



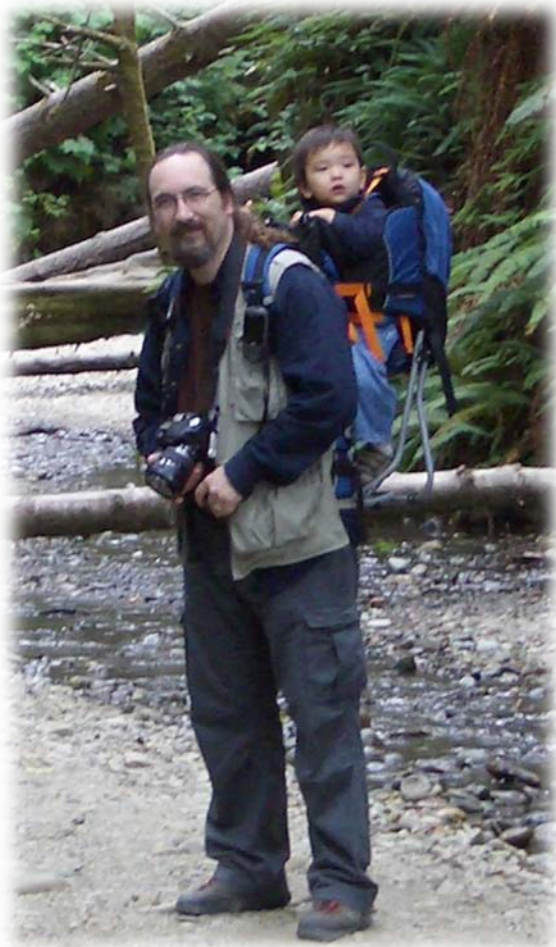
The OWASP Foundation
<http://www.owasp.org>

Web Application Vulnerability Testing with Nessus

Rik A. Jones, CISSP

rikjones@computer.org

Rik A. Jones



- Web developer since 1995 (16+ years)
- Involved with information security since 2006 (5+ years)



- Senior Information Security Analysts for Dallas County Community College District

- CISSP and GIAC certified



- Member of the Dallas OWASP Leadership Team



- Member of the Dallas Chapter of InfraGard





This is not a sales presentation

I am not affiliated with Tenable or Nessus other than being a knowledgeable and frequent user.

I am here to show you how to use Nessus as a tool, one of many tools I keep in my toolbox



Introduction to Nessus

Nessus is a multiple platform network and host vulnerability scanner

Server Supported on:

- Window
- Linux
- Mac OS
- UNIX

Clients: Web based and Mobile (IOS, Android)

Introduction to Nessus

Nessus has 2 licensing models (plugin feeds)

- **ProfessionalFeed**
 - Commercial use
 - Access to support portal
- **HomeFeed**
 - No charge
 - Personal use only
 - Some limits to functionality
 - Only 16 IP addresses
 - No compliance/audit checks
 - No scan scheduling

Introduction to Nessus

Nessus Terminology

- **Policy** – Configuration settings for conducting a scan
- **Scan** – Associates a list of IPs and/or domain names with a policy
 - Basic Scan (Run Now)
 - Template
 - Scheduled Template (ProfessionalFeed Only)
 - One time or repeating
- **Report** – The result of a specific instance of a scan
- **Plugin** – A security check, or a scan settings window
- **Plugin Family** – A group of plugins with something in common (e.g. FTP, Web Servers, Cisco)

Introduction to Nessus

Nessus Customization Options

- **Reports Templates** – Coded in XSLT
- **Plugins** – Coded in NASL (Nessus Attack Scripting Language)
- **Audit Files** – Coded in Pseudo-XML [ProfessionalFeed Only]
- **Import/Export** – Nessus & Nessus 2 format coded in XML. Same format for reports and profiles

Logging in to Nessus

By default Nessus runs on port 8834 and can be accessed with any Flash enabled Web Browser



Basic Navigation

There are four navigation tabs at the top

- Reports
- Scans
- Policies
- Users



Reports Tab

The Reports tab list the results of scans you have conducted, are currently running or have imported



| Name | Status | Last Updated |
|-----------------------|---------|--------------------|
| 192.168.206.134 DVWA | Running | Jan 22, 2012 02:13 |
| 192.168.206.134 Basic | Running | Jan 22, 2012 01:55 |

Scans Tab

The Scans tab list currently running scans, scan templates and scheduled scans



The screenshot shows the Nessus web interface with the 'Scans' tab selected. The interface includes a navigation bar with 'Reports', 'Scans', 'Policies', and 'Users'. Below the navigation bar is a toolbar with buttons for 'Add', 'Edit', 'Browse', 'Launch', 'Pause', 'Stop', and 'Delete'. The main content area displays a table with the following data:

| Name | Owner | Status | Start Time |
|-----------------------|-------|---------------|--------------------|
| 192.168.206.134 Basic | demo | Template | Never |
| 192.168.206.134 Basic | demo | 0 IPs / 1 IPs | Jan 22, 2012 01:55 |
| 192.168.206.134 DVWA | demo | 0 IPs / 1 IPs | Jan 22, 2012 02:12 |
| 192.168.206.134 DVWA | demo | Template | Never |

Policies Tab

The Policies tab list the scan configurations available for scans



The screenshot shows the Nessus web interface. At the top left is the Nessus logo. On the right of the top bar are links for 'demo', 'Help', 'About', and 'Log out'. Below the top bar is a navigation menu with 'Policies' selected, and other options 'Reports', 'Scans', and 'Users'. Below the navigation menu is a toolbar with buttons for 'Add', 'Import', 'Export', 'Copy', 'Edit', and 'Delete'. Below the toolbar is a table with the following data:

| Name | Visibility | Owner |
|-----------------------------|------------|-------------------------------------|
| Basic Web App Tests | Shared | demo |
| DVWA Advanced Web App Tests | Shared | demo |
| External Network Scan | Shared | Tenable Policy Distribution Service |
| Internal Network Scan | Shared | Tenable Policy Distribution Service |
| Prepare for PCI DSS audits | Shared | Tenable Policy Distribution Service |
| Web App Tests | Shared | Tenable Policy Distribution Service |

Users Tab

The Users tab list users and allows the addition, deletion or editing of users accounts

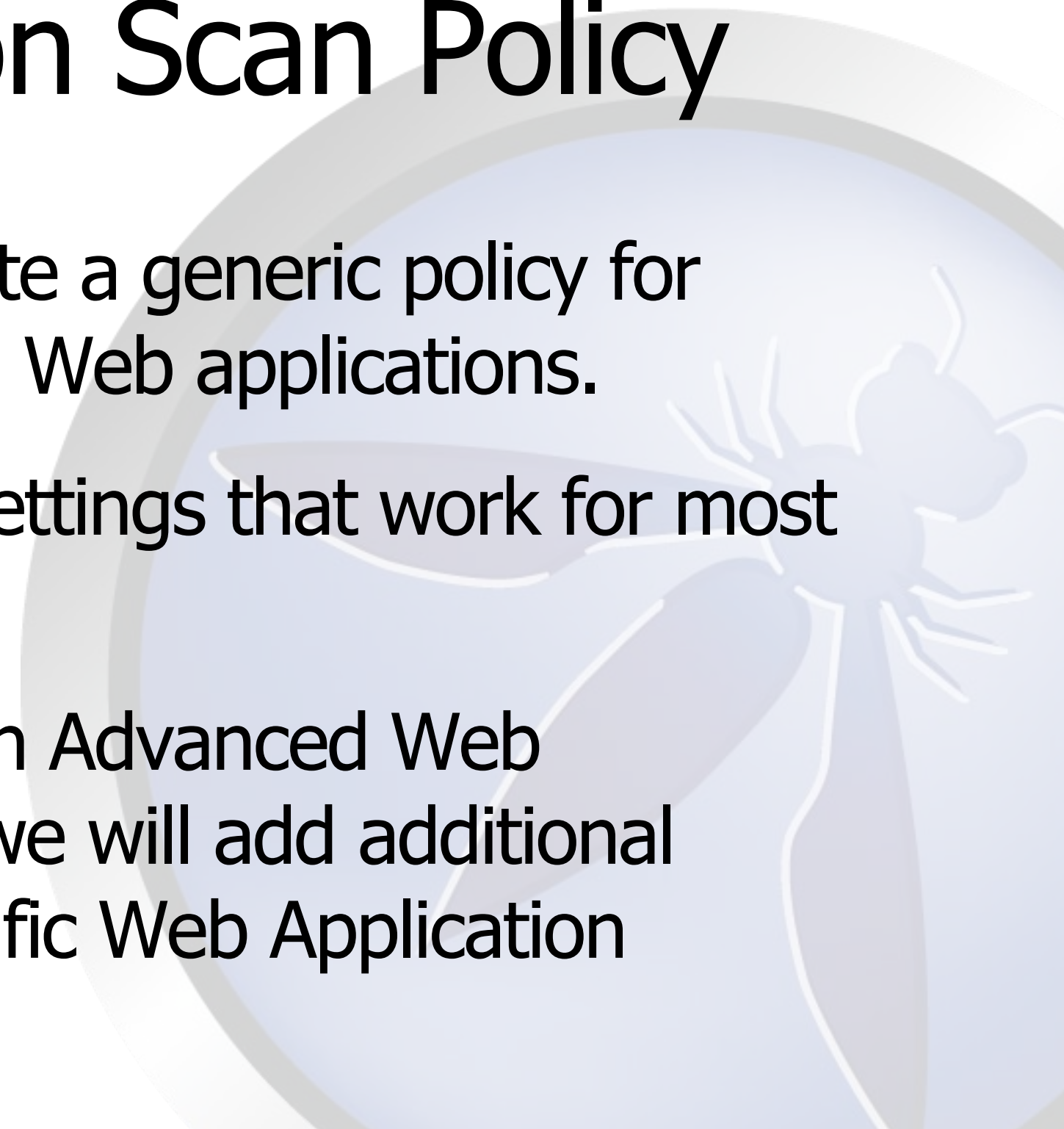


The screenshot shows the Nessus web interface. At the top left is the Nessus logo. On the right of the top bar are links for 'demo', 'Help', 'About', and 'Log out'. Below the top bar is a navigation menu with 'Users' selected. To the right of the menu are three buttons: 'Add' (with a green plus icon), 'Edit' (with a blue circular arrow icon), and 'Delete' (with a red minus icon). Below these buttons is a table with the following data:

| Name | Username | Role | Last Login |
|------|----------|---------------|--------------------|
| demo | demo | Administrator | Jan 22, 2012 17:22 |
| Rik | Rik | Administrator | Never Logged In |
| User | User | User | Never Logged In |



Creating a Basic Web Application Scan Policy

- ❖ The goal is to create a generic policy for scanning unknown Web applications.
 - ❖ We will set basic settings that work for most Web Applications
 - ❖ When we create an Advanced Web application policy we will add additional settings for a specific Web Application
- 

Creating a Basic Web Application Scan Policy

Step 1: Go to the Policies Tab and select the default "Web App Test" policy



The screenshot shows the Nessus web interface. The top navigation bar includes the Nessus logo, a user name 'demo', and links for 'Help', 'About', and 'Log out'. Below the navigation bar, there are tabs for 'Policies', 'Reports', 'Scans', and 'Users'. The 'Policies' tab is active. A toolbar contains buttons for 'Add', 'Import', 'Export', 'Copy', 'Edit', and 'Delete'. A table lists several policies with columns for Name, Visibility, and Owner. The 'Web App Tests' policy is highlighted in blue, and a red arrow points to it from the left.

| Name | Visibility | Owner |
|-----------------------------|------------|-------------------------------------|
| Basic Web App Tests | Shared | demo |
| DVWA Advanced Web App Tests | Shared | demo |
| External Network Scan | Shared | Tenable Policy Distribution Service |
| Internal Network Scan | Shared | Tenable Policy Distribution Service |
| Prepare for PCI DSS audits | Shared | Tenable Policy Distribution Service |
| Web App Tests | Shared | Tenable Policy Distribution Service |

Creating a Basic Web Application Scan Policy

Step 2: Click on the "Copy" button. This will create a new Policy called "Copy of Web App Test"



The screenshot shows the Nessus web interface. At the top, there is a navigation bar with the Nessus logo and user information (demo, Help, About, Log out). Below this is a secondary navigation bar with tabs for Policies, Reports, Scans, Policies, and Users. The main content area features a toolbar with buttons for Add, Import, Export, Copy, and Delete. A red arrow points to the Copy button. Below the toolbar is a table listing various scan policies.

| Name | Visibility | Owner |
|-----------------------------|------------|-------------------------------------|
| Basic Web App Tests | Shared | demo |
| DVWA Advanced Web App Tests | Shared | demo |
| External Network Scan | Shared | Tenable Policy Distribution Service |
| Internal Network Scan | Shared | Tenable Policy Distribution Service |
| Prepare for PCI DSS audits | Shared | Tenable Policy Distribution Service |
| Web App Tests | Shared | Tenable Policy Distribution Service |

Creating a Basic Web Application Scan Policy

Step 3: Select the new policy "Copy of Web App Test"



The screenshot shows the Nessus interface with the 'Policies' tab selected. The table below lists various policies, with 'Copy of Web App Tests' highlighted and a red arrow pointing to it.

| Name | Visibility | Owner |
|-----------------------------|------------|-------------------------------------|
| Basic Web App Tests | Shared | demo |
| Copy of Web App Tests | Shared | demo |
| DVWA Advanced Web App Tests | Shared | demo |
| External Network Scan | Shared | Tenable Policy Distribution Service |
| Internal Network Scan | Shared | Tenable Policy Distribution Service |
| Prepare for PCI DSS audits | Shared | Tenable Policy Distribution Service |
| Web App Tests | Shared | Tenable Policy Distribution Service |

Creating a Basic Web Application Scan Policy

Step 4: Click on the Edit Button



The screenshot shows the Nessus web interface. At the top left is the Nessus logo. The top right corner contains links for 'demo', 'Help', 'About', and 'Log out'. Below the logo is a navigation bar with tabs for 'Policies', 'Reports', 'Scans', 'Policies', and 'Users'. Underneath the navigation bar is a toolbar with buttons for 'Add', 'Import', 'Export', 'Copy', and 'Edit'. A red arrow points to the 'Edit' button. Below the toolbar is a table listing various scan policies.

| Name | Visibility | Owner |
|-----------------------------|------------|-------------------------------------|
| Basic Web App Tests | Shared | demo |
| Copy of Web App Tests | Shared | demo |
| DVWA Advanced Web App Tests | Shared | demo |
| External Network Scan | Shared | Tenable Policy Distribution Service |
| Internal Network Scan | Shared | Tenable Policy Distribution Service |
| Prepare for PCI DSS audits | Shared | Tenable Policy Distribution Service |
| Web App Tests | Shared | Tenable Policy Distribution Service |

Creating a Basic Web Application Scan Policy

This will open the Edit Policy screen

Edit Policy

General

Credentials

Plugins

Preferences

Basic

Name: Copy of Web App Tests

Visibility: Shared

Description:

Scan

Save Knowledge Base

Safe Checks

Silent Dependencies

Log Scan Details to Server

Stop Host Scan on Disconnect

Avoid Sequential Scans

Consider Unscanned Ports as Closed

Designate Hosts by their DNS Name

Network Congestion

Reduce Parallel Connections on Congestion

Use Kernel Congestion Detection (Linux Only)

Port Scanners

TCP Scan SNMP Scan Ping Host

UDP Scan Netstat SSH Scan

SYN Scan Netstat WMI Scan

Port Scan Options

Port Scan Range: default

Performance

Max Checks Per Host: 5

Max Hosts Per Scan: 80

Network Receive Timeout (seconds): 5

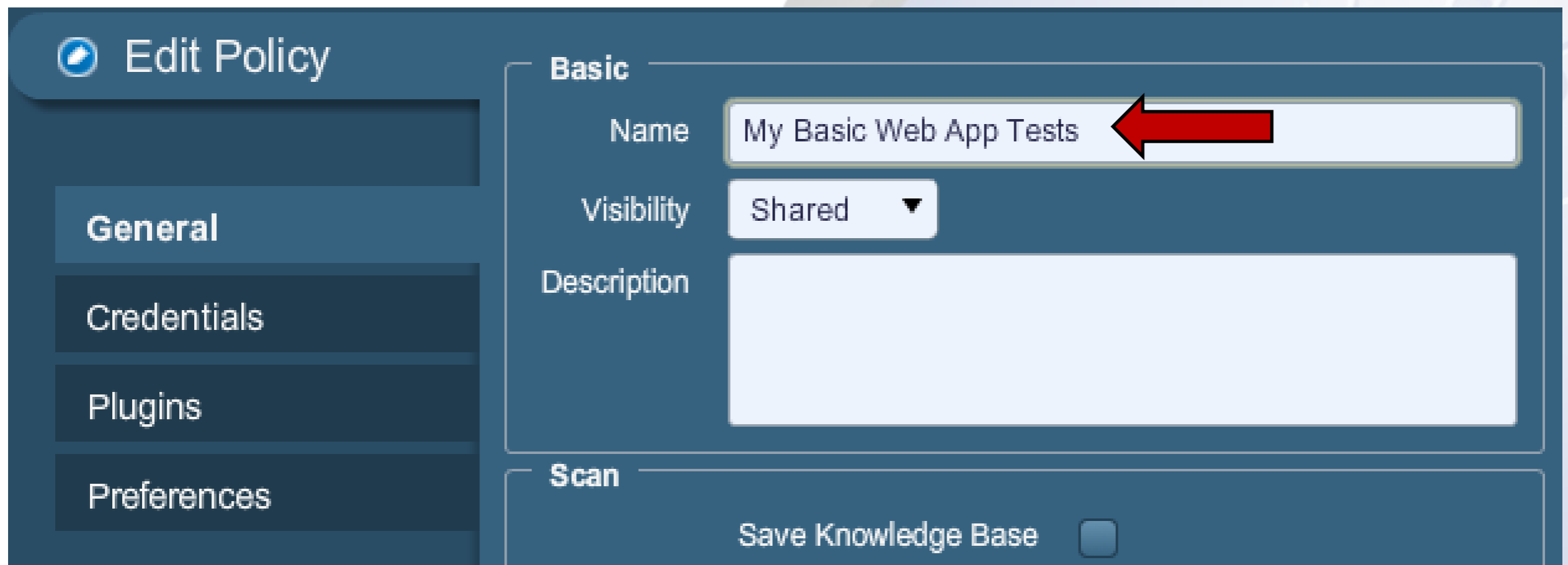
Max Simultaneous TCP Sessions Per Host: unlimited

Max Simultaneous TCP Sessions Per Scan: unlimited

Cancel Submit

Creating a Basic Web Application Scan Policy

Step 5: Change the policy name



The screenshot shows the 'Edit Policy' interface. On the left is a sidebar with a blue header 'Edit Policy' and four menu items: 'General', 'Credentials', 'Plugins', and 'Preferences'. The main area is divided into two sections: 'Basic' and 'Scan'. In the 'Basic' section, there are three fields: 'Name' with the text 'My Basic Web App Tests', 'Visibility' with a dropdown menu set to 'Shared', and 'Description' with an empty text area. A red arrow points to the 'Name' field. In the 'Scan' section, there is a checkbox labeled 'Save Knowledge Base' which is currently unchecked.

Creating a Basic Web Application Scan Policy

Step 6: Uncheck all port scanners except for "TCP Scan" and "Ping Host"

| Port Scanners | | | |
|---------------|-------------------------------------|------------------|-------------------------------------|
| TCP Scan | <input checked="" type="checkbox"/> | NMP Scan | <input type="checkbox"/> |
| UDP Scan | <input type="checkbox"/> | Netstat SSH Scan | <input type="checkbox"/> |
| SYN Scan | <input type="checkbox"/> | Netstat WMI Scan | <input type="checkbox"/> |
| | | Ping Host | <input checked="" type="checkbox"/> |

Creating a Basic Web Application Scan Policy

Step 7: Set the Port Scan Range

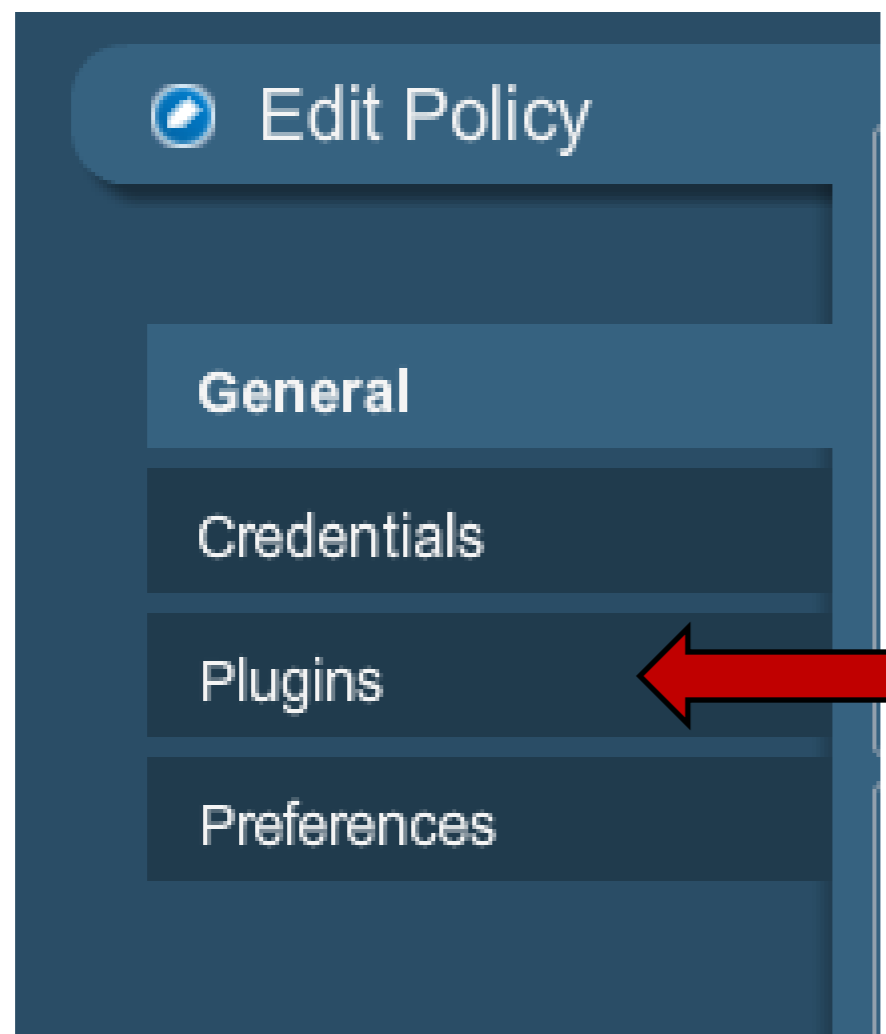
- default = all common ports listed in the "nessus-services" configuration file
- all = every port (1 - 65,535)
- Specific list (e.g. 80, 443, 8080, 8009)

Port Scan Options

Port Scan Range ←

Creating a Basic Web Application Scan Policy

Step 8: Click on the "Plugins" Side Tab



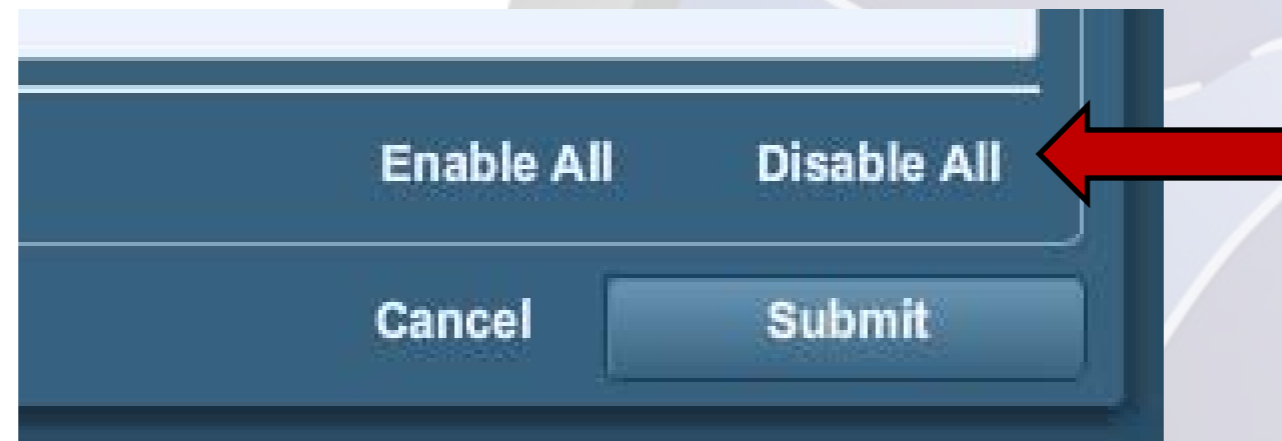
Creating a Basic Web Application Scan Policy

This should take you to the Plugins selection

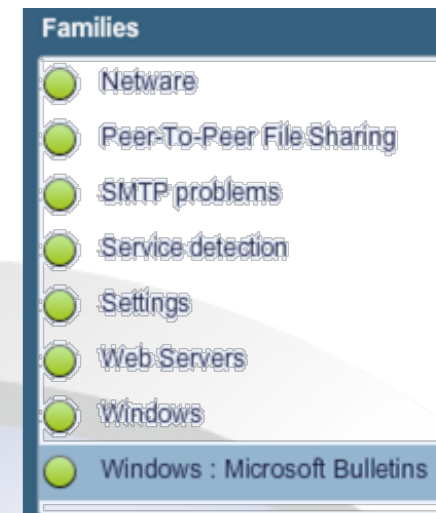
The screenshot displays the Nessus web interface. At the top left is the Nessus logo. The top navigation bar includes 'demo', 'Help', 'About', and 'Log out'. Below this is a secondary navigation bar with 'Policies', 'Reports', 'Scans', 'Policies', and 'Users'. The main content area is titled 'Edit Policy' and features a sidebar on the left with options: 'General', 'Credentials', 'Plugins' (selected), and 'Preferences'. The main area contains a 'Filter' section with a 'Name' dropdown and a search input field, a 'Show Only Enabled Plugins' checkbox, and a 'Reset Filter' button. Below the filter is a list of 'Families' with radio buttons: AIX Local Security Checks, Backdoors, Brute force attacks, CGI abuses, CGI abuses : XSS, CISCO, CentOS Local Security Checks, and DNS. To the right of the families list is an empty 'Plugins' selection area. At the bottom of the main area is a 'Plugin Description' text area. At the very bottom, there are statistics: 'Enabled Families: 43' and 'Enabled Plugins: 46891', along with 'Enable All', 'Disable All', 'Cancel', and 'Submit' buttons.

Creating a Basic Web Application Scan Policy

Step 9: Click on "Disable All" to disable all plugin families



Creating a Basic Web Application Scan Policy

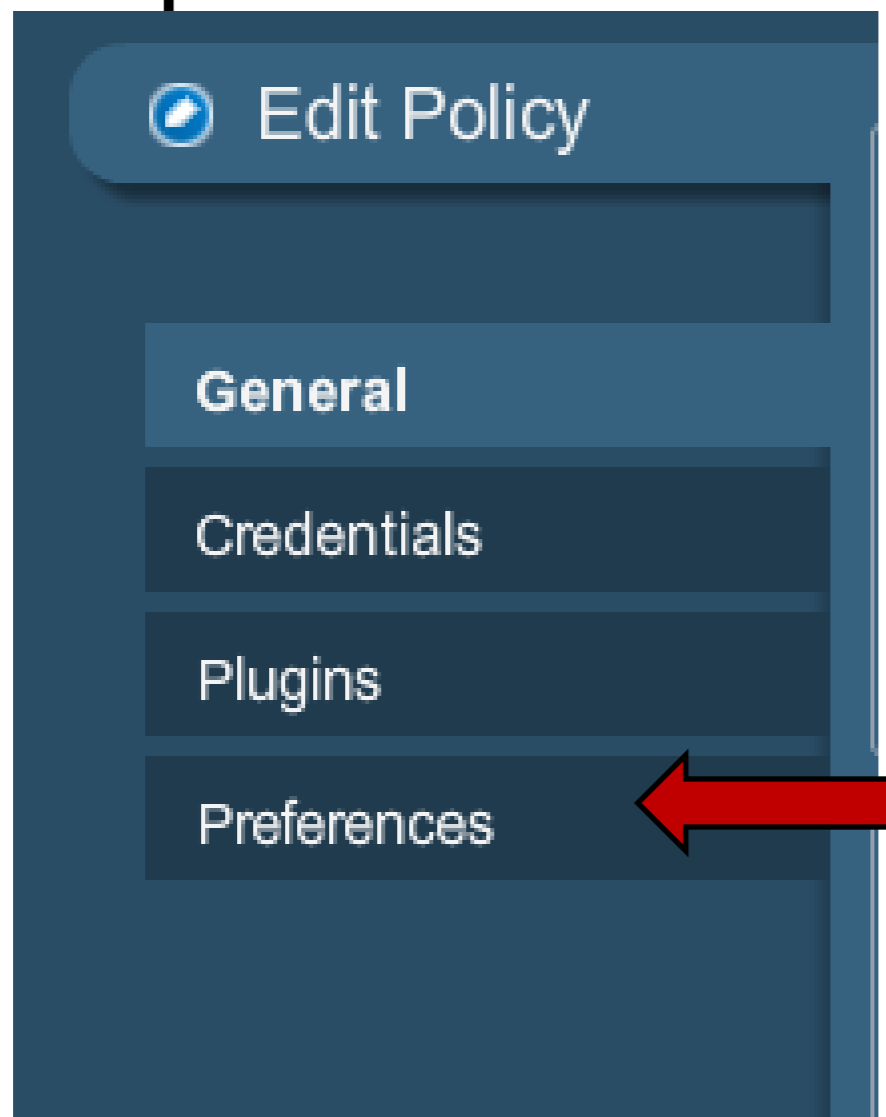


Step 10: Enable the following plugin families by clicking on the grey dot next to the family name

- Backdoors
- CGI Abuses
- CGI Abuses : XSS
- Cisco
- Databases
- FTP
- Firewalls
- Gain a shell remotely
- General
- Misc.
- Netware
- Peer-To-Pear File Sharing
- SMTP problems
- Service detection
- Settings
- Web Servers
- Windows
- Windows: Microsoft Bulletins

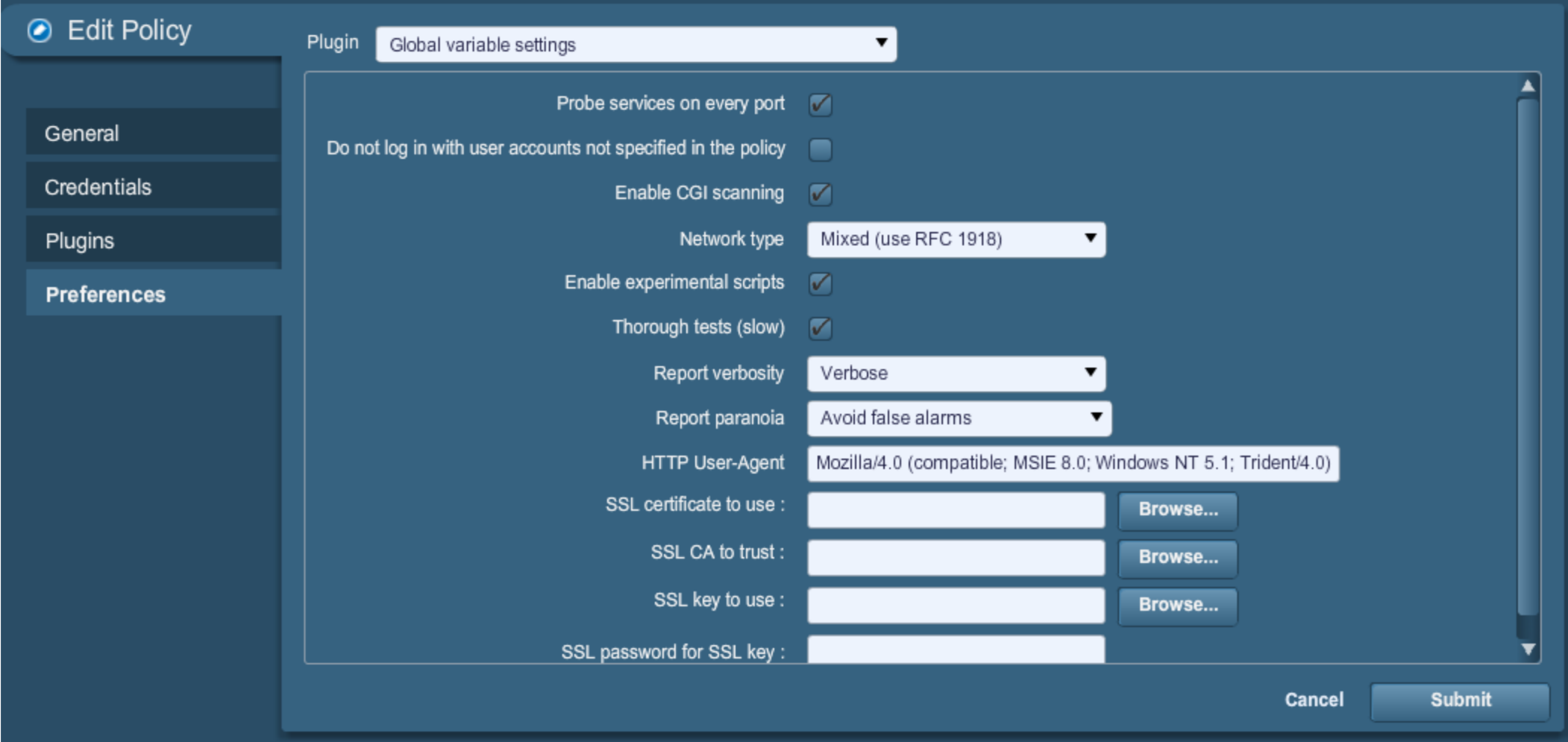
Creating a Basic Web Application Scan Policy

Step 11: Click on the "Preferences" Side Tab



Creating a Basic Web Application Scan Policy

This should take you to the Preferences section



The screenshot shows the 'Edit Policy' window with the 'Preferences' section selected in the left sidebar. The main area displays settings for the 'Global variable settings' plugin. The settings include:

- Probe services on every port:
- Do not log in with user accounts not specified in the policy:
- Enable CGI scanning:
- Network type: Mixed (use RFC 1918)
- Enable experimental scripts:
- Thorough tests (slow):
- Report verbosity: Verbose
- Report paranoia: Avoid false alarms
- HTTP User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
- SSL certificate to use: [text input] Browse...
- SSL CA to trust: [text input] Browse...
- SSL key to use: [text input] Browse...
- SSL password for SSL key: [text input]

Buttons for 'Cancel' and 'Submit' are located at the bottom right of the window.

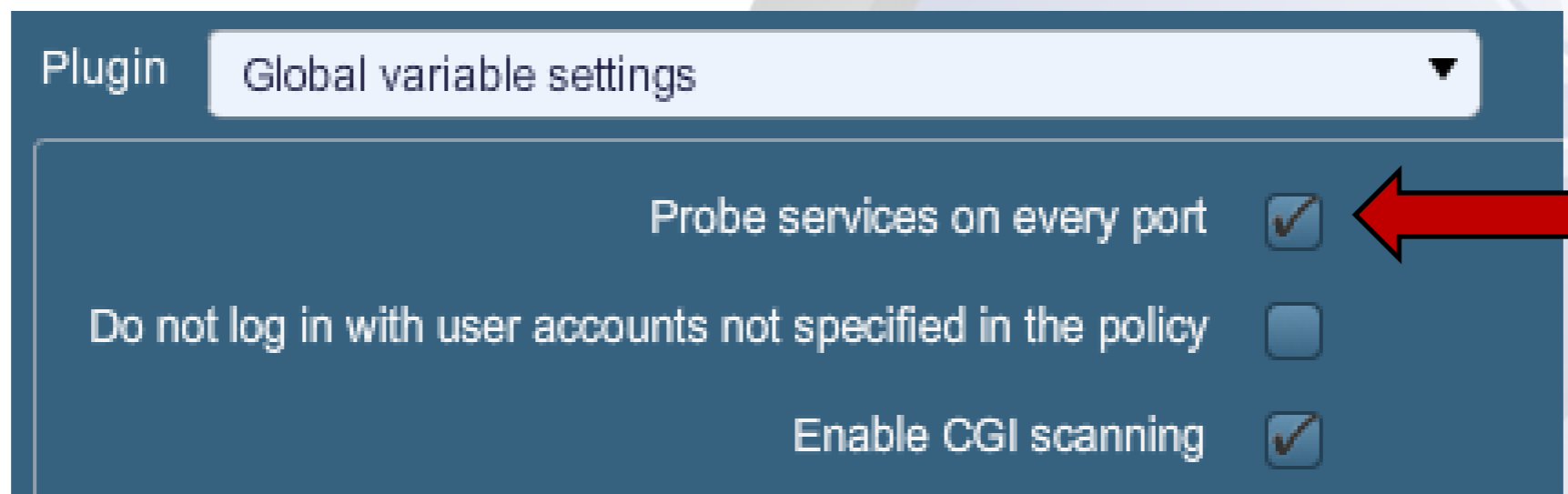
Creating a Basic Web Application Scan Policy

Step 12: Select "Global variable settings" from the Plugin pull down menu



Creating a Basic Web Application Scan Policy

Step 13: Check the "Probe services on every port" checkbox on "Global variable settings"

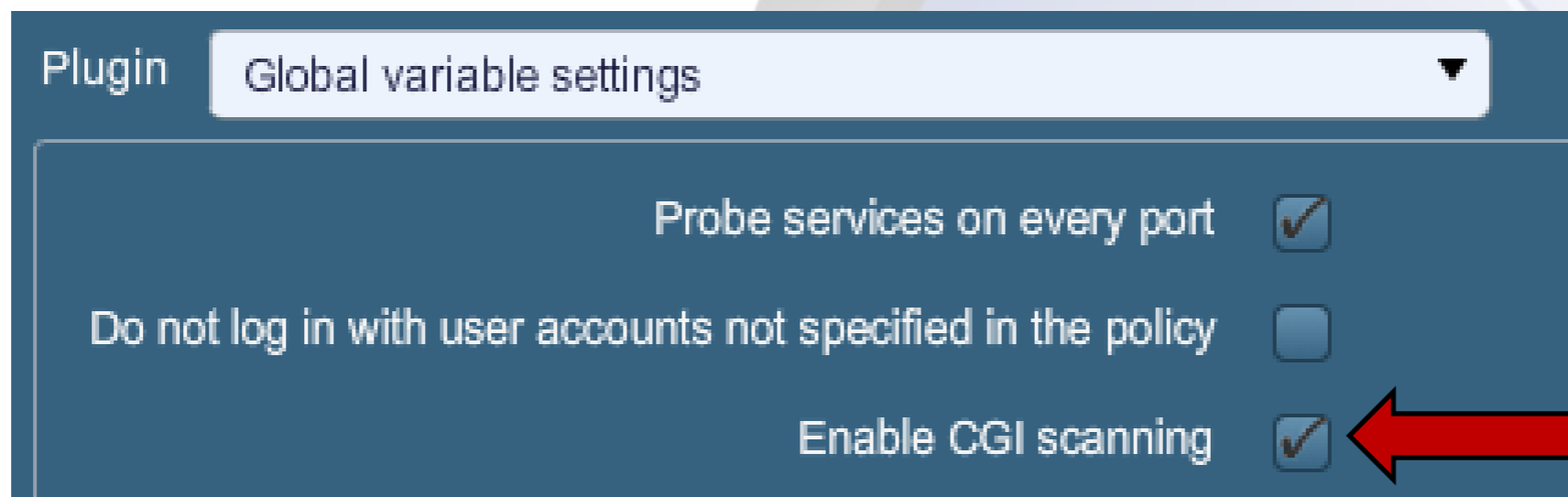


Plugin Global variable settings

| | |
|--|-------------------------------------|
| Probe services on every port | <input checked="" type="checkbox"/> |
| Do not log in with user accounts not specified in the policy | <input type="checkbox"/> |
| Enable CGI scanning | <input checked="" type="checkbox"/> |

Creating a Basic Web Application Scan Policy

Step 14: Check the "Enable CGI scanning" checkbox on "Global variable settings"

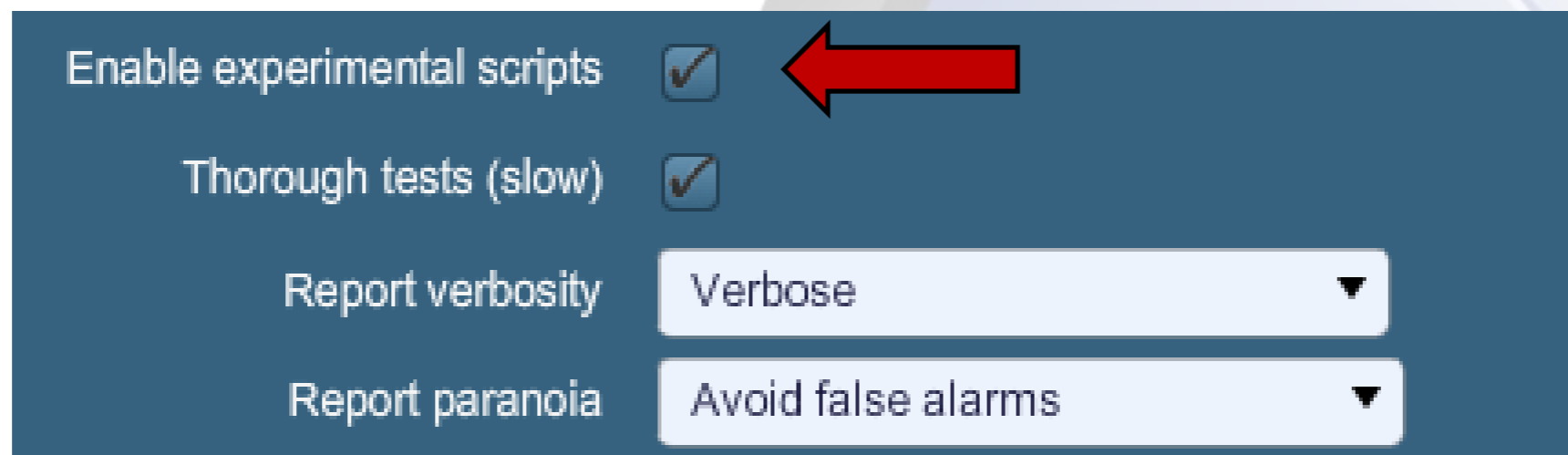


Plugin Global variable settings

| | |
|--|-------------------------------------|
| Probe services on every port | <input checked="" type="checkbox"/> |
| Do not log in with user accounts not specified in the policy | <input type="checkbox"/> |
| Enable CGI scanning | <input checked="" type="checkbox"/> |

Creating a Basic Web Application Scan Policy

Step 15: Check the “Enable experimental scripts” checkbox on “Global variable settings”

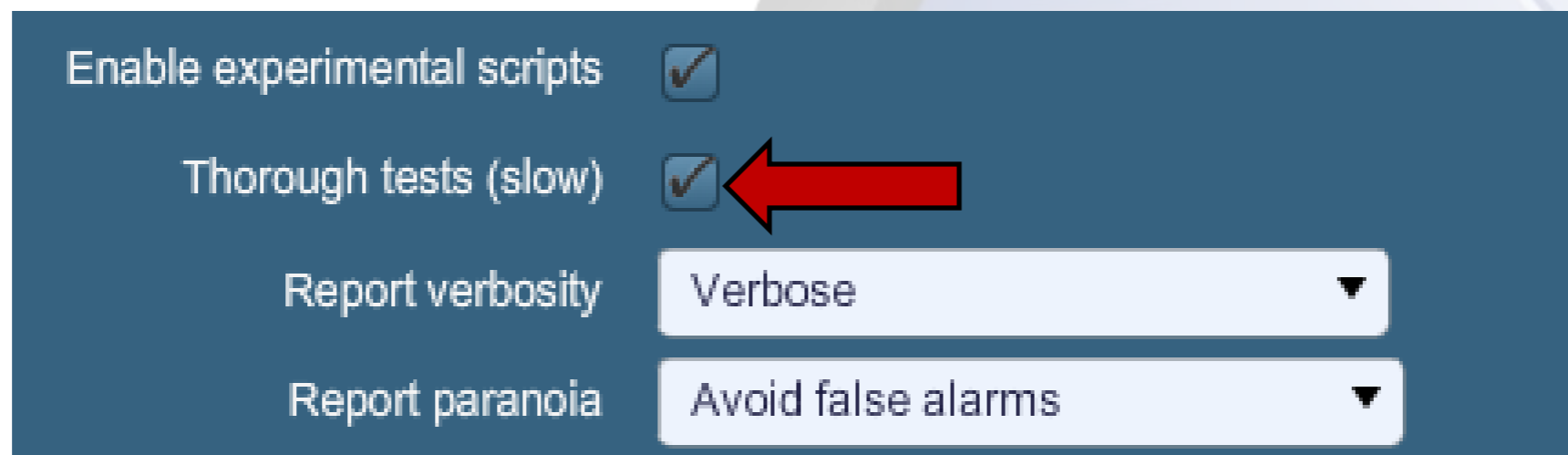


The screenshot shows a configuration panel with a dark blue background. It contains four settings:

- Enable experimental scripts (A red arrow points to this checkbox)
- Thorough tests (slow)
- Report verbosity: Verbose (dropdown menu)
- Report paranoia: Avoid false alarms (dropdown menu)

Creating a Basic Web Application Scan Policy

Step 16: Check the “Through test (slow)” checkbox on “Global variable settings”

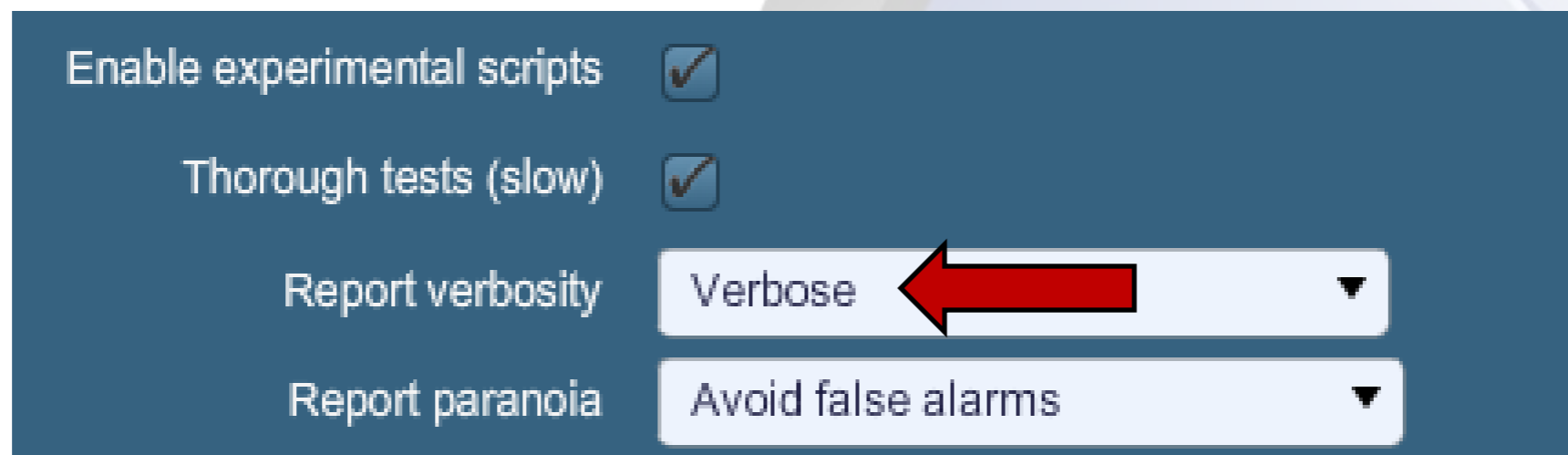



The screenshot shows a settings panel with a dark blue background. It contains four rows of settings:

- Enable experimental scripts:
- Thorough tests (slow): (highlighted with a red arrow)
- Report verbosity:
- Report paranoia:

Creating a Basic Web Application Scan Policy

Step 17: Set the "Report Verbosity" pull-down menu to "Verbose" on "Global variable settings"



| | |
|-----------------------------|---|
| Enable experimental scripts | <input checked="" type="checkbox"/> |
| Thorough tests (slow) | <input checked="" type="checkbox"/> |
| Report verbosity | Verbose  |
| Report paranoia | Avoid false alarms |

Creating a Basic Web Application Scan Policy

Step 18: Set the "Report paranoia" pull down menu to "Normal" on "Global variable settings"

| | |
|-----------------------------|-------------------------------------|
| Enable experimental scripts | <input checked="" type="checkbox"/> |
| Thorough tests (slow) | <input checked="" type="checkbox"/> |
| Report verbosity | Verbose ▼ |
| Report paranoia | Normal ← ▼ |

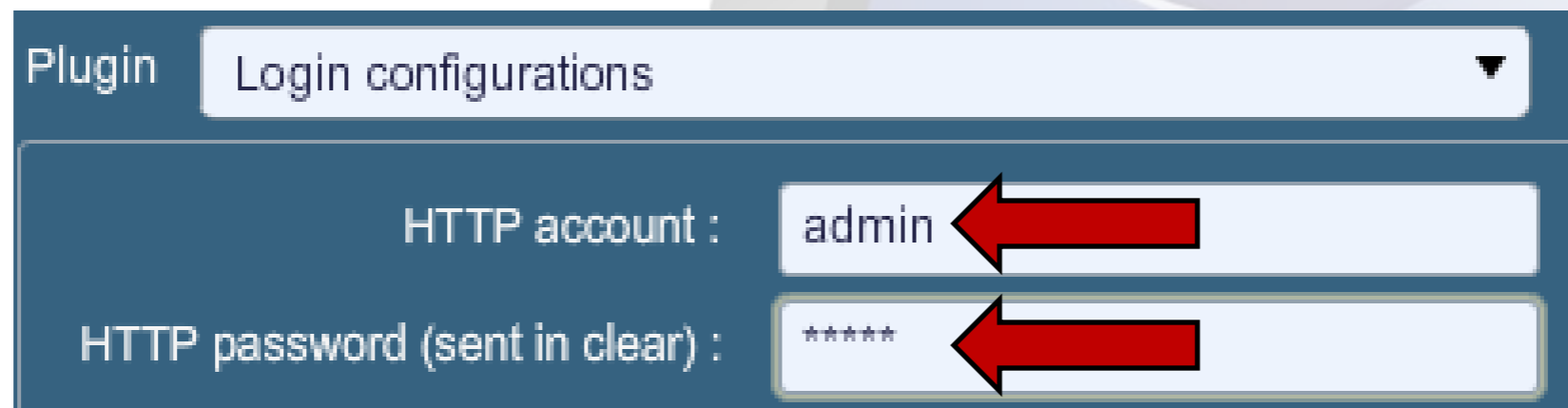
Creating a Basic Web Application Scan Policy

Step 19: Select "Login configurations" from the Plugin pull down menu



Creating a Basic Web Application Scan Policy

Step 20: Set the "HTTP account" and "HTTP password" on "Login configurations" to a value that is a common default in your environment.



Plugin Login configurations

HTTP account : admin

HTTP password (sent in clear) : *****

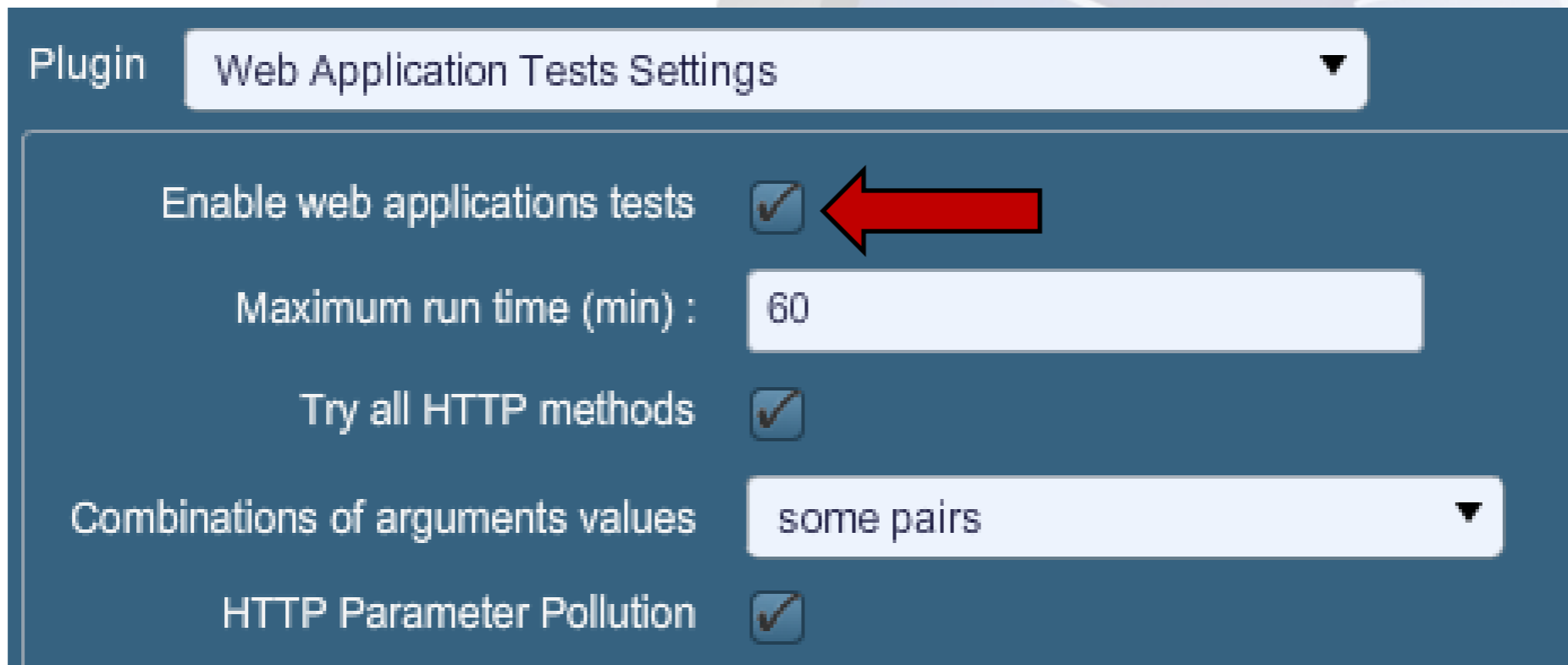
Creating a Basic Web Application Scan Policy

Step 21: Select “Web Application Test Settings” from the Plugin pull down menu



Creating a Basic Web Application Scan Policy

Step 22: Make sure that the “Enable web application test” checkbox is checked on “Web Application Test Settings”

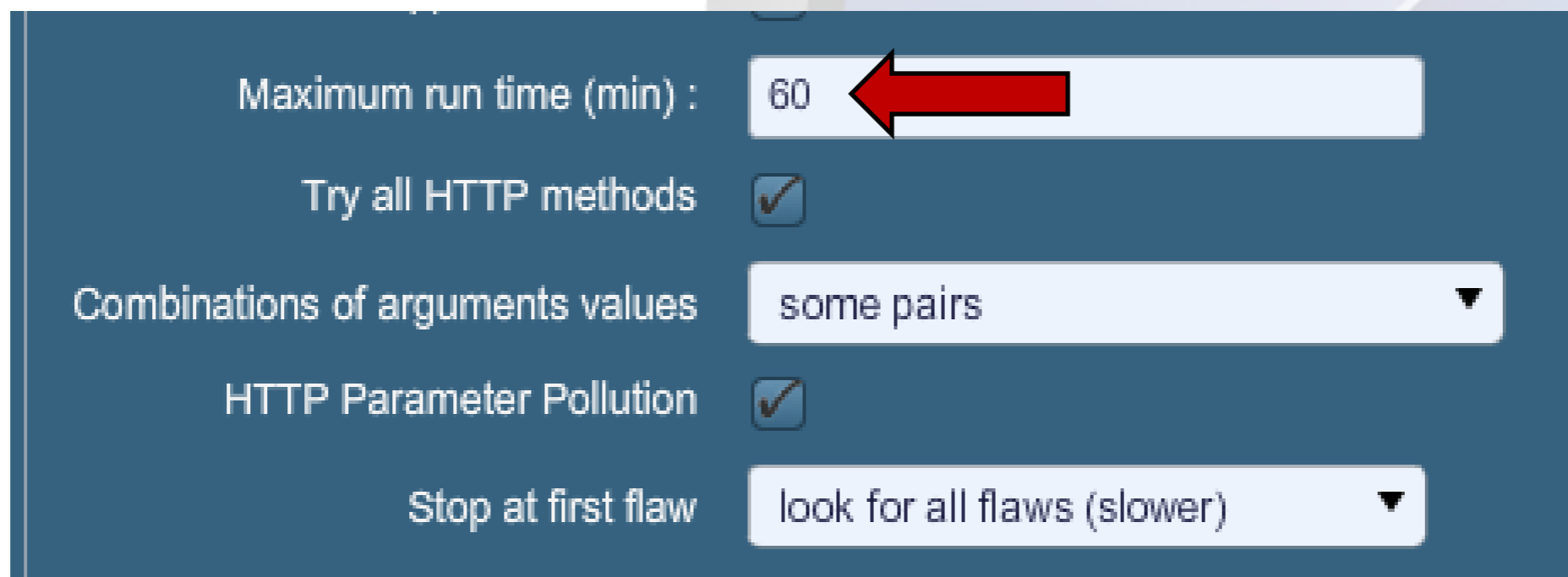


Plugin: Web Application Tests Settings

| | |
|----------------------------------|-------------------------------------|
| Enable web applications tests | <input checked="" type="checkbox"/> |
| Maximum run time (min) : | 60 |
| Try all HTTP methods | <input checked="" type="checkbox"/> |
| Combinations of arguments values | some pairs |
| HTTP Parameter Pollution | <input checked="" type="checkbox"/> |

Creating a Basic Web Application Scan Policy

Step 23: The “Maximum run time” on “Web Application Test Settings” can be left at the default of 60 min. If you see timeouts in the result you may need to increase this value

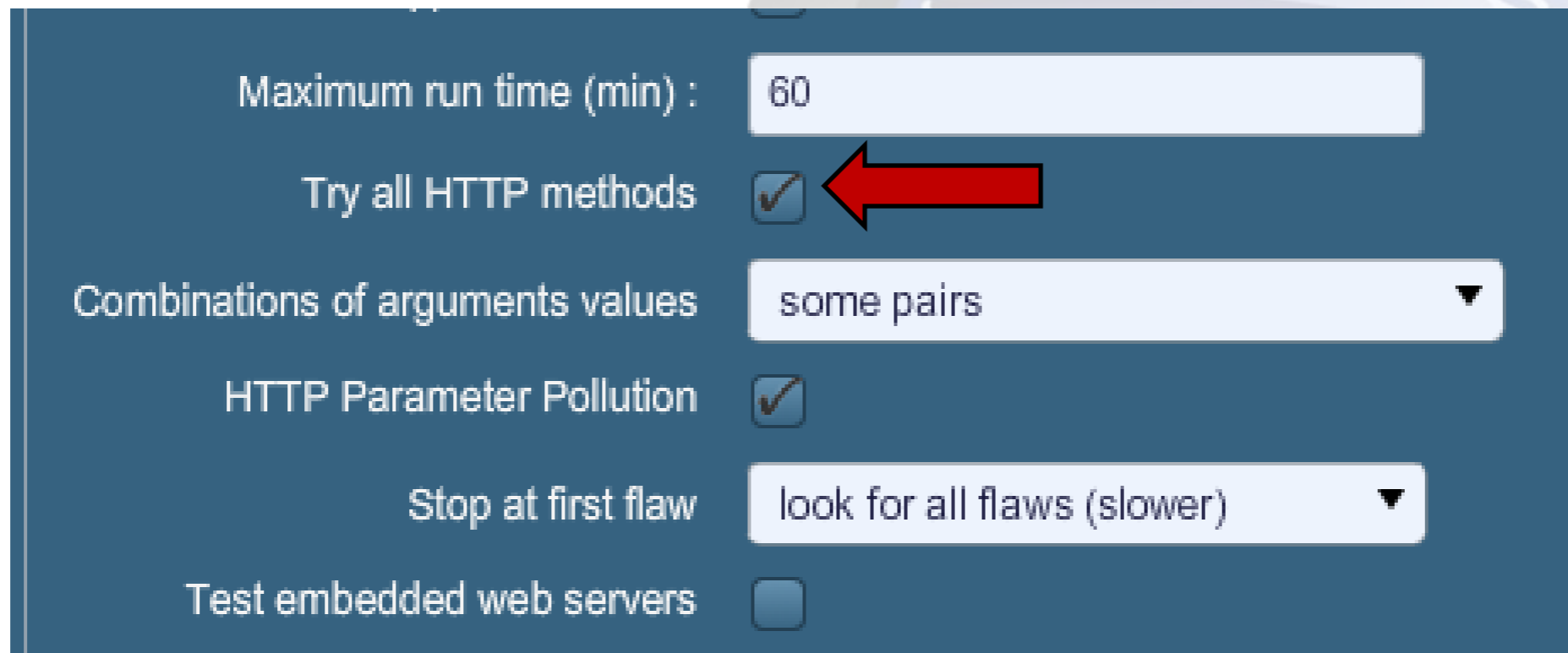


The screenshot shows a configuration panel for web application test settings. It includes a text input field for 'Maximum run time (min)' set to 60, a checked checkbox for 'Try all HTTP methods', a dropdown menu for 'Combinations of arguments values' set to 'some pairs', a checked checkbox for 'HTTP Parameter Pollution', and a dropdown menu for 'Stop at first flaw' set to 'look for all flaws (slower)'. A red arrow points to the '60' value in the run time field.

| | |
|----------------------------------|-------------------------------------|
| Maximum run time (min) : | 60 |
| Try all HTTP methods | <input checked="" type="checkbox"/> |
| Combinations of arguments values | some pairs |
| HTTP Parameter Pollution | <input checked="" type="checkbox"/> |
| Stop at first flaw | look for all flaws (slower) |

Creating a Basic Web Application Scan Policy

Step 24: Check the “Try all HTTP methods” on “Web Application Test Settings”



The screenshot shows a configuration window with a dark blue background and white text. It contains several settings for a web application scan. A red arrow points to the 'Try all HTTP methods' checkbox, which is checked. Other settings include a maximum run time of 60 minutes, combinations of argument values set to 'some pairs', HTTP parameter pollution checked, and the option to stop at the first flaw set to 'look for all flaws (slower)'. The 'Test embedded web servers' checkbox is unchecked.

| | |
|----------------------------------|--|
| Maximum run time (min) : | <input type="text" value="60"/> |
| Try all HTTP methods | <input checked="" type="checkbox"/> ← |
| Combinations of arguments values | <input type="text" value="some pairs"/> |
| HTTP Parameter Pollution | <input checked="" type="checkbox"/> |
| Stop at first flaw | <input type="text" value="look for all flaws (slower)"/> |
| Test embedded web servers | <input type="checkbox"/> |

Creating a Basic Web Application Scan Policy

Step 25: Set the “Combinations of Arguments values” pull-down menu to “some pairs”

| | |
|----------------------------------|-------------------------------------|
| Combinations of arguments values | some pairs |
| HTTP Parameter Pollution | <input checked="" type="checkbox"/> |
| Stop at first flaw | look for all flaws (slower) |
| Test embedded web servers | <input type="checkbox"/> |

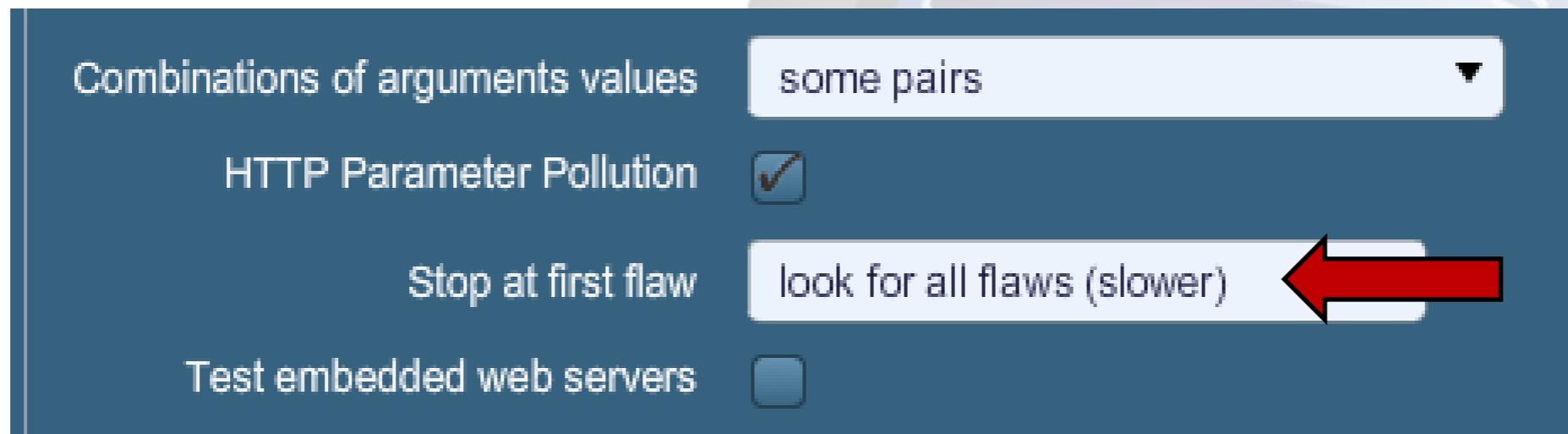
Creating a Basic Web Application Scan Policy

Step 26: Check the “HTTP Parameter Pollution” checkbox

| | | |
|----------------------------------|-------------------------------------|-----------------------------|
| Combinations of arguments values | <input type="checkbox"/> | some pairs |
| HTTP Parameter Pollution | <input checked="" type="checkbox"/> | |
| Stop at first flaw | <input type="checkbox"/> | look for all flaws (slower) |
| Test embedded web servers | <input type="checkbox"/> | |

Creating a Basic Web Application Scan Policy

Step 27: Set the “Stop at first flaw” pull-down menu to “look for all flaws” or “per parameter”



| | | |
|----------------------------------|-------------------------------------|-----------------------------|
| Combinations of arguments values | <input type="checkbox"/> | some pairs |
| HTTP Parameter Pollution | <input checked="" type="checkbox"/> | |
| Stop at first flaw | <input type="checkbox"/> | look for all flaws (slower) |
| Test embedded web servers | <input type="checkbox"/> | |

Creating a Basic Web Application Scan Policy

Step 28: Un-check the "Test embedded web servers" checkbox

| | |
|----------------------------------|--|
| Combinations of arguments values | <input type="text" value="some pairs"/> |
| HTTP Parameter Pollution | <input checked="" type="checkbox"/> |
| Stop at first flaw | <input type="text" value="look for all flaws (slower)"/> |
| Test embedded web servers | <input type="checkbox"/> ← |

Creating a Basic Web Application Scan Policy

Step 29: Select "Web mirroring" from the Plugin pull down menu



Creating a Basic Web Application Scan Policy

Step 30: Make sure that the “Follow dynamic pages” checkbox is checked on “Web mirroring”

Follow dynamic pages :



Creating a Basic Web Application Scan Policy

Step 31: Select "HTTP login page" from the Plugin pull down menu



Creating a Basic Web Application Scan Policy

Step 32: Check "Automated login page search" checkbox is checked on "HTTP login page"

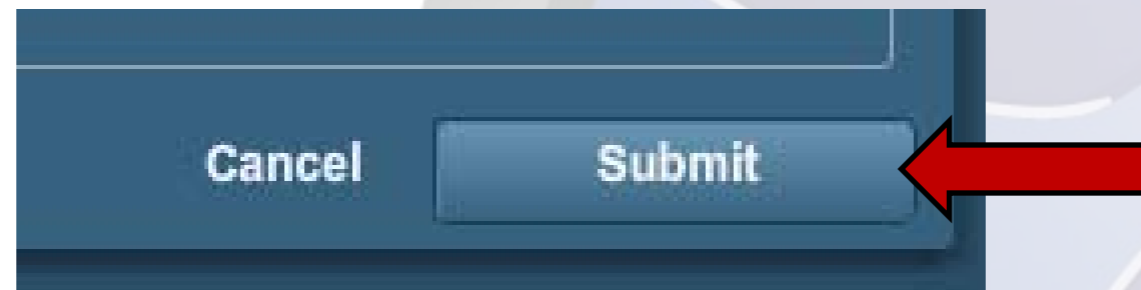
We will look at the other settings on this page in the Advanced Scan policy section

Automated login page search



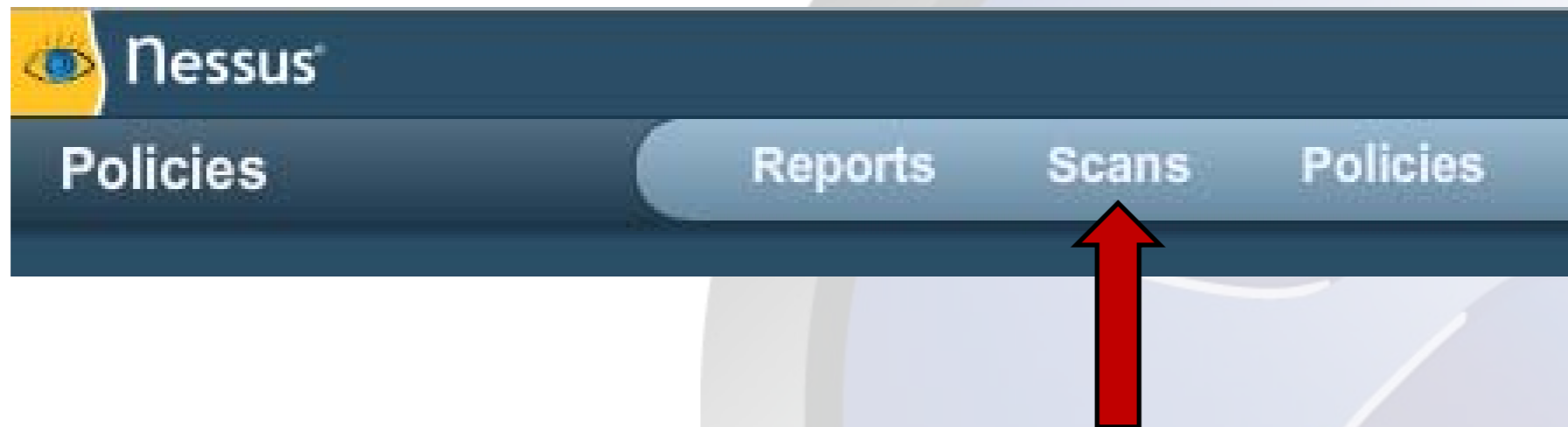
Creating a Basic Web Application Scan Policy

Step 33: Click on the Submit Button in lower right corner to save your policy



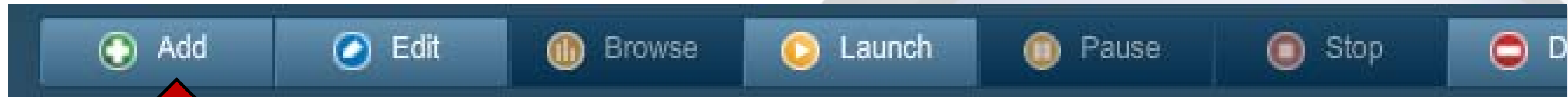
Create Basic Scan Template

Step 1: Click on the "Scan" tab on the top



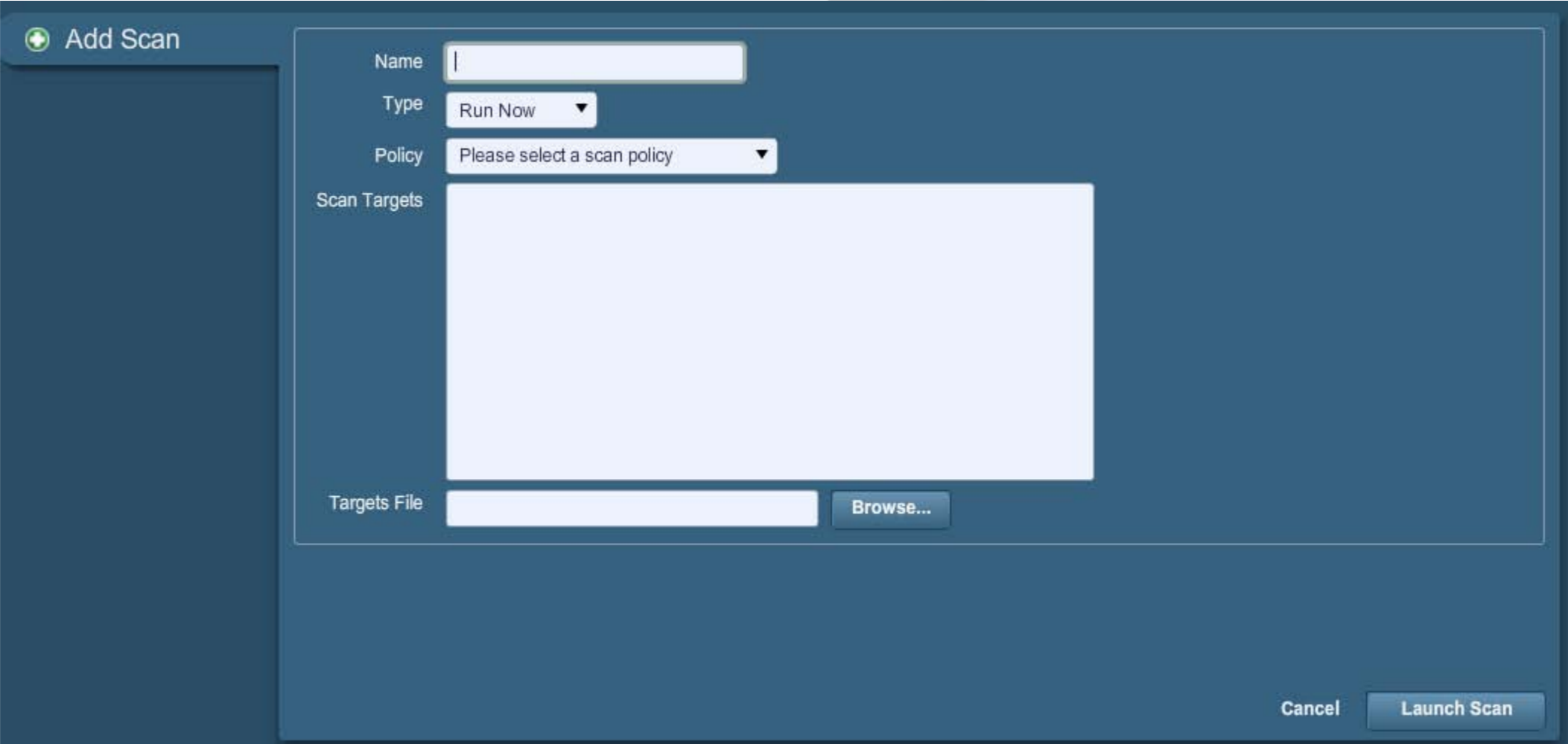
Create Basic Scan Template

Step 2: Click on the "Add" button



Create Basic Scan Template

This should take you to the interface to create a new scan.

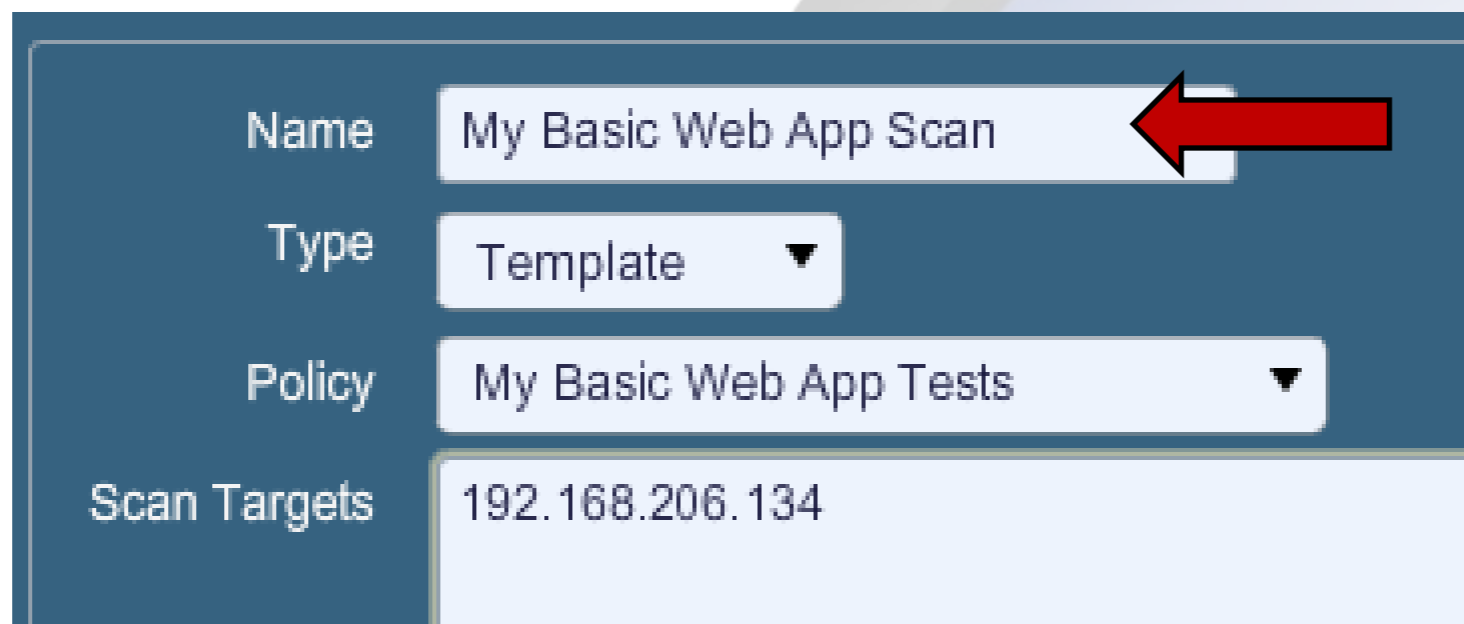


The screenshot displays a software interface titled "Add Scan". It features several input fields and buttons:

- Name:** A text input field.
- Type:** A dropdown menu currently set to "Run Now".
- Policy:** A dropdown menu with the text "Please select a scan policy".
- Scan Targets:** A large, empty text area.
- Targets File:** A text input field followed by a "Browse..." button.
- Buttons:** "Cancel" and "Launch Scan" buttons are located at the bottom right of the interface.

Create Basic Scan Template

Step 3: Name the Scan



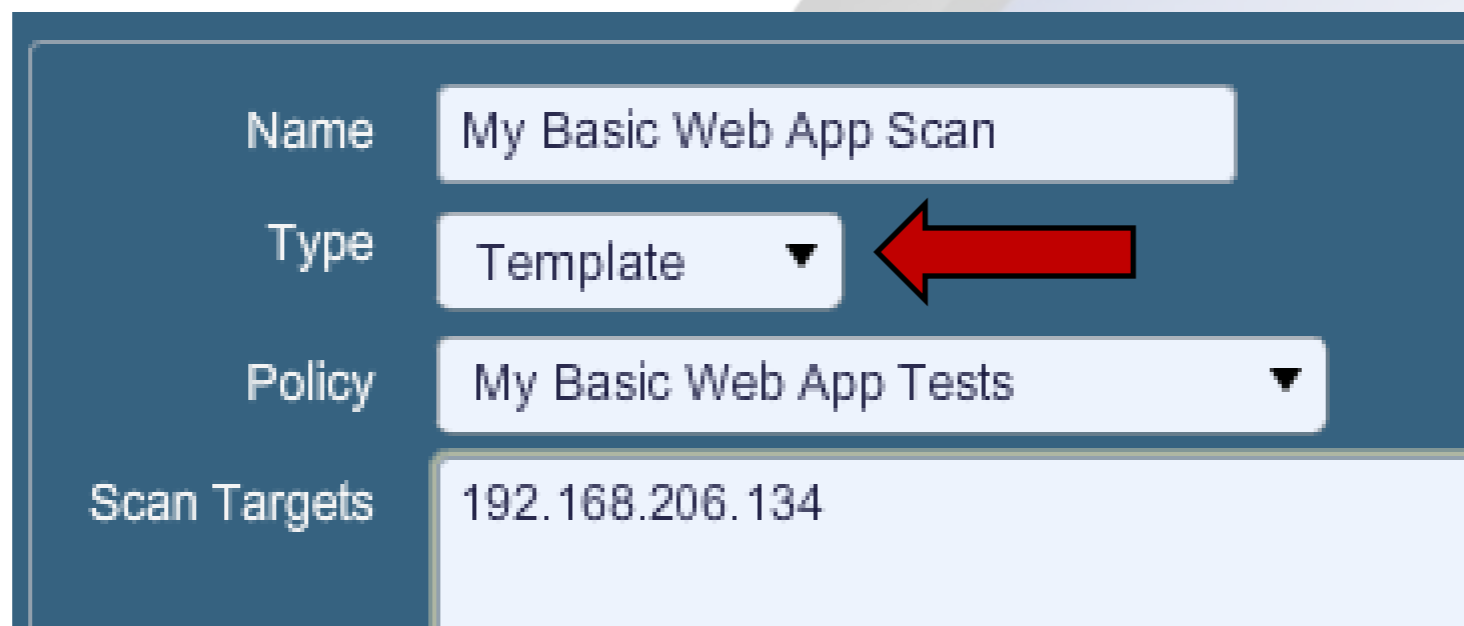
The screenshot shows a configuration form with the following fields:

| | |
|--------------|------------------------|
| Name | My Basic Web App Scan |
| Type | Template |
| Policy | My Basic Web App Tests |
| Scan Targets | 192.168.206.134 |


A red arrow points to the 'Name' field.

Create Basic Scan Template

Step 4: Set the scan Type to "Template"

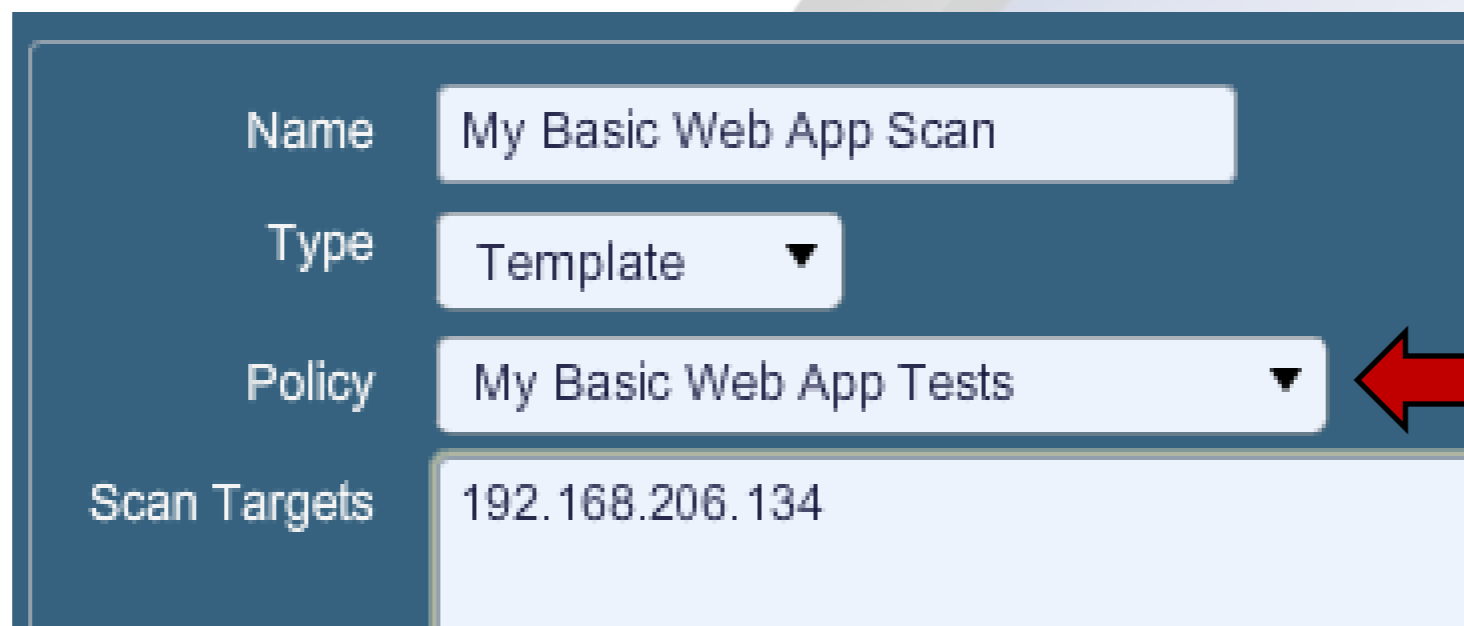


The screenshot shows a configuration form with the following fields:

| | |
|--------------|--|
| Name | My Basic Web App Scan |
| Type | Template  |
| Policy | My Basic Web App Tests |
| Scan Targets | 192.168.206.134 |

Create Basic Scan Template

Step 5: Select the Basic Web App policy you just created



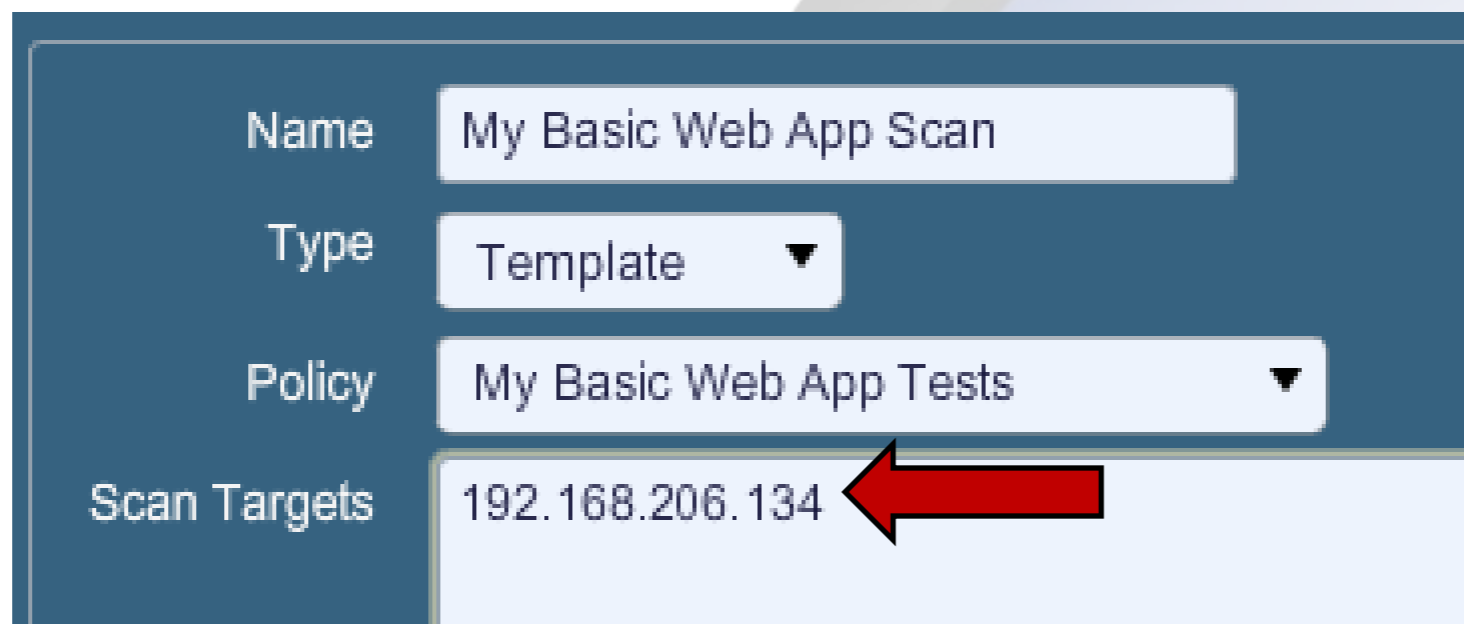
The screenshot shows a configuration form for a scan template. The form has a dark blue header and a light blue body. The fields are as follows:

| | |
|--------------|--------------------------|
| Name | My Basic Web App Scan |
| Type | Template ▼ |
| Policy | My Basic Web App Tests ▼ |
| Scan Targets | 192.168.206.134 |

A red arrow points to the 'Policy' dropdown menu, which is currently set to 'My Basic Web App Tests'.

Create Basic Scan Template

Step 6: Enter you scan target IP, domain name or network range

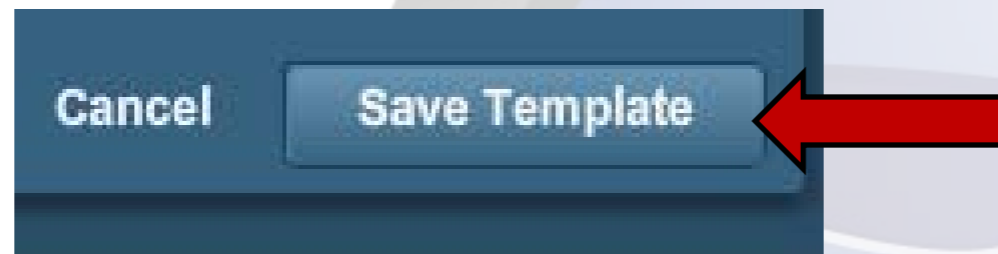


| | |
|--------------|--------------------------|
| Name | My Basic Web App Scan |
| Type | Template ▼ |
| Policy | My Basic Web App Tests ▼ |
| Scan Targets | 192.168.206.134 |

- single IP address or comma separated list (e.g., 192.168.0.1,192.168.206.134)
- IP range (e.g., 192.168.0.1-192.168.0.255)
- subnet with CIDR notation (e.g., 192.168.0.0/24)
- or resolvable host (e.g., www.nessus.org).

Create Basic Scan Template

Step 7: Click on the "Save Template" button to save your scan template



Running Basic Scan Template

Step 1: Select you Basic Scan Template on the Scans Tab



The screenshot shows a web application security tool interface. At the top, there are tabs for 'Scans', 'Reports', 'Policies', and 'Users'. Below the tabs, there are buttons for 'Add', 'Edit', 'Browse', 'Launch', 'Pause', and 'Stop'. The main area displays a table of scan templates.

| Name | Owner | Status | Start Time |
|-----------------------|-------|----------|------------|
| 192.168.206.134 Basic | demo | Template | Never |
| 192.168.206.134 DVWA | demo | Template | Never |
| My Basic Web App Scan | demo | Template | Never |

Running Basic Scan Template

Step 2: Click on the Launch Button



The screenshot shows a web application security tool interface. At the top, there are tabs for 'Reports', 'Scans', 'Policies', and 'Users'. Below the tabs is a toolbar with buttons for 'Add', 'Edit', 'Browse', 'Launch', 'Pause', and 'Stop'. The 'Launch' button is highlighted with a red arrow. Below the toolbar is a table with the following data:

| Name | Owner | Status | Start Time |
|-----------------------|-------|----------|------------|
| 192.168.206.134 Basic | demo | Template | Never |
| 192.168.206.134 DVWA | demo | Template | Never |
| My Basic Web App Scan | demo | Template | Never |

Running Basic Scan Template

“Template was successfully launched” should appear at the top of the screen and a “running copy” of your scan will appear in the list with a progress bar.

The screenshot shows the Nessus web interface. At the top, a yellow notification bar displays the message "Template was successfully launched." with a red arrow pointing to it. Below the notification, the "Scans" section is active, showing a table of scan templates. The table has columns for Name, Owner, Status, and Start Time. The third row, "My Basic Web App Scan", is highlighted in blue and shows a progress bar with the text "0 IPs / 1 IPs" and a red arrow pointing to it. The other rows are "192.168.206.134 Basic", "192.168.206.134 DVWA", and "My Basic Web App Scan".

| Name | Owner | Status | Start Time |
|-----------------------|-------|---------------|--------------|
| 192.168.206.134 Basic | demo | Template | Never |
| 192.168.206.134 DVWA | demo | Template | Never |
| My Basic Web App Scan | demo | 0 IPs / 1 IPs | , 2012 16:54 |
| My Basic Web App Scan | demo | Template | Never |

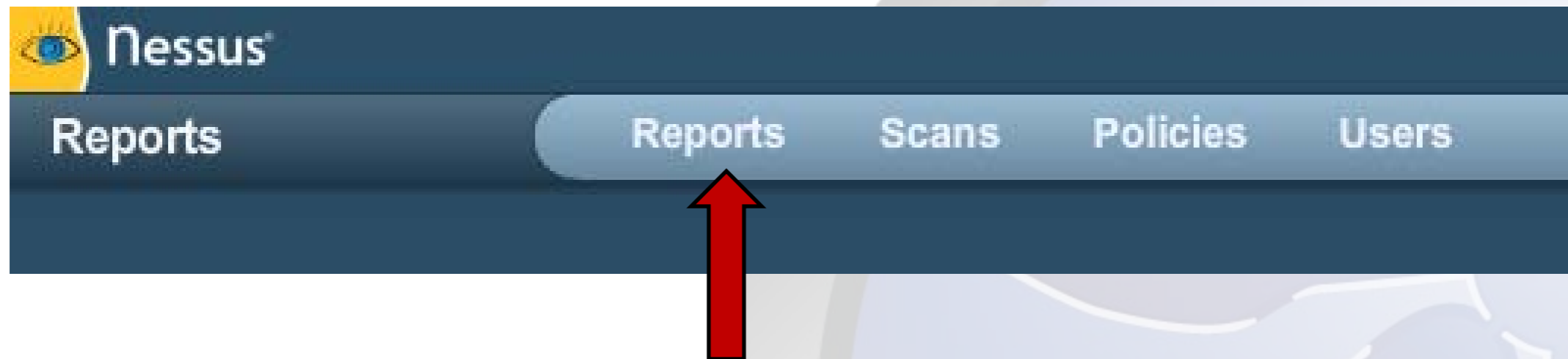
Basic Scan Policy Demo

The screenshot shows the Nessus web interface in a Mozilla Firefox browser window. The browser's address bar displays the URL `https://127.0.0.1:8834/`. The Nessus interface includes a navigation menu with 'Policies', 'Reports', 'Scans', and 'Users'. Below the menu is a toolbar with buttons for 'Add', 'Import', 'Export', 'Copy', 'Edit', and 'Delete'. The main content area is a table listing various scan policies.

| Name | Visibility | Owner |
|-----------------------------|------------|-------------------------------------|
| Basic Web App Tests 2 | Shared | demo |
| DVWA Advanced Web App Tests | Shared | demo |
| External Network Scan | Shared | Tenable Policy Distribution Service |
| Internal Network Scan | Shared | Tenable Policy Distribution Service |
| My Basic Web App Tests | Shared | demo |
| My Basic Web App Tests 1 | Shared | demo |
| My DVWA Web App Tests 1 | Private | demo |
| My DVWA Web App Tests 2 | Private | demo |
| Prepare for PCI DSS audits | Shared | Tenable Policy Distribution Service |
| Web App Tests | Shared | Tenable Policy Distribution Service |

Reviewing the Scan Report

Click on the Reports tab



Reviewing the Scan Report

To open the report double-click on your scan report or select it and click on the Browse button

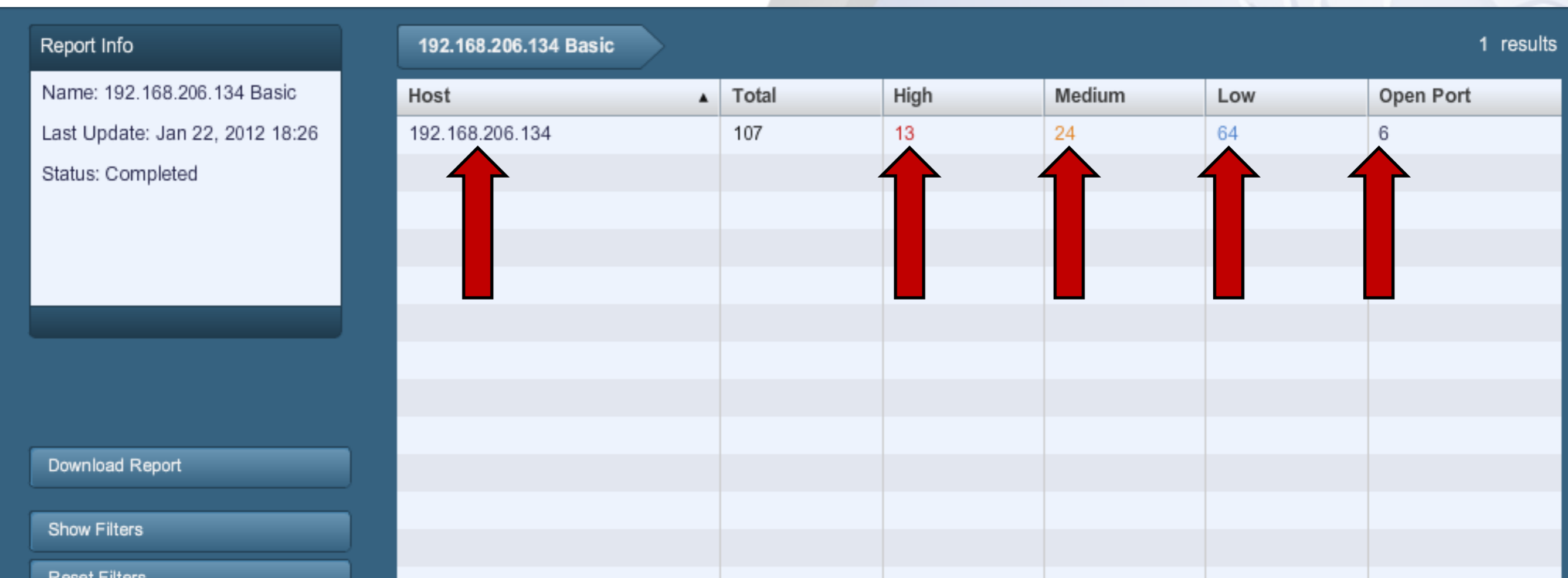


The screenshot shows the Nessus interface with the 'Reports' tab selected. A table lists scan reports with columns for Name, Status, and Last Updated. The 'Browse' button is highlighted with a red arrow, and the first row of the table is also highlighted with a red arrow.

| Name | Status | Last Updated |
|-----------------------|-----------|--------------------|
| My Basic Web App Scan | Running | Jan 25, 2012 12:09 |
| My Basic Web App Scan | Completed | Jan 24, 2012 17:01 |
| 192.168.206.134 DVWA | Completed | Jan 22, 2012 19:38 |
| 192.168.206.134 Basic | Completed | Jan 22, 2012 18:26 |

Reviewing the Scan Report

The scan report shows a list of IPs or domain names with indication of the number of High, Medium and Low Vulnerabilities and open ports



Report Info

Name: 192.168.206.134 Basic
Last Update: Jan 22, 2012 18:26
Status: Completed

Download Report
Show Filters
Reset Filters

192.168.206.134 Basic 1 results

| Host | Total | High | Medium | Low | Open Port |
|-----------------|-------|------|--------|-----|-----------|
| 192.168.206.134 | 107 | 13 | 24 | 64 | 6 |

Reviewing the Scan Report

Single click on the IP address to drill into each scanned device to get a list of open ports with vulnerability counts

| 192.168.206.134 Basic | | 192.168.206.134 | | 8 results | | | |
|-----------------------|----------|-----------------|-------|-----------|--------|-----|-----------|
| Port | Protocol | SVC Name | Total | High | Medium | Low | Open Port |
| 0 | udp | general | 1 | 0 | 0 | 1 | 0 |
| 0 | tcp | general | 9 | 0 | 0 | 9 | 0 |
| 0 | icmp | general | 1 | 0 | 0 | 1 | 0 |
| 22 | tcp | ssh | 4 | 0 | 0 | 3 | 1 |
| 80 | tcp | www | 66 | 13 | 22 | 29 | 2 |
| 143 | tcp | imap? | 2 | 0 | 0 | 1 | 1 |
| 445 | tcp | cifs | 1 | 0 | 0 | 1 | 0 |
| 8080 | tcp | www | 23 | 0 | 2 | 19 | 2 |

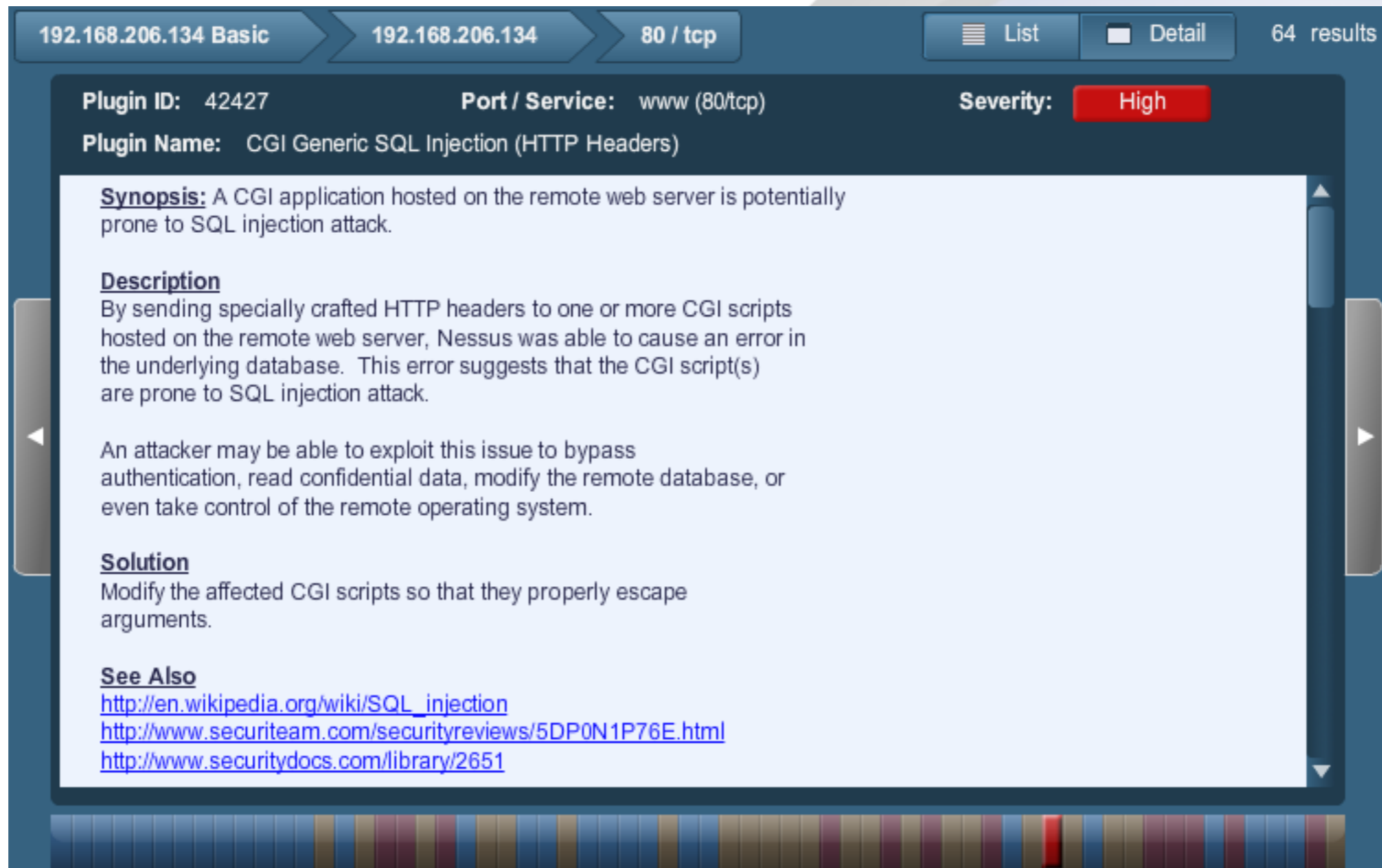
Reviewing the Scan Report

Single click on a port row to drill into the port to get a list of vulnerabilities found

| Plugin ID | Name | Port | Severity |
|-----------|---|--------------|----------|
| 24011 | WordPress Trackback Charset Decoding SQL Injection | www (80/tcp) | Medium |
| 55976 | Apache HTTP Server Byte Range DoS | www (80/tcp) | High |
| 47830 | CGI Generic Injectable Parameter | www (80/tcp) | Low |
| 47832 | CGI Generic On Site Request Forgery (OSRF) | www (80/tcp) | Medium |
| 42427 | CGI Generic SQL Injection (HTTP Headers) | www (80/tcp) | High |
| 49067 | CGI Generic HTML Injections (quick test) | www (80/tcp) | Medium |
| 33817 | CGI Generic Tests Load Estimation (all tests) | www (80/tcp) | Low |
| 50494 | CGI Generic Path Traversal (quick test) | www (80/tcp) | Medium |
| 51972 | CGI Generic Cross-Site Scripting (Parameters Names) | www (80/tcp) | Medium |
| 51973 | CGI Generic SQL Injection (Parameters Names) | www (80/tcp) | High |
| 11139 | CGI Generic SQL Injection | www (80/tcp) | High |

Reviewing the Scan Report

Single click on a vulnerabilities to see the details



The screenshot shows a Nessus scan report for a vulnerability. The interface includes a breadcrumb trail: 192.168.206.134 Basic > 192.168.206.134 > 80 / tcp. There are buttons for 'List' and 'Detail', and a '64 results' indicator. The vulnerability details are as follows:

Plugin ID: 42427 **Port / Service:** www (80/tcp) **Severity:** High

Plugin Name: CGI Generic SQL Injection (HTTP Headers)

Synopsis: A CGI application hosted on the remote web server is potentially prone to SQL injection attack.

Description
By sending specially crafted HTTP headers to one or more CGI scripts hosted on the remote web server, Nessus was able to cause an error in the underlying database. This error suggests that the CGI script(s) are prone to SQL injection attack.

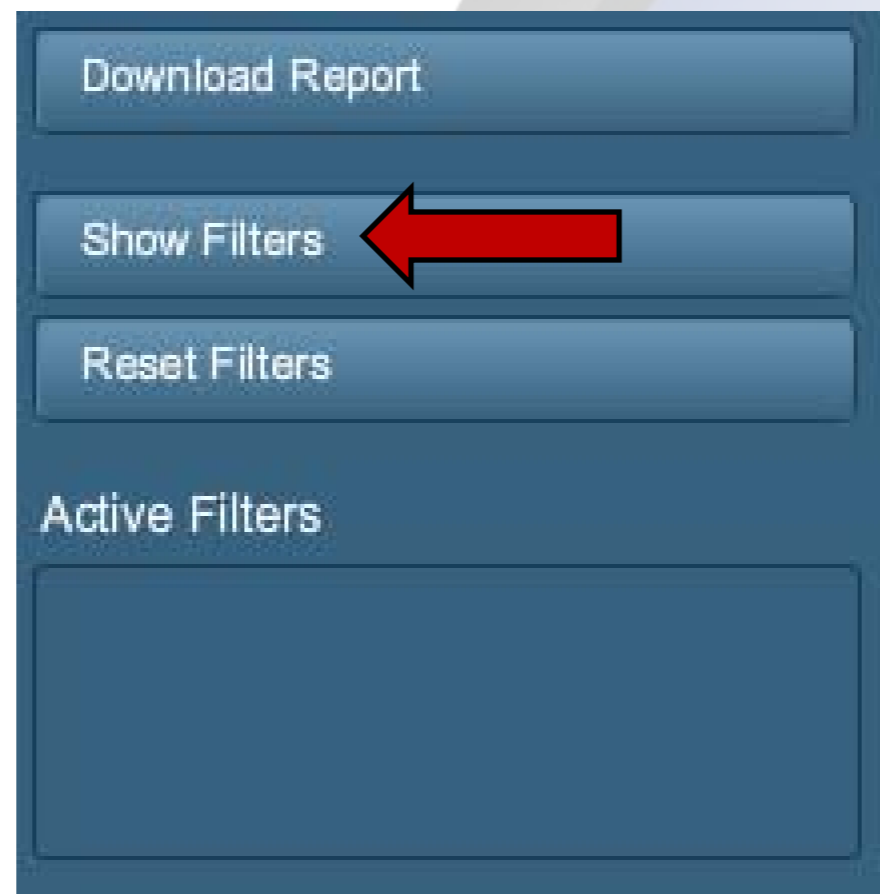
An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.

Solution
Modify the affected CGI scripts so that they properly escape arguments.

See Also
http://en.wikipedia.org/wiki/SQL_injection
<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
<http://www.securitydocs.com/library/2651>

Reviewing the Scan Report

To find a specific vulnerability click on the "Show Filters" button



Reviewing the Scan Report

You have lot of options here. We are going to look for a specific Plugin by ID to check for Timeouts

The screenshot shows a 'Filters' dialog box with the following configuration:

| Field | Operator | Value |
|--------------------|--------------------------|-------|
| Plugin ID | is equal to | 39470 |
| Plugin Name | contains | |
| Vulnerability Text | contains | |
| Host | contains | |
| Ports | is equal to | |
| Protocol | contains | |
| Severity | All | |
| Exploits Exist | <input type="checkbox"/> | |

Buttons: Cancel, Apply

Reviewing the Scan Report

Looking at the details of Plugin #39470 will tell you if you need to increase your CGI run time

Plugin ID: 39470

Port / Service: www (80/tcp)

Plugin Name: CGI Generic Tests Timeout

Synopsis: Some generic CGI attacks ran out of time.

Description

Some generic CGI tests ran out of time during the scan.
The results may be incomplete.



Solution

Run your run scan again with a longer timeout or less ambitious options :

- Combinations of arguments values = 'all combinations' is much slower than 'two pairs' or 'single'.
- Stop at first flaw = 'per port' is quicker.

Downloading Scan Report

To download your scan report select it in the reports list and click on the "Download" button

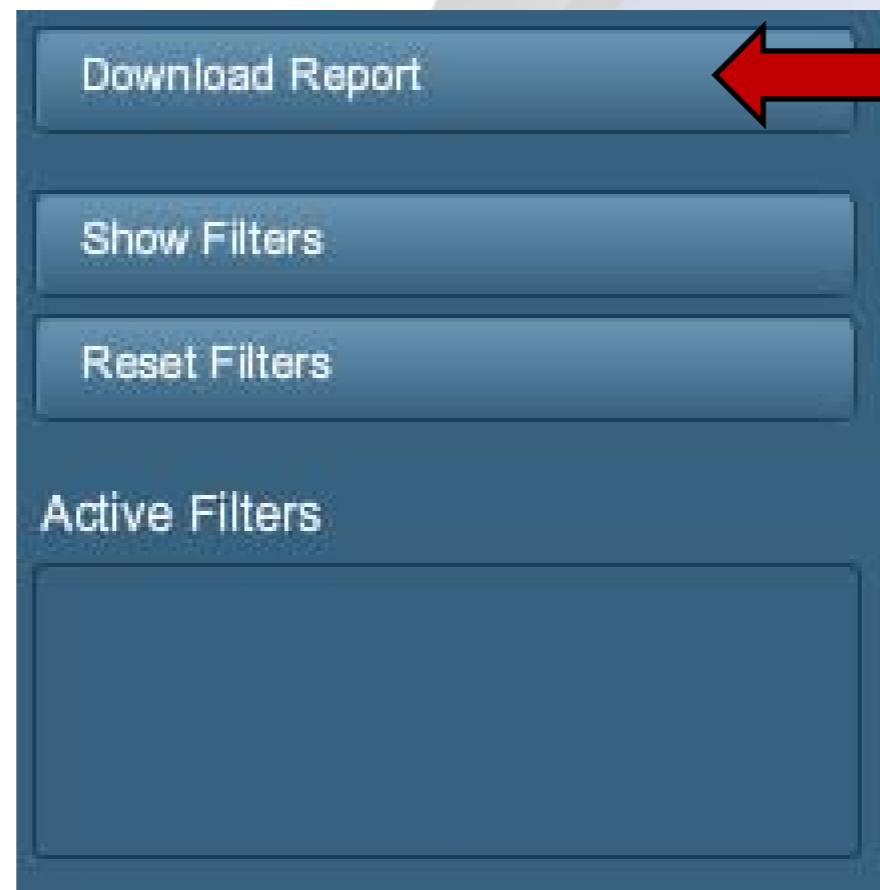


The screenshot shows the Nessus web interface. At the top left is the Nessus logo. The top right corner has links for 'demo', 'Help', and 'About'. Below the logo is a navigation bar with 'Reports', 'Scans', 'Policies', and 'Users'. Underneath is a toolbar with buttons for 'Browse', 'Compare', 'Upload', 'Download', and a minus sign. A red arrow points to the 'Download' button. Below the toolbar is a table with three columns: 'Name', 'Status', and 'Last Updated'.

| Name | Status | Last Updated |
|-----------------------|-----------|--------------------|
| My Basic Web App Scan | Running | Jan 25, 2012 12:09 |
| My Basic Web App Scan | Completed | Jan 24, 2012 17:01 |
| 192.168.206.134 DVWA | Completed | Jan 22, 2012 19:38 |
| 192.168.206.134 Basic | Completed | Jan 22, 2012 18:26 |

Downloading Scan Report

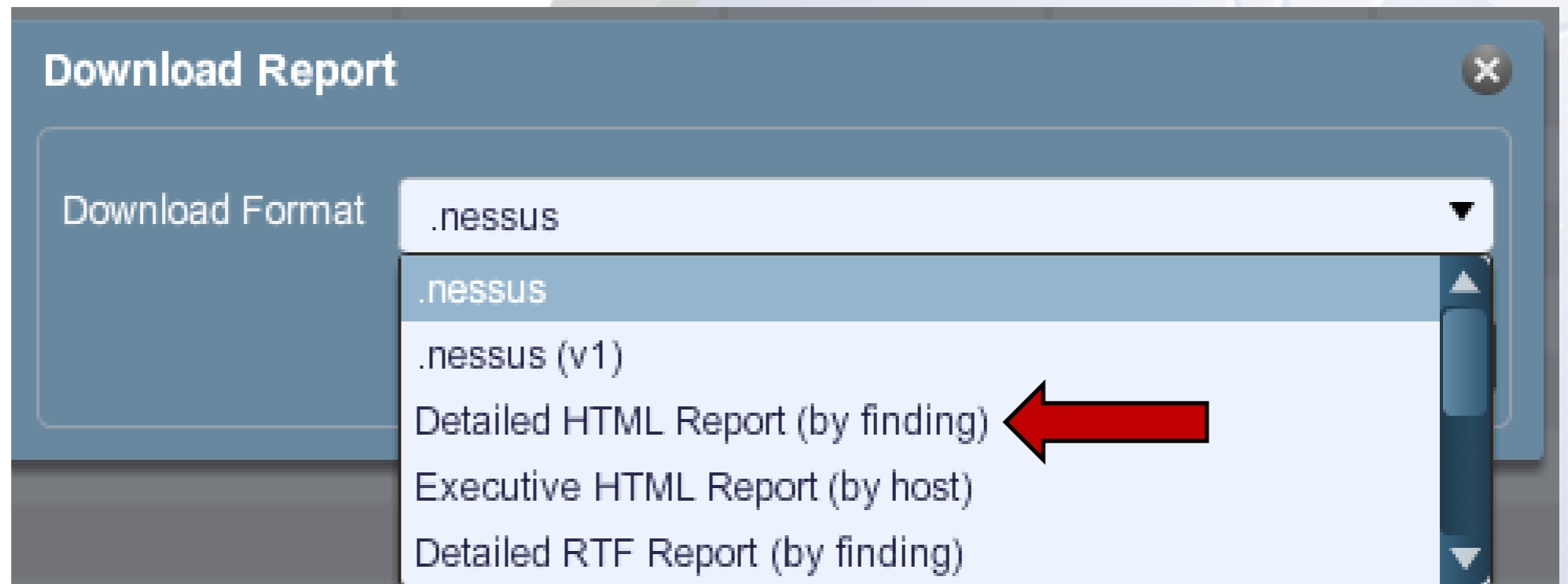
or when viewing the report click on the download button. Note that any filters current applied will be applied to the downloaded report



Downloading Scan Report

Select a Download format

- .nessus & .nessus(v1) can edited and re-imported (XML)
- HTML Detailed or HTML Executive Reports
- RTF
- Custom



HTML Standard Report

List of hosts

[192.168.206.134](#)

High Severity problem(s) found

[\[^\] Back](#)

192.168.206.134

Scan Time

| | |
|--------------|--------------------------|
| Start time : | Sun Jan 22 01:55:10 2012 |
| End time : | Sun Jan 22 18:26:17 2012 |

Number of vulnerabilities

| | |
|--------------|----|
| Open ports : | 4 |
| High : | 13 |
| Medium : | 24 |
| Low : | 64 |

Remote host information

| | |
|--------------------|--|
| Operating System : | Linux Kernel 2.6 on Ubuntu 10.04 (lucid) |
| NetBIOS name : | OWASPBWA |
| DNS name : | |

[\[^\] Back to 192.168.206.134](#)

Port general (0/udp)

[\[-/+\]](#)

Traceroute Information

Synopsis:

It was possible to obtain traceroute information.

HTML Detailed Report



List of Plugin IDs

[>PRINT](#)

The following plugin IDs have problems associated with them. Select the ID to review more detail.

| PLUGIN ID# | # OF ISSUES | PLUGIN NAME | SEVERITY |
|-----------------------|-------------|---|----------------------------------|
| 26968 | 1 | TikiWiki tiki-graph_formula.php f Parameter Arbitrary Command Execution | High Severity problem(s) found |
| 15780 | 1 | phpBB viewtopic.php highlight Parameter SQL Injection | High Severity problem(s) found |
| 17225 | 1 | phpBB <= 2.0.12 Multiple Vulnerabilities | High Severity problem(s) found |
| 13655 | 1 | phpBB < 2.0.9 Multiple Vulnerabilities | High Severity problem(s) found |
| 11938 | 1 | phpBB < 2.0.7 Multiple Script SQL Injection | High Severity problem(s) found |
| 25116 | 1 | myGallery mygallerybrowser.php myPath Parameter Remote File Inclusion | High Severity problem(s) found |
| 48927 | 1 | CGI Generic SQL Injection Detection (potential, 2nd order, 2nd pass) | High Severity problem(s) found |
| 51973 | 1 | CGI Generic SQL Injection (Parameters Names) | High Severity problem(s) found |
| 42427 | 1 | CGI Generic SQL Injection (HTTP Headers) | High Severity problem(s) found |
| 42479 | 1 | CGI Generic SQL Injection (2nd pass) | High Severity problem(s) found |
| 11139 | 1 | CGI Generic SQL Injection | High Severity problem(s) found |
| 44967 | 1 | CGI Generic Command Execution (time-based) | High Severity problem(s) found |
| 55976 | 1 | Apache HTTP Server Byte Range DoS | High Severity problem(s) found |
| 33821 | 2 | .svn/entries Disclosed via Web Server | Medium Severity problem(s) found |
| 34844 | 1 | WordPress Trackback Check & Reading SQL Injection | Medium Severity problem(s) found |

HTML Executive Report



Executive Summary:

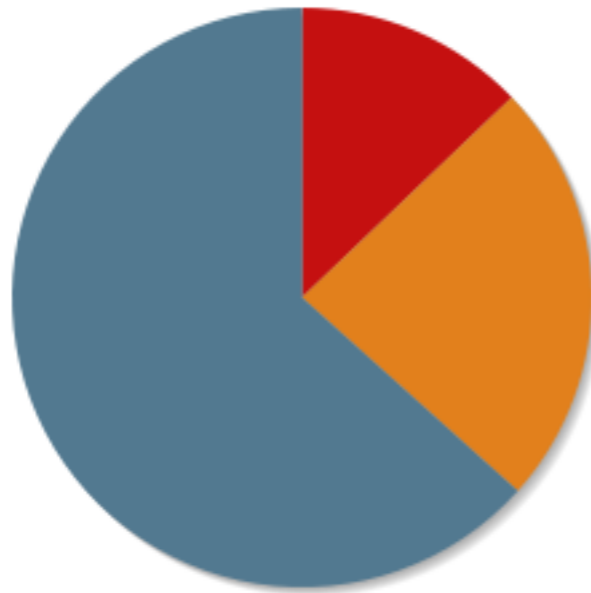
[>PRINT](#)

TOP 10 HOSTS with ISSUES

[192.168.206.134](#)

High Severity problem(s) found

- 12% High Severity
- 23% Medium Severity
- 63% Low Severity



PLUGIN IDS ISSUES

| | |
|-----------------------|---|
| 47863 | 2 |
| 10107 | 2 |
| 26194 | 2 |
| 52973 | 2 |
| 42057 | 2 |
| 14772 | 2 |
| 43111 | 2 |
| 33817 | 2 |
| 40665 | 2 |
| 24260 | 2 |
| 10662 | 2 |
| 40406 | 2 |
| 33821 | 2 |
| 34850 | 2 |
| 39521 | 2 |
| 39463 | 2 |
| 39470 | 2 |
| 44020 | 2 |

| PLUGIN IDS | SEVERITY | # OF ISSUES | SYNOPSIS |
|------------|----------|-------------|---|
| 42479 | High | 1 | CGI Generic SQL Injection (2nd pass) A web application is potentially vulnerable to SQL injection. |
| 13655 | High | 1 | phpBB < 2.0.9 Multiple Vulnerabilities A remote web application is vulnerable to SQL injection. myGallery mygallerybrowser.php myPath Parameter |

HTML Custom Report

Report: 192.168.206.134 Basic

Scan Time:

Start Time: Sun Jan 22 01:55:09 2012

End Time: Sun Jan 22 18:26:19 2012

List of Hosts

| | Severity of Problems Found | PCI Compliance | PCI Failing | High Vul. | Medium Vul. | Low Vul. | Open Ports |
|---|----------------------------|----------------------|-------------|-----------|-------------|----------|------------|
| 192.168.206.134 OWASPBWA | High | Fail | 37 | 13 | 24 | 64 | 4 |
| 192.168.206.134 Basic Totals | | 1 of 1 IPs Failed | 37 | 13 | 24 | 64 | 4 |

Information about the Scan

- The Low Vul. Category includes informational items that may or may not be vulnerabilities; these in some cases require manual checking.
- The PCI Failing column is the sum of the following:
 - High Vul.
 - Medium Vul.

RTF Report

NESSUS REPORT

List of Plugin IDs

The following plugin IDs have problems associated with them. Select the ID to review more detail.

| PLUGIN ID# | # | PLUGIN NAME | SEVERITY |
|------------|---|--|--------------------------------|
| 55976 | 1 | Apache HTTP Server Byte Range DoS | High Severity problem(s) found |
| 51973 | 1 | CGI Generic SQL Injection (Parameters Names) | High Severity problem(s) found |
| 48927 | 1 | CGI Generic SQL Injection Detection (potential, 2nd order, 2nd pass) | High Severity problem(s) found |
| 44967 | 1 | CGI Generic Command Execution (time-based) | High Severity problem(s) found |
| 42479 | 1 | CGI Generic SQL Injection (2nd pass) | High Severity problem(s) found |
| 42427 | 1 | CGI Generic SQL Injection (HTTP Headers) | High Severity problem(s) found |
| 26068 | 1 | TikiWiki tiki-graph_formula.php f Parameter Arbitrary Command | High Severity problem(s) |

.nessus Export

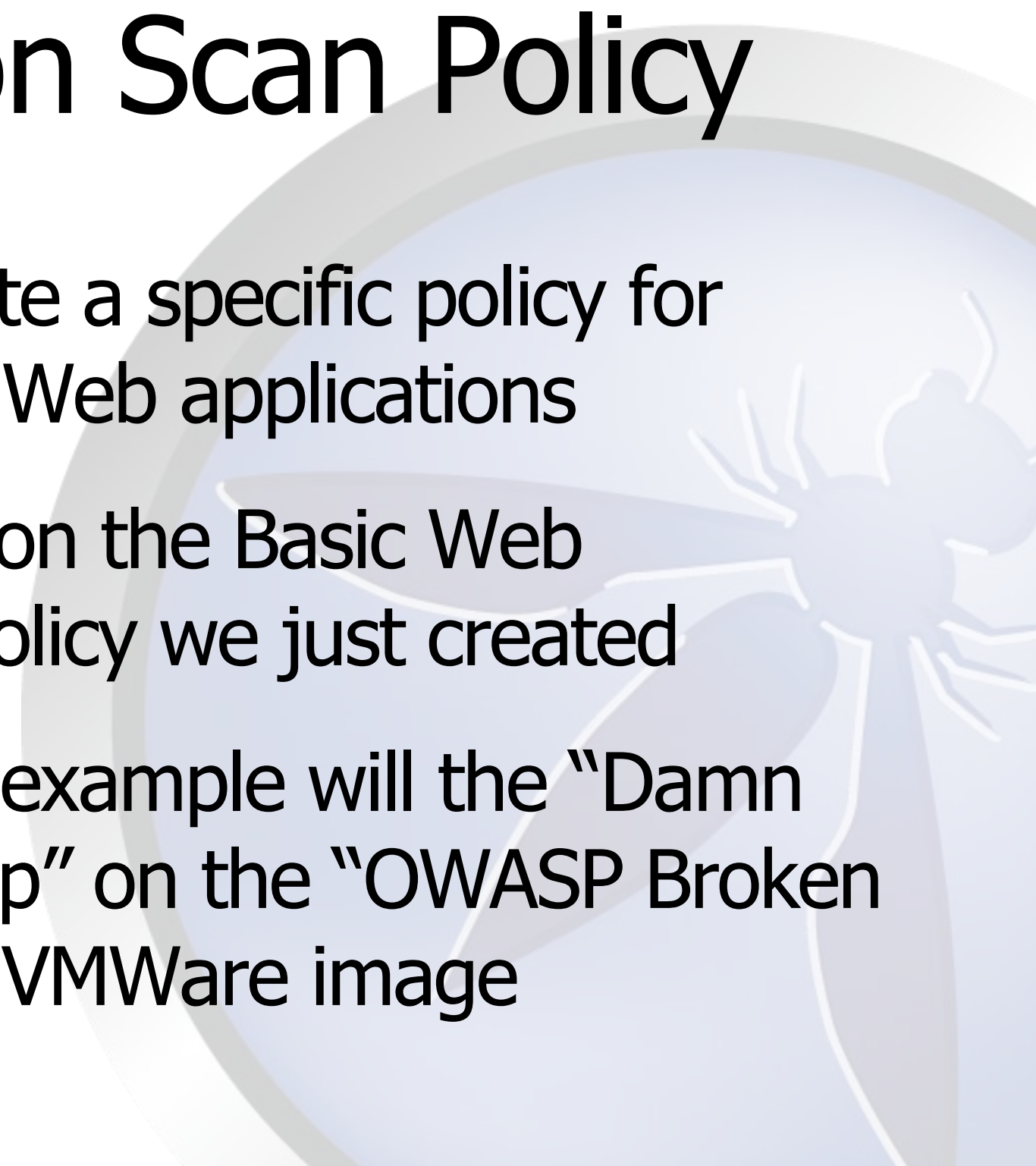
```
<?xml version="1.0" ?>
<NessusClientData_v2>
<Policy>
<policyName>Basic Web App Tests</policyName>
<policyComments></policyComments>
<Preferences>
<ServerPreferences>
<preference>
<name>max_simult_tcp_sessions</name>
<value>unlimited</value>
</preference>
<preference>
<name>use_mac_addr</name>
<value>no</value>
</preference>
<preference>
<name>plugin_set</name>
<value>17803;38808;44943;16058;39500;14325;10702;10777;40886;24698;17312;11769;11234;11985;10569;10447;10830;36088
value>
</preference>
<preference>
<name>TARGET</name>
<value>192.168.206.134</value>
</preference>
<preference>
<name>throttle_scan</name>
<value>yes</value>
</preference>
<preference>
```


.nessus v1 Export

```
<?xml version="1.0" ?>
<NessusClientData>
<Targets>
<Target>
<selected>yes</selected>
<type>hostname</type>
<value>192.168.206.134</value></Target>
</Targets>
<Policies>
<Policy>
<policyName>Basic Web App Tests</policyName>
<policyComments></policyComments>
<Preferences>
<ServerPreferences>
<preference>
<name>max_simult_tcp_sessions</name>
<value>unlimited</value>
</preference>
<preference>
<name>use_mac_addr</name>
<value>no</value>
</preference>
<preference>
<name>plugin_set</name>
<value>17803;38808;44943;16058;39500;14325;10702;10777;40886;24698;17312;11769;11234;11985;10569;10447;10830;36088
value>
</preference>
<preference>
<name>TARGET</name>
```



Creating an Advanced Web Application Scan Policy

- ❖ The goal is to create a specific policy for scanning a known Web applications
 - ❖ This will be based on the Basic Web Application Scan Policy we just created
 - ❖ Our target for this example will be the “Damn Venerable Web App” on the “OWASP Broken Web Applications” VMWare image
- 

Creating an Advanced Web Application Scan Policy

Step 1: Go to the Policies Tab and select the Basic Web Applications policy you just created



The screenshot displays the 'Policies' tab in a web application security tool. The interface includes a navigation bar with tabs for 'Reports', 'Scans', 'Policies', and 'Users'. Below the navigation bar, there are action buttons: 'Add', 'Import', 'Export', 'Copy', 'Edit', and a minus sign. The main content area is a table with the following data:

| Name | Visibility | Owner |
|-----------------------------|------------|-------------------------------------|
| Basic Web App Tests | Shared | demo |
| DVWA Advanced Web App Tests | Shared | demo |
| External Network Scan | Shared | Tenable Policy Distribution Service |
| Internal Network Scan | Shared | Tenable Policy Distribution Service |
| My Basic Web App Tests | Shared | demo |
| Prepare for PCI DSS audits | Shared | Tenable Policy Distribution Service |
| Web App Tests | Shared | Tenable Policy Distribution Service |

Creating an Advanced Web Application Scan Policy

Step 2: Click on the "Copy" button. This will create a new Policy called "Copy of ..."



The screenshot shows a web application security tool interface. At the top, there are tabs for 'Policies', 'Reports', 'Scans', 'Policies', and 'Users'. Below the tabs is a toolbar with buttons for 'Add', 'Import', 'Export', 'Copy', and a minus sign. A red arrow points to the 'Copy' button. Below the toolbar is a table with three columns: 'Name', 'Visibility', and 'Owner'.

| Name | Visibility | Owner |
|-----------------------------|------------|-------------------------------------|
| Basic Web App Tests | Shared | demo |
| DVWA Advanced Web App Tests | Shared | demo |
| External Network Scan | Shared | Tenable Policy Distribution Service |
| Internal Network Scan | Shared | Tenable Policy Distribution Service |
| My Basic Web App Tests | Shared | demo |
| Prepare for PCI DSS audits | Shared | Tenable Policy Distribution Service |
| Web App Tests | Shared | Tenable Policy Distribution Service |

Creating an Advanced Web Application Scan Policy

Step 3: Select the new policy "Copy of ..."



The screenshot shows a web application security tool interface with a 'Policies' tab selected. The interface includes a navigation bar with 'Reports', 'Scans', 'Policies', and 'Users' tabs. Below the navigation bar is a toolbar with buttons for 'Add', 'Import', 'Export', 'Copy', 'Edit', and a minus sign. The main area displays a table of policies with columns for Name, Visibility, and Owner. A red arrow points to the row 'Copy of My Basic Web App Tests'.

| Name | Visibility | Owner |
|--------------------------------|------------|-------------------------------------|
| Basic Web App Tests | Shared | demo |
| Copy of My Basic Web App Tests | Shared | demo |
| DVWA Advanced Web App Tests | Shared | demo |
| External Network Scan | Shared | Tenable Policy Distribution Service |
| Internal Network Scan | Shared | Tenable Policy Distribution Service |
| My Basic Web App Tests | Shared | demo |
| Prepare for PCI DSS audits | Shared | Tenable Policy Distribution Service |
| Web App Tests | Shared | Tenable Policy Distribution Service |

Creating an Advanced Web Application Scan Policy

Step 4: Click on the Edit Button



The screenshot shows a web application security tool interface. At the top, there are tabs for 'Policies', 'Reports', 'Scans', 'Policies', and 'Users'. Below the tabs is a toolbar with buttons for 'Add', 'Import', 'Export', 'Copy', and 'Edit'. A red arrow points to the 'Edit' button. Below the toolbar is a table with the following columns: Name, Visibility, and Owner.

| Name | Visibility | Owner |
|--------------------------------|------------|-------------------------------------|
| Basic Web App Tests | Shared | demo |
| Copy of My Basic Web App Tests | Shared | demo |
| DVWA Advanced Web App Tests | Shared | demo |
| External Network Scan | Shared | Tenable Policy Distribution Service |
| Internal Network Scan | Shared | Tenable Policy Distribution Service |
| My Basic Web App Tests | Shared | demo |
| Prepare for PCI DSS audits | Shared | Tenable Policy Distribution Service |
| Web App Tests | Shared | Tenable Policy Distribution Service |

Creating an Advanced Web Application Scan Policy

This will open the Edit Policy screen

Edit Policy

General

Credentials

Plugins

Preferences

Basic

Name: Copy of My Basic Web App Tests

Visibility: Shared

Description:

Scan

Save Knowledge Base

Safe Checks

Silent Dependencies

Log Scan Details to Server

Stop Host Scan on Disconnect

Avoid Sequential Scans

Consider Unscanned Ports as Closed

Designate Hosts by their DNS Name

Network Congestion

Reduce Parallel Connections on Congestion

Use Kernel Congestion Detection (Linux Only)

Port Scanners

TCP Scan SNMP Scan Ping Host

UDP Scan Netstat SSH Scan

SYN Scan Netstat WMI Scan

Port Scan Options

Port Scan Range: default

Performance

Max Checks Per Host: 5

Max Hosts Per Scan: 80

Network Receive Timeout (seconds): 5

Max Simultaneous TCP Sessions Per Host: unlimited

Max Simultaneous TCP Sessions Per Scan: unlimited

Cancel Submit

Creating an Advanced Web Application Scan Policy

Step 5: Change the policy name

Basic

| | |
|-------------|--|
| Name | <input type="text" value="My DVWA Web App Tests"/> ← |
| Visibility | Private ▼ |
| Description | <input type="text"/> |

Creating an Advanced Web Application Scan Policy

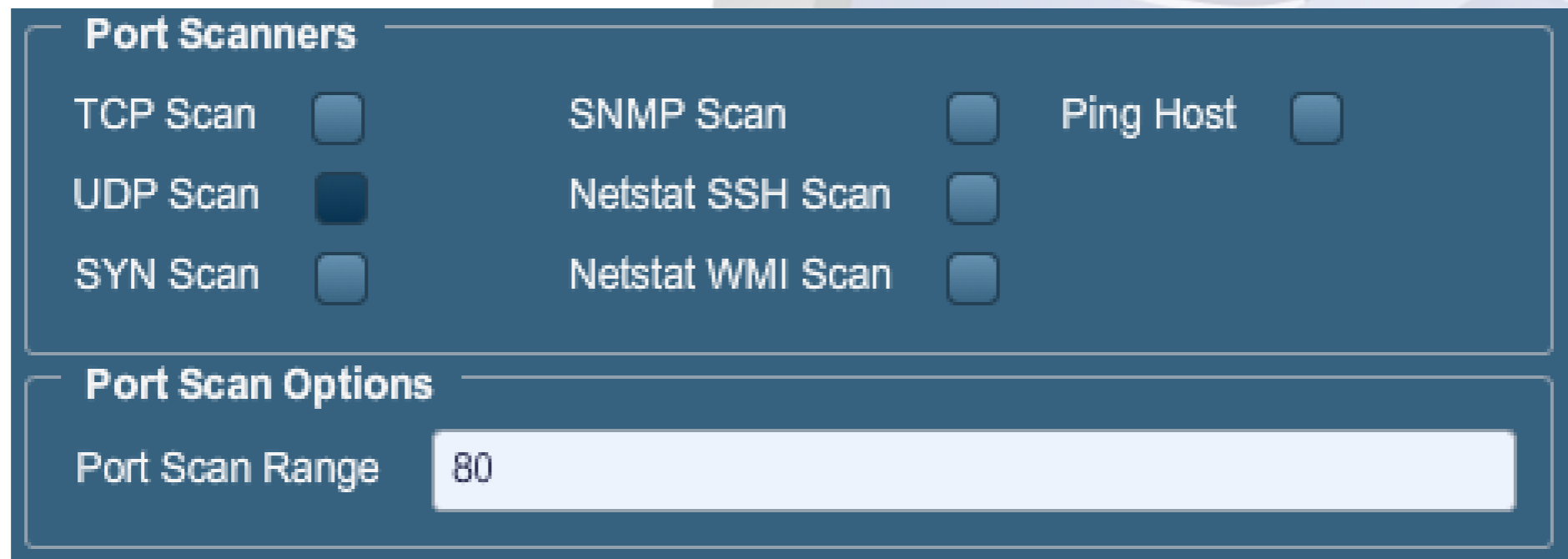
Step 6: Change the Visibility to Private

Basic

| | |
|-------------|--|
| Name | <input type="text" value="My DVWA Web App Tests"/> |
| Visibility | <input type="text" value="Private"/>  |
| Description | <input type="text"/> |

Creating an Advanced Web Application Scan Policy

Step 6: Uncheck all port scanners. We know what port we want



The screenshot shows a configuration window with two sections: 'Port Scanners' and 'Port Scan Options'. In the 'Port Scanners' section, the 'UDP Scan' checkbox is checked, while all other checkboxes (TCP Scan, SYN Scan, SNMP Scan, Netstat SSH Scan, Netstat WMI Scan, and Ping Host) are unchecked. In the 'Port Scan Options' section, the 'Port Scan Range' is set to '80'.

| Port Scanners | | |
|------------------|-------------------------------------|--|
| TCP Scan | <input type="checkbox"/> | |
| UDP Scan | <input checked="" type="checkbox"/> | |
| SYN Scan | <input type="checkbox"/> | |
| SNMP Scan | <input type="checkbox"/> | |
| Netstat SSH Scan | <input type="checkbox"/> | |
| Netstat WMI Scan | <input type="checkbox"/> | |
| Ping Host | <input type="checkbox"/> | |

| Port Scan Options | |
|-------------------|----|
| Port Scan Range | 80 |

Creating an Advanced Web Application Scan Policy

Step 7: Set the "Port Scan Range" to only the ports the target Web application is using. In our example we are running on port 80

Port Scanners

| | | | | | |
|----------|-------------------------------------|------------------|--------------------------|-----------|--------------------------|
| TCP Scan | <input type="checkbox"/> | SNMP Scan | <input type="checkbox"/> | Ping Host | <input type="checkbox"/> |
| UDP Scan | <input checked="" type="checkbox"/> | Netstat SSH Scan | <input type="checkbox"/> | | |
| SYN Scan | <input type="checkbox"/> | Netstat WMI Scan | <input type="checkbox"/> | | |

Port Scan Options

Port Scan Range ←

Creating an Advanced Web Application Scan Policy

Step 8: Select "HTTP login page" from the Plugin pull down menu



Creating an Advanced Web Application Scan Policy

We will need to do some reconnaissance to get the values for these fields.

| | |
|---------------------|--|
| Login page : | <input type="text" value="/"/> |
| Login form : | <input type="text"/> |
| Login form fields : | <input type="text" value="user=%USER%&pass=%PASS%"/> |
| Login form method : | <input type="text" value="POST"/> |

Creating an Advanced Web Application Scan Policy

Step 9: Find the Login Screen

`/dvwa/login.php`



Creating an Advanced Web Application Scan Policy

Step 10: Enter the Login page path (not the full URL)

| | |
|---------------------|--|
| Login page : | <input type="text" value="/dwwa/login.php"/> ← |
| Login form : | <input type="text"/> |
| Login form fields : | <input type="text" value="user=%USER%&pass=%PASS%"/> |
| Login form method : | <input type="text" value="POST"/> |

Creating an Advanced Web Application Scan Policy

Step 11: View source on the login page to find the "Login Form" (action) and "Login Form Method"

```
<form method="post" action="login.php">  
  <fieldset>  
    <label for="user">Username </label>  
    <input class="loginInput" type="text" name="username" size="20">  
    <br>  
    <label for="pass">Password </label>  
    <input class="loginInput" type="password" name="password" size="20" autocomplete="off">  
    <br>  
    <p class="submit">  
      <input type="submit" name="Login" value="Login">  
    </p>  
  </fieldset>  
</form>
```


Creating an Advanced Web Application Scan Policy

Step 12: Enter the "Login form" path (not full URL) based on the "action" attribute of the form

| | |
|---------------------|--|
| Login page : | <input type="text" value="/dwa/login.php"/> |
| Login form : | <input type="text" value="/dwa/login.php"/> ← |
| Login form fields : | <input type="text" value="user=%USER%&pass=%PASS%"/> |
| Login form method : | <input type="text" value="POST"/> |

Creating an Advanced Web Application Scan Policy

Step 13: Enter the "Login form method" based on the "method" attribute of the form

| | |
|---------------------|--|
| Login page : | <input type="text" value="/dwa/login.php"/> |
| Login form : | <input type="text" value="/dwa/login.php"/> |
| Login form fields : | <input type="text" value="user=%USER%&pass=%PASS%"/> |
| Login form method : | <input type="text" value="POST"/> ← |

Creating an Advanced Web Application Scan Policy

Step 14: Determine the "Login form fields" and values by trapping the login with tamper data or a Web proxy

| | |
|----------------|---|
| Referer | http://192.168.206.134/dvwa/login.php |
| Cookie | security=high; PHPSESSID=dq3thqopdjvljie5nfibhg5i3... |
| Content-Type | application/x-www-form-urlencoded |
| Content-Length | 41 |
| POSTDATA | username=admin&password=admin&Login=Login |

Creating an Advanced Web Application Scan Policy

Step 15: Enter the "Login from fields"
Substitute %USER% for the user name
Substitute %PASS% for the password

| | |
|---------------------|--|
| Login page : | <input type="text" value="/dwa/login.php"/> |
| Login form : | <input type="text" value="/dwa/login.php"/> |
| Login form fields : | <input type="text" value="username=%USER%&password=%PASS%&Login=Login"/> |
| Login form method : | <input type="text" value="POST"/> |

Creating an Advanced Web Application Scan Policy

Step 16: Uncheck "Automated login page search" since we have told Nessus where the login form is located



Creating an Advanced Web Application Scan Policy

Step 17: Find criteria to confirm login

- Authenticated page path
- Text in the page HTML



http://192.168.206.134/dvwa/index.php

you have logge

Logout

```
<ul>  
  <li class="" onclick="window.location='logout.php'">  
    <a href="logout.php">Logout  
  </li>  
</ul>
```

Creating an Advanced Web Application Scan Policy

Step 18: Enter the "Check authentication on page" path

| | |
|---|--|
| Check authentication on page : | <input type="text" value="/dwwa/index.php"/> ← |
| Follow 30x redirections (# of levels) : | <input type="text" value="2"/> |
| Authenticated regex : | <input type="text" value="[L]ogout"/> |

Creating an Advanced Web Application Scan Policy

Step 19: Enter the "Authentication regex."
This pattern allows the "L" to be case insensitive

| | |
|---|--|
| Check authentication on page : | <input type="text" value="/dwwa/index.php"/> |
| Follow 30x redirections (# of levels) : | <input type="text" value="2"/> |
| Authenticated regex : | <input type="text" value="[L]ogout"/> ← |

Creating an Advanced Web Application Scan Policy

Step 20: Select “Web Application Test Settings” from the Plugin pull down menu



Creating an Advanced Web Application Scan Policy

Step 21: Increase the “Maximum run time” value. Remember that the Basic Policy timed out.

Maximum run time (min) : ←

Creating an Advanced Web Application Scan Policy

Step 22: Select "Web mirroring" from the Plugin pull down menu



Creating an Advanced Web Application Scan Policy

Step 23: Set the Start page to go to the target Web Application

| | |
|-----------------------------|---|
| Number of pages to mirror : | <input type="text" value="1000"/> |
| Maximum depth : | <input type="text" value="6"/> |
| Start page : | <input type="text" value="/dvwa/login.php"/> ← |
| Excluded items regex : | <input type="text" value="logout\.php /phpmyadmin /WebGoat /ghost/"/> |
| Follow dynamic pages : | <input checked="" type="checkbox"/> |

Creating an Advanced Web Application Scan Policy

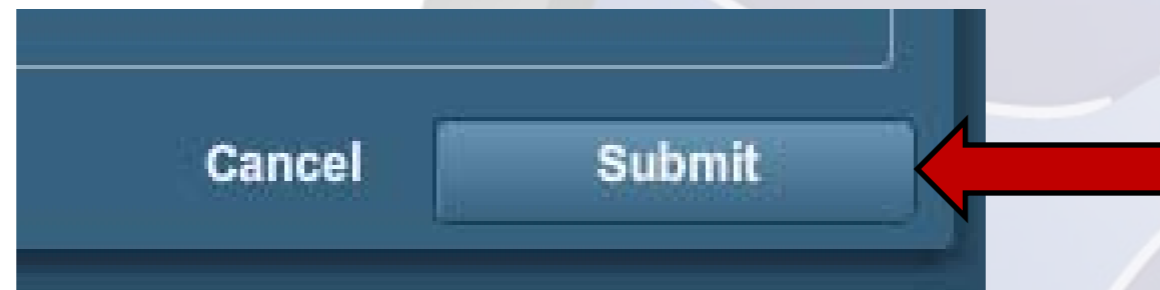
Step 24: Set the "Exclude Items regex" to avoid logging out or going to places that we don't want to test.

| | |
|-----------------------------|---|
| Number of pages to mirror : | <input type="text" value="1000"/> |
| Maximum depth : | <input type="text" value="6"/> |
| Start page : | <input type="text" value="/dvwa/login.php"/> |
| Excluded items regex : | <input type="text" value="logout\.php /phpmyadmin /WebGoat /ghost/"/> |
| Follow dynamic pages : | <input checked="" type="checkbox"/> |



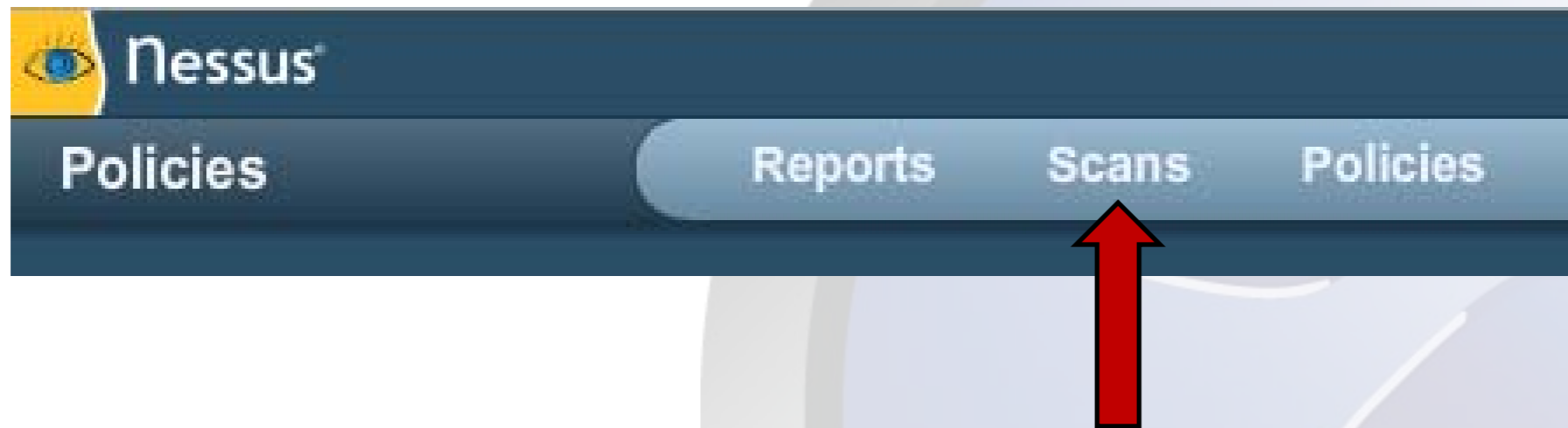
Creating an Advanced Web Application Scan Policy

Step 25: Click on the Submit Button in lower right corner to save your policy



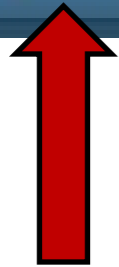
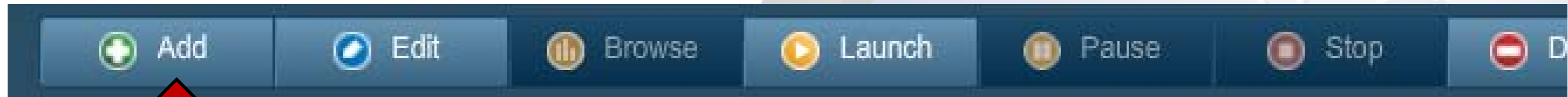
Create Advanced Scan Template

Step 1: Click on the "Scan" tab on the top



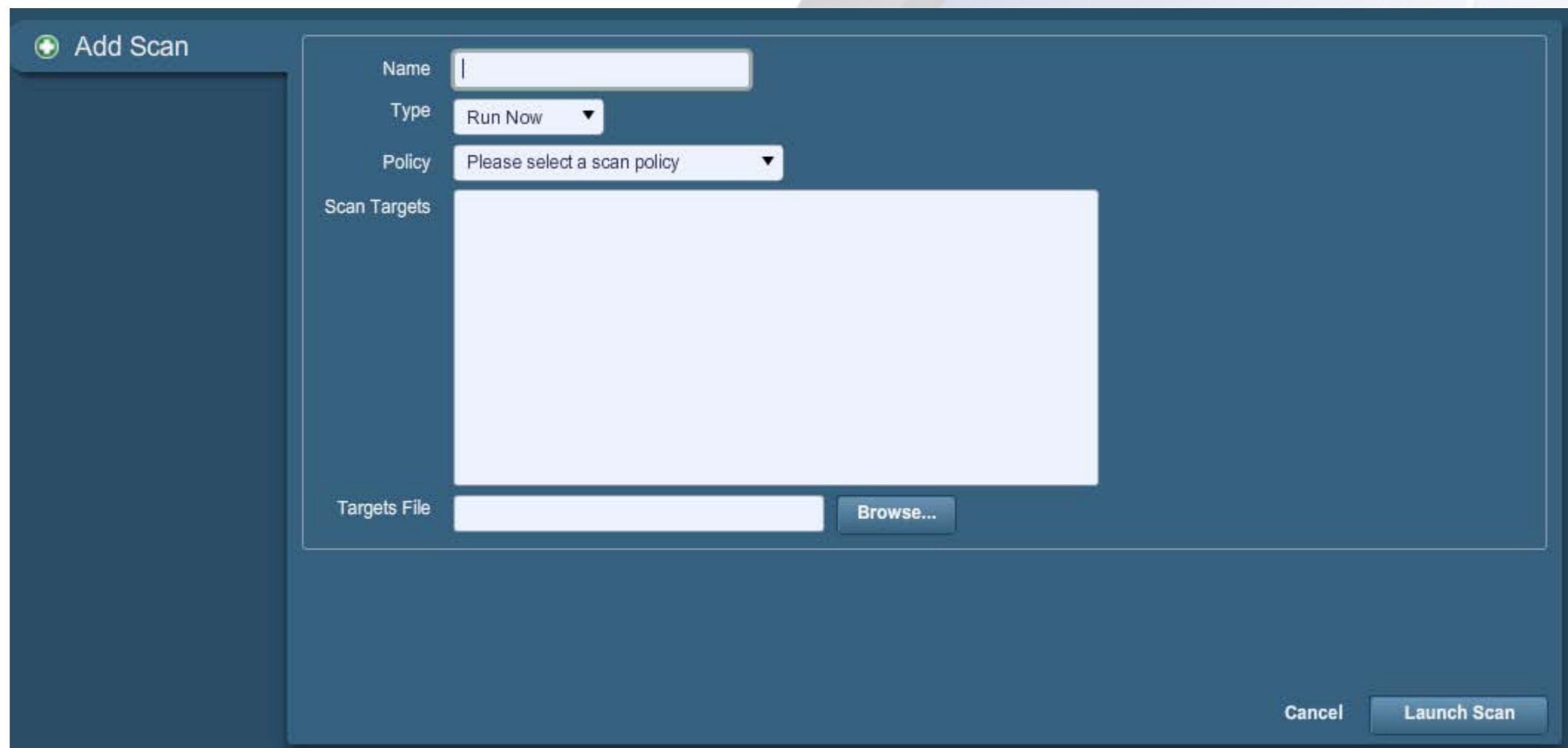
Create Advanced Scan Template

Step 2: Click on the "Add" button



Create Advanced Scan Template

This should take you to the interface to create a new scan.



The screenshot shows a dialog box titled "Add Scan" with a green plus icon. The dialog contains the following fields and controls:

- Name:** A text input field.
- Type:** A dropdown menu with "Run Now" selected.
- Policy:** A dropdown menu with "Please select a scan policy" selected.
- Scan Targets:** A large, empty text area.
- Targets File:** A text input field with a "Browse..." button next to it.
- Buttons:** "Cancel" and "Launch Scan" buttons are located at the bottom right of the dialog.

Create Advanced Scan Template

Step 3: Name the Scan

| | |
|--------------|---|
| Name | <input type="text" value="My DVWA Web App Scan"/> ← |
| Type | Template ▾ |
| Policy | My DVWA Web App Tests ▾ |
| Scan Targets | 192.168.206.134 |


Create Advanced Scan Template

Step 4: Set the scan Type to "Template"

| | |
|--------------|--|
| Name | <input type="text" value="My DVWA Web App Scan"/> |
| Type | <input type="text" value="Template"/> ← |
| Policy | <input type="text" value="My DVWA Web App Tests"/> |
| Scan Targets | 192.168.206.134 |

Create Advanced Scan Template

Step 5: Select the Advanced Web App policy you just created

| | |
|--------------|--|
| Name | <input type="text" value="My DVWA Web App Scan"/> |
| Type | <input type="text" value="Template"/> |
| Policy | <input type="text" value="My DVWA Web App Tests"/>  |
| Scan Targets | <input type="text" value="192.168.206.134"/> |

Create Advanced Scan Template

Step 6: Enter your scan target IP, domain name or network range



The screenshot shows a configuration form with the following fields:

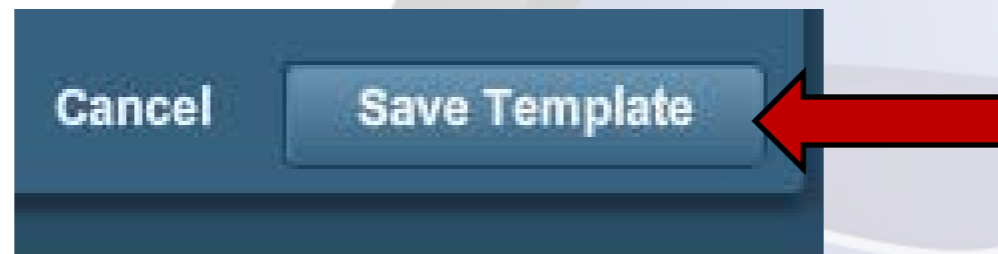
| | |
|--------------|-----------------------|
| Name | My DVWA Web App Scan |
| Type | Template |
| Policy | My DVWA Web App Tests |
| Scan Targets | 192.168.206.134 |

A red arrow points to the IP address in the Scan Targets field.

- single IP address or comma separated list (e.g., 192.168.0.1,192.168.206.134)
- IP range (e.g., 192.168.0.1-192.168.0.255)
- subnet with CIDR notation (e.g., 192.168.0.0/24)
- or resolvable host (e.g., www.nessus.org).

Create Advanced Scan Template

Step 7: Click on the "Save Template" button to save your scan template



Advanced Scan Demo

The screenshot shows a Mozilla Firefox browser window displaying the Nessus web interface. The browser's address bar shows the URL `https://127.0.0.1:8834/`. The Nessus interface includes a navigation menu with 'Policies', 'Reports', 'Scans', and 'Users'. Below the menu is a toolbar with buttons for 'Add', 'Import', 'Export', 'Copy', 'Edit', and 'Delete'. The main content area displays a table of policies.

| Name | Visibility | Owner |
|-----------------------------|------------|-------------------------------------|
| Basic Web App Tests 2 | Shared | demo |
| DVWA Advanced Web App Tests | Shared | demo |
| External Network Scan | Shared | Tenable Policy Distribution Service |
| Internal Network Scan | Shared | Tenable Policy Distribution Service |
| My Basic Web App Tests | Shared | demo |
| My Basic Web App Tests 1 | Shared | demo |
| My Basic Web App Tests 3 | Shared | demo |
| My DVWA Web App Tests 1 | Private | demo |
| My DVWA Web App Tests 2 | Private | demo |
| Prepare for PCI DSS audits | Shared | Tenable Policy Distribution Service |
| Web App Tests | Shared | Tenable Policy Distribution Service |

Reviewing the Report for OWASP Top Items

A1 – Injection

- SQL Injection (CGI abuses) > 11139, 42424, 42426, 42427, 42479, 43160, 51973
- XML Injection (CGI abuses) > 46196
- HTTP Header Injection (CGI abuses: XSS) > 39468, 49067
- Cookie Injection > 44135 (CGI abuses)

A2 – Cross-Site Scripting (XSS)

- Cross-Site Scripting (CGI abuses: XSS) > 10815, 39466, 42425, 47831, 46193, 49067, 51972

A3 – Broken Authentication and Session Management

- Authentication not over SSL > 26194, 34850
- Is SSL Implement Properly > 15901, 20007, 26928, 35291, 42053, 42873, 42880, 53491, 53360, 56043, 56284, 56984, 57041

Reviewing the Report for OWASP Top Items Cont.

A4 –Insecure Direct Object References

- Browsable Web Directories > 40984
- Path Transversal (CGI abuses)> 50494
- Parameters identified for manual testing > 40773, 44134, 47830 *

A5 –Cross-Site Request Forgery (CSRF)

- CGI Generic On Site Request Forgery (OSRF) > 47832
- Specific Product checks with known CSRF Vulnerabilities

A6 –Security Misconfiguration

- Covered by Nessus Audit Checks in the ProfessionFeed
- Identifies Open ports and services for manual review
- Many checks for default accounts and passwords

Reviewing the Report for OWASP Top Items Cont.

A9 –Insufficient Transport Layer Protection

- Authentication not over SSL > 26194, 34850
- Is SSL Implement Properly > 15901, 20007, 26928, 35291, 42053, 42873 , 42880, 53491, 53360, 56043, 56284, 56984, 57041
- Secure Cookie Use > 49218, 84832

A10 –Unvalidated Redirects and Forwards

- CGI Generic Open Redirection > 47834

Reviewing the Report for 2007 OWASP Top Items

2007 A3–Malicious File Execution

- Command Execution (CGI abuses) > 39465, 44967

2007 A6 –Information Leakage and Improper Error Handling

- Directory Traversal (CGI abuses) > 39467, 46195, 46194
- File Inclusion (CGI abuses) > 39469, 42056, 42872
- Server Side Includes (CGI abuses) > 42423, 42054
- Error Messages > 40406, 48926, 48927

Other Nessus CGI checks

- Format String (CGI abuses) > 42055
- Cookie Manipulation (CGI abuses) > 44136
- Additional attacks (CGI abuses) > 44134, 47830, 47832, 47834

Resources

Nessus Website

<http://www.nessus.org/products/nessus>

My Email

rikjones@computer.org

