviga	ate
N DEFEN	-Stal	ker						1
Products	Defense	Customer Cer	nter Conto	ict Buy 1	Now Ab	out N-Stalker	Language	
Overview	ON-Stealth S	Security Scanner	N-Stealth Log	Analyser				
		E H	YOU AF As	E JUST ON Sessing Y	E CLICK AW/ Our web si	AY FROM Ecurity Issi	JES! y now ! Download †	th
± News & U	odates		₩ Features					
Update Jun 21st, 200 PHP-Fusion v	16 vulnerabilities an	d new updates	O Searc	h OR	Jownload	Buy Now! Discover you Buy N-Stalker	r vulnerabilities b now !	ef
Captured Session	1							-
URI				Data				T
http://www.nsta	lker.com/							

• Step 3 – Choose Multiple Options



Development / QA         Stage 1 of SDLC - These are the policy templates for Development and QA Security analysis. These rules include Cross-Site scripting and SQL Injection, Buffer Overflow test cases, Parameter Tampering rules.         Choose Scan Options :            Web Application requires Javascript parsing             Follow links over secure and non-secure protocols (HTTP and HTTPS)             Auto-discover server-side technology (i.e: PHP, ASP, J2EE)             Search for Robots.txt file and parse for hidden URLs             Disable Quick-Scan method (fast scan and positive hit caching mode)             Web Application requires special user authentication	Veb Application URL (i.e: http://nstalker.net/myWebApp/)	Charle Gran
Development / QA         Stage 1 of SDLC - These are the policy templates for Development and QA Security analysis. These rules include Cross-Site scripting and SQL Injection, Buffer Overflow test cases, Parameter Tampering rules.         Choose Scan Options :            Web Application requires Javascript parsing             Follow links over secure and non-secure protocols (HTTP and HTTPS)             Auto-discover server-side technology (i.e: PHP, ASP, J2EE)             Search for Robots.txt file and parse for hidden URLs             Disable Quick-Scan method (fast scan and positive hit caching mode)             Web Application requires special user authentication		peare pear
Stage 1 of SDLC - These are the policy templates for Development and QA Security analysis. These rules include Cross-Site scripting and SQL Injection, Buffer Overflow test cases, Parameter Tampering rules.         Choose Scan Options :            Web Application requires Javascript parsing             Follow links over secure and non-secure protocols (HTTP and HTTPS)             Auto-discover server-side technology (i.e: PHP, ASP, J2EE)             Search for Robots.txt file and parse for hidden URLs             Disable Quick-Scan method (fast scan and positive hit caching mode)             Web Application requires special user authentication	Development / QA	
Choose Scan Options :          Web Application requires Javascript parsing         Follow links over secure and non-secure protocols (HTTP and HTTPS)         Auto-discover server-side technology (i.e: PHP, ASP, J2EE)         Search for Robots.txt file and parse for hidden URLs         Disable Quick-Scan method (fast scan and positive hit caching mode)         Web Application requires special user authentication	Stage 1 of SDLC - These are the policy templates for Development and QAS include Cross-Site scripting and SQL Injection, Buffer Overflow test cases, P	Security analysis. These rules Parameter Tampering rules.
<ul> <li>Web Application requires Javascript parsing</li> <li>Follow links over secure and non-secure protocols (HTTP and HTTPS)</li> <li>Auto-discover server-side technology (i.e: PHP, ASP, J2EE)</li> <li>Search for Robots.txt file and parse for hidden URLs</li> <li>Disable Quick-Scan method (fast scan and positive hit caching mode)</li> <li>Web Application requires special user authentication</li> </ul>	Choose Scan Options :	
<ul> <li>Follow links over secure and non-secure protocols (HTTP and HTTPS)</li> <li>Auto-discover server-side technology (i.e: PHP, ASP, J2EE)</li> <li>Search for Robots.txt file and parse for hidden URLs</li> <li>Disable Quick-Scan method (fast scan and positive hit caching mode)</li> <li>Web Application requires special user authentication</li> </ul>	✓ Web Application requires Javascript parsing	
<ul> <li>Auto-discover server-side technology (i.e: PHP, ASP, J2EE)</li> <li>Search for Robots.txt file and parse for hidden URLs</li> <li>Disable Quick-Scan method (fast scan and positive hit caching mode)</li> <li>Web Application requires special user authentication</li> </ul>	✓ Follow links over secure and non-secure protocols (HTTP and HTTPS)	
<ul> <li>Search for Robots.txt file and parse for hidden URLs</li> <li>Disable Quick-Scan method (fast scan and positive hit caching mode)</li> <li>Web Application requires special user authentication</li> </ul>	▼ Auto-discover server-side technology (i.e: PHP, ASP, J2EE)	
Disable Quick-Scan method (fast scan and positive hit caching mode)     Web Application requires special user authentication  Step 3 of 3	Search for Robots.txt file and parse for hidden URLs	
Web Application requires special user authentication Step 3 of 3	Disable Quick-Scan method (fast scan and positive hit caching mode)	
Step 3 of 3	Web Application requires special user authentication	
	Step 3 of 3	<< Back
ick to Wizard menu	ck to Wizard menu	

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.



### ✓ 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.

Web Application URL (i.e: http://n: example.com	stalker.net/myWebApp/) Start Scan
Development / QA Stage 1 of SDLC - These are th include Cross-Site scripting and	e policy templates for Development and QA Security analysis. These rules SQL Injection, Buffer Overflow test cases, Parameter Tampering rules.
Choose Authentication Options : Authentication Options HTTP Authentication Web Form Authentication Cookie Authentication x.509 Authentication	<ul> <li>Prompt for password when HTTP authentication is required</li> <li>Prompt for password when Web Form authentication is required</li> </ul>
Step 4 of 4	< <back next="">&gt;</back>
Back to Wizard menu	

### ✓ 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 authentication is required
Prompt for password when Web Form authentication is required

Prompt for password	When e	nabled,	N-St	alker	will
when HTTP	manually	prompt	for	user	and
	password	whene	ver	а	HTTP

authentication is	authentication is required.		
required			
Prompt for password	When enabled, N-Stalker will		
when Web Form	manually prompt for user and		
authentication is	password whenever a web form		
required	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		
Username :		
Password :	(Use domain\user for NTLM-based authentication)	

Enable Host	When host (HTTP) authentication is		
Authentication	required, you must enable this		
	option.		
Username	Enter username for HTTP		
	authentication. You may use MS		
	Windows <sup>™</sup> 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.



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

	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.
	5

**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 :	
(i.e: auth=admin01; pass=test01)	

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 :	<u>i</u>
(Choose an ASN.1 or PEM encoded certificates)	
Private Key Path :	<u>i</u>
(Choose an ASN.1 or PEM encoded keys)	
Key Password :	
(If you need a password to decrypt the private key)	

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.



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

Scan Session Information			
Server URL : http://www			
Current Attack Module : N-Stalker Web Spider Module (Spider mode)			
Last Event : Adding URI [/publicidade.php]			
Progress Status :		(#8)	
Vulnerabilities Found : 1	Objects Found: 77	# Threads : (none)	
Scan Information Scan Statistics	Scan Policy Scan Components Log	Information	

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	
Session Information	
Average Response Time Average Request Size Total Discovered Servers Last Vulnerable Object Number of scanned URLs	(0ms/1625ms/3953ms) 28770 bytes 1 /cadastro.php 8
Scan Information Scan Statistics S	can Policy Scan Components Log Information

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 URI
Average Response Size	Average size (in bytes) of response obtained
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.

N-Stalker Web Application Security Scanner 2006 | www.nstalker.com All Rights reserved ZMT Comunicações e Tecnologia Ltda.



### 1.3.2.3. Scan Policy

Scan Session Policy Policy Name : Common OWASP Top 10 Check		
Rule Name	Status	
Web Resources Spider and Analysis File & Directory Exposure Attacks Cross-site Scripting Attacks SQL Injection Attacks	In progress Not tested Not tested Not tested	<b>•</b>
Scan Information Scan Statistics Scan Policy Scan Components Log Information		

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	<ul> <li>Rule table provides the name of the rule and its current status:</li> <li>In progress: currently in execution</li> <li>Not tested: scheduled to be executed</li> <li>OK: already tested</li> </ul>	

### 1.3.2.4. Scan Components

Scan Components			
Location	Component Type	Component Name	Detected Type
http://www http://www	Web Server Server-side Tec	Apache PHP Framework (v4.4.2)	Apache/1.3.x N/A
Scan Information Scan Stat	istics Scan Policy Sc	an Components Log Information	on

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

Web Servers.

### 1.3.2.5. Log Information

[06/15/2006 17:32:16] ZMain(): License agreement successfully attached. Engine Version [6.0].
[06/15/2006 17:32:33] Main(): Resolving hostname [0.13.1.3]
[06/15/2006 17:32:33] ZServerInfo(): New Server version found [Apache]
[06/15/2006 17:32:46] ZServerInfo(): Exceeded reset errors (#10053) - skipping HTTP check
[06/15/2006 17:32:46] Possible match found for http://www/: [Apache/1.3.x]
[06/15/2006 17:32:48] ZServerInfo(): False positive control (root page) enabling hash-based protection.
[06/15/2006 17:32:53] ZSpider(): HTTP Redirect (http://www/error.php)
[06/15/2006 17:32:53] ZSpider(): HTTP Redirect (http://www/error.php)
[06/15/2006 17:32:58] ZSpider(): Auto-complete feature is not disabled on a password-based form [/cadastro.php]
Scan Information Scan Statistics Scan Policy Scan Components 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.

Website Tree Events List

### 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

	some aspects of URI, including URI string itself, Post data and Session Information.
Delete URI	This option will remove URI from
	website free.
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 Server-Side Support
View URI details
Edit URI details
Delete URI
Open in Browser
Copy to clipboard

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.



1				see details
Server Information		Request Informat		
The Hostname	www	② Method	GET	
📅 Port	80	<li>Title</li>	SecureNet	
Trotocol	HTTP	<li>② Size</li>	336	
🔝 SSL Cipher	N/A	Petch Time	15ms	
🕡 Server Type	Apache	# Variations		
🕡 Detected Type	Apache/1.3.x	🚺 Post Data	(no content)	
🕡 Server-Side	PHP			
Object Information		Vulnerability Informat	tion	
🛓 Scripts	1 (92 bytes)	🗘 High	0	
Comments	0 (0 bytes)	🔔 Medium	0	
E-mails	0	🗘 Low	0	
URI Information Object	cts Information			

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.

N-Stalker Web Application Security Scanner 2006 | www.nstalker.com 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

Objects Found /site/catalogo/	
Comments E-mails Scripts Forms	
Comments (650 bytes) (Robot commands: All, None, Index, No Index, Follow, No Follow) InÃcio dos includes Fim dos includes PHPCOMPONENTE promocoes PHPCOMPONENTE categoria PHPCOMPONENTE Cesta PHPCOMPONENTE Login PHPCOMPONENTE resumos BEGIN b_linha END b_linha BEGIN main PHPCOMPONENTE materias BEGIN b_linha	
Search Expression	Search 🗌 Use Regex
URI Information Objects Information	

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
	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



purposes, enable this option first.

• E-mails

Objects Found /site/catalogo/	
Comments E-mails Scripts Forms	
E-mail	Count
comercial@com.br	4
URI Information Objects Information	

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



Ô,	Objects Found /site/catalogo/
Comments	E-mails Scripts Forms
= <mark>Scripts (63</mark> fonaName =	3 bytes) = "";
var oprient. (nam – d) ( document.js function init function init initArray.ar sat picris03781: piczis03781:	$ \frac{1837814649 + 0^{\circ} (intrition gointoge 18378 t+649(val) { variatum = current1837814649 (val) if  (num = pic (18376 1+649 length-1) (intrition 2) (2218378 1+649 (variatum = 0)) { mm = 0}  (ing 18370 1+649 and = pic (18378 t+30 (num)) current (8378 1+649 = num) }  Arrav() { wisilength = intArray (arguments its ight; for (variate 0) i < methods (14+) { % r(i) =  gomental(i)}  7814649 = constants(0)  4649 (push(i)) (bitos/65/g0 (050 - main.jpgii); //$

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
0	expression keywords for search
	purposes, enable this option first.

• Forms



Ob /sit	ojects Found te/catalogo/			
Comments E-r (Name: userna Action Detai	mails Scripts Form ame) ils: (POST) /site/cata	ns alogo/		
Field Name		Field Type	Field Value	
entrar senha username		Image Password Text		
URI Information	Objects Information			

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 <b>Text</b> ,
	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.



N HTTP Response Viewer	
URL /site/catalogo/	Details - Send
HTTP Request GET /site/catalogo/ HTTP/1.1 Referer: http://www/index.php Host: www User-Agent: Mozilla/4.0 (compatible) Cookie: inodesite =acacb62270c0d61d1f14090e64dd4927;	
HTTP Response HTTP/1.1 200 OK Date: Sun, 16 Jul 2005 19:54:23 GMT Server: Apache/2.0.XX (CentOS) X-Powered-By: PHP/4.4.2 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cachee Control: postore poscache must revalidate postscheck=0, prescheck=0	
Pragma: no-cache Connection: dose Transfer-Encoding: chunked Content-Type: text/html; charset=ISO-8859-1 Search response	▼ ▶ Regex
Text View Browser View Hex View	

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.

NTTP Response Viewer	
URL /site/catalogo/	Details 🔻 Send
HTTP Request	Post Content



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.

📉 HTTP Resp	onse Viewer						<u>- 🗆 ×</u>
URL /eng/						Details -	Send
	-Sta	Iker					
Products	Defense	Customer Cent	er Contact	t Buy Now	About N	I-Stalker	Langi
Overview	O N-Stealth	n Security Scanner	ON-Stealth Log	Analyser			
		E H	YOU AR As	E JUST ONE Sessing Yo	CLICK AWAY UR WEB SEC	FROM CURITY IS	SUES! Try now !
± News & U	lpdates		兼 Features				
Update Jun 21st, 20 PHP-Fusion Update May 29th, 2	06 vulnerabilities 006	and new updates	© Search	h OK		Buy Now! Discover ye Buy N-Stall	our vulne ker now !
Pequest On-lin	e Desource					wave on line	browser
Request On-In	e Resource					ways on the	Drowser
Text View Bro	wser View Hex	View					

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

🕥 нт	TP Res	ponse	Viev	ver												
URL	/eng/														Details 🔻	Send
_																
	0000 000c 0018 0024 0030 003c 0048 0054 0054 0060 0078 0078 0090 0090 0090 0090 0090 009	48 20 53 32 65 0A 45 75 65 78 0A 45 75 78 0A 3E 50 22 20 73 32 20 40 63 20 63 20 63	54 475 300 58 300 66 66 54 473 20 54 473 20 30 8 473 20 30 8 473 20 24 30 24 30 24 30 24 30 25 24 30 20 24 24 55 20 20 20 20 20 20 20 20 20 20 20 20 20	54 4B 320 47A 220 63 72F 20A 20D 201 20A 20D 201 20D 202 53 25 25 25 25 25 25 25 25 25 25	50 02C 36D 250 554 65D 665D 665D 667 667 649 245 59 0A 259	2F 0D 200 54 46 54 64 64 64 64 64 64 64 64 64 0A 66 1 3D 0 50 379 66 1 3D 0 50 50 50 50 50 50 50 50 50 50 50 50 5	31 0A 312 0A 777 60 0D 0C 522 54 60 0D 0E 522 54 60 3D 9 45	2E4436200161526EE00070062549652262730	31 61 04 63 73 63 63 63 65 65 65 65 65 22 65 22 65 22	20 74 430 53 66 26 43 43 00 68 56 66 20 48 66 20 48 66 20 48 65 27 4	32655664467076656663666565	30 32 32 32 32 22 22 22 30 22 22 22 22 22 22 22 22 22 22 22 22 22	30 20 32 70 42 20 42 20 68 432 68 430 66 49 20 64 9 30 22 45 74 27 73	HTTP/1.1 200 OKDate: Sun, 16 Jul 2006 22:06:2 4 GMTServ er: Apache. X-Powered-B y: PHP/4.4.2 Transfer- Encoding: ch unkedCont ent-Type: te xt/html <html &gt;<scri PT language= "JavaScript" src="/eng/j s/top.js"&gt;<!--<br-->SCRIPT&gt; <link re<br=""/>L=StyleSheet HREF="/eng/ css/site.css " TYPE="text</scri </html 		Load
Text	View B	rowser	View	Hex	View											
Text	View B	rowser	View	Hex	View											

Load	Click	on	"Load"	button	to	display
	reque	st in	hexadec	imal table	э.	

### 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.

Website Tree Events List

### 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



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:

N-Stalker Web Application Security Scanner



### User's Manual | Getting Started

No information available.

See Request Details

### 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).

🖃 💮 Objects
吏 🔶 Cookies (1)
🖭 🛓 Scripts (72)
🗄 🗐 Comments (45)
🗄 🖶 Web Forms (47)
🗄 🖂 E-mails (2)
🗄 🖶 Broken pages (8)
⊕ ↔ Hidden Fields (121)
i Information Leakage

These are the list of objects and available functionalities:

Cookies

Cookies (1)

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



### • Scripts

🖃 🖆 Scripts (72)	
-/	
···· /topo.asp	
··· /js/script.js	
···· /js/menucentro.js	-
··· /js/menu.js	
···· /resp.asp	



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.

60	Objects Found /login.asp		
Scripts			
Scripts (1	199 bytes)		
'toolbar=n	function popup <b>senha</b> (pag) { window.open(pag, 'esquecis no,location=no,status=no,scrollbars=no,director }	enha', ies=no,width=280,h	eight=250,top=
return Vali	idaForm(this);		
Search E	xpression	Found	Search

### • Comments

📮 🗐 Comments (45)
-1
··· /resp.asp
···· /projeto.asp
···· /cons.asp
/gov.asp
/esporte.asp
···· /tecnologia.asp
/educ.asp

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.



<i>(0)</i>	Objects Found /sta.asp		
Comments			
Comment size: 10p size: 10p	ts (207 bytes) x;"> <fo x;"&gt;14</fo 	"2"> <font #479852;="" color:="" f<="" style="color: #00000&lt;br&gt;nt style=" td=""><td>0; font-family: v ont-family: ve</td></font>	0; font-family: v ont-family: ve
-Search F	voression		
size(.+)10	)	Found	Search

### • 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.

2	Ô,	Objects Found /ecc.asp			
	Forms				
	-(Name: fr	mLogin)			
	Action Details: (POST) login.asp				
	Field Name	2	Field Type	Field Value	
	exc		Hidden		
	pag		Hidden	ok	
	txtLogin		Text		
	txtSenha		Password		



• E-mails

⊑		
···· info@nstalker.com		
page@nstalker.com		
··· fidden@nstalker.com		
lea@nstalker.com		

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

🖃 📑 Broken pages (2)
http://www/five
http://www/eton

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.

Broken pages (2)	
Broken Pages	
404 Link Refer Page	
http://www/five http://www:80/Help http://www/tone http://www:80/supp	

### • Hidden Fields

⊟ ↔ Hidden Fields (43)
https://www/ytootou

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.



Ę	Ô,	Objects Found Hidden Fields (43)	
ſ	Hidden Fiel	ds	
	Hidden Fie	eld	Refer URL
	VIEWST _TargetPa _TargetPa actionpage actionpage BuscaNom	ATE=dDwyMDg1OTY2MDcwO3Q ge=_parentw1OTY2MDcwO3Qbr ge=hDwyMDg1OTY2MDcwO3Qbr e=_parent e=_parent e (empty value)	https://www.etoutour.com.yy:443/publica https://www.etoutour.com.yy:443/publica https://www.etoutour.com.yy:443/publica https://www.etoutour.com.yy:443/publica https://www.etoutour.com.yy:443/publica https://www.etoutour.com.yy:443/publica

### • 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.

Objects Found Editor Tool Meta-Tag Information Leak			
Meta Tag			
Field Valu Microsoft	e Visual Studio 7.0	Refer URL https://www.etoytour.com.yy:443/i	

### 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.

Opti	ons 🔻	
	Debug <u>H</u> TTP Request	
	Save Scan Session	
	General Options	۲
	Spider Options	×
	Session Options	۲
	WAS Engine v6.0	



### 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.

Https://www/stam.vxl				
HTTP Request GET /stam.vxl HTTP/1.1 Referer: http://www/publicad?RE Host: www User-Agent: Mozilla/4.0 (compati Cookie: ASPSESSIONIDSCCBQRD	idirectasp ble) R=JOHCOGLBFODBIICHNDNJD	LHG; ASP.NET_	SessionId=rk1whk5	▲ 552ik0ds45ues
HTTP Response				
HTTP/1.1 200 OK Date: Mon, 17 Jul 2006 17:06:24 Server: Microsoft-IIS/6.0 X-Powered-By: ASP.NET X-AspNet-Version: 1.1.4322	GMT			-
Cache-Control: private Content-Type: text/html; charse	t=iso-8859-1			• •
Step Request	73451 bytes loaded.	C None	Step-by-Step	C Slide Show
URI Information Objects Inform	ation HTTP Debug			

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").

Step Request	73451 bytes loaded.	C None	Step-by-Step	$ \mathbb{C} $ Slide Show
URI Information Objects Informatio	n HTTP Debug			

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

None



"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.		

**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

Pause after Web URL Spidering		
Insert new URL via Browser		
Max URL Nodes	0	
Max URL Depth	0	
HTTP Timeout	12	
HTTP Reset Retries	10	

"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

N-Stalker Web Application Security Scanner 2006 | www.nstalker.com All Rights reserved ZMT Comunicações e Tecnologia Ltda.



Edit HTTP Session Remove HTTP Session

"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:

Do you want to cancel the current scanning session ?
⑦ Yes, shut it down (you will have the chance to save it).
$\ensuremath{\mathbb{C}}$ No, I will continue from this point on.
OK

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:

Do you want to save the scan session results ?
Yes, I would like to resume the session in the future.
C Yes, I would like to resume it but also generate reports.
C No, discard all results.
ОК

• 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



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;





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.



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



### 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.

💦 N-Stalke	r Report Manager		
Eile Tool	s A <u>b</u> out		
Saved Sessio	ns Tree	Session Information	
Scan Sessions 		9999999	
🗄 🕡 🗄	Reload Sessions	Server Information	
	Technical Report	IP Address Port	10.3.3.98 80
i i i i i i i i i i i i i i i i i i i	Executive Report	Protocol	HTTP
÷. 🖏 🗤	Comparison Report	Scan Time	Jun 19 19:34:02 2006
🛓 💮 🗤	Delete Session	Scan Duration Vulnerabilities	722 secs 17
÷. 🕡 wv	NW	Vanier abilities	17
		Policy Information	
	:	Policy Name Policy Type	Complete Pentest Check Audit & Pen-test Assessment

### 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.



💦 N-Stalker Report Manager		
Eile Tools About		
Saved Sessions Tree	Session Information	
⊡ Scan Sessions ⊕ 10.3.3.98	3333333	
Reload Sessions	Server Information	
Technical Report     Executive Report	IP Address Port Protocol	10.3.3.98 80 HTTP
	Scan Time Scan Duration	Jun 19 19:34:02 2006 722 secs
Jul 09 20:21:36 2006	vuinerabiilües	17
- •	Policy Information	
	Policy Name Policy Type	Complete Pentest Check Audit & Pen-test Assessment