
Acunetix Web Vulnerability Scanner

Getting Started

V8

By Acunetix Ltd.

Starting a Scan

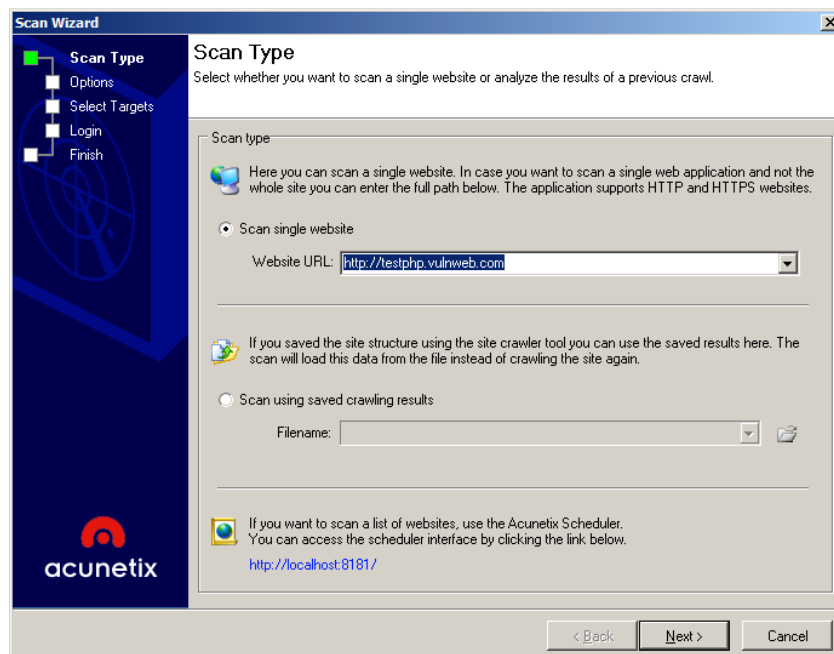
The Scan Wizard allows you to quickly set-up an automated scan of your website. An automated scan provides a comprehensive understanding of the level website security by simply reviewing the individual alerts returned.

This Getting Started guide explains the process of launching a security audit of your website through the Scan wizard.

NOTE: DO NOT SCAN A WEBSITE WITHOUT PROPER AUTHORISATION!

Step 1: Select Target to Scan

1. Click on File > New > New Website Scan to start the Scan Wizard, or click the New Scan button on the top left hand of the Acunetix WVS menu bar.



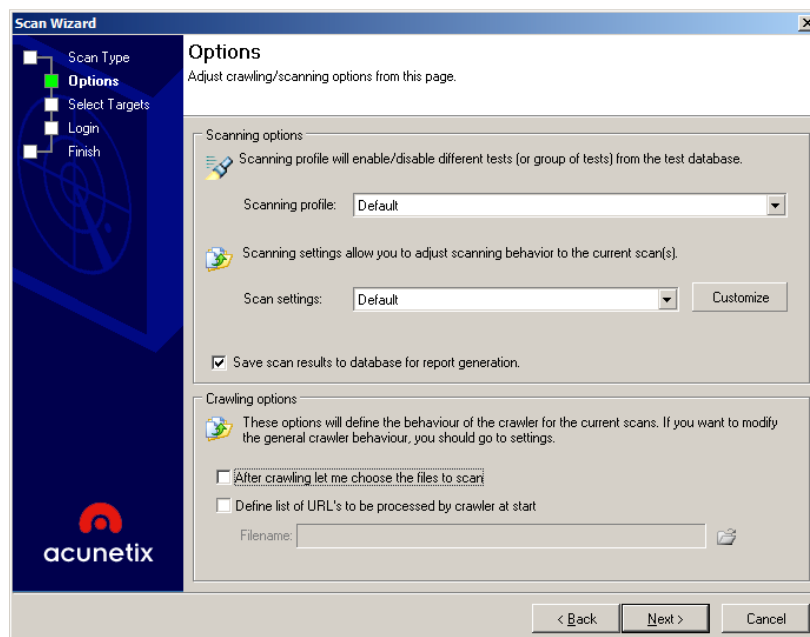
Screenshot 1 – Scan Wizard Select Scan Type

2. Specify the website to be scanned. The scan target options are:

- **Scan single website** - e.g. <http://testphp.vulnweb.com>.
- **Scan using saved crawling results** - If you previously crawled a website, you can use the saved crawl to launch a scan instead of having to crawl the website again.

You can scan multiple websites simultaneously using the **Acunetix WVS Scheduler**. For more information please refer to 'The Scheduler' chapter in the Acunetix WVS user manual.

Step 2: Specify Scanning Profile, Scan Settings Template and Crawling Options



Screenshot 2 – Scanning Profile and Scan Settings template

Scanning Profile

Select a scanning profile (e.g. SQL Injection, XSS) to be launched against the target website. A scanning profile defines which vulnerability checks will be launched against your website. The Default scanning profile will test your website for all known web vulnerabilities. For more information please refer to 'Scanning Profiles' chapter in the Acunetix WVS user manual.

Scan Settings template

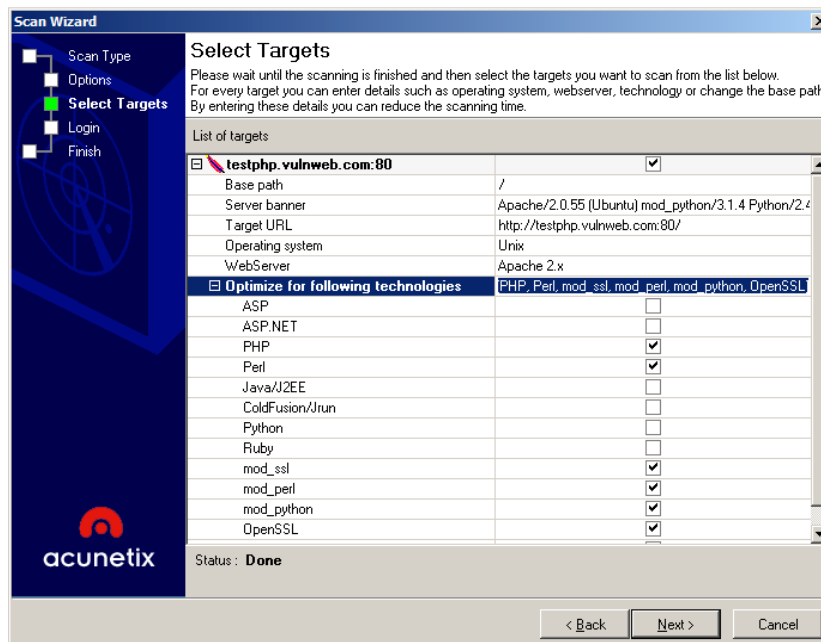
The Scan Settings template will determine what Crawler (HTTP protocol, advanced crawling) and Scanner settings are to be used during a scan. You can customize the scan settings using the 'Customize' button. Any changes made will affect only the current scan. If you wish to save these scan settings configuration, then you can save the template at the Finish section of the Scan Wizard. For more information please refer to Section 'Scan Settings Templates' of the manual.

Crawling Options

If you want to manually select which files and directories should be scanned after crawl, select the **After crawling let me choose which files to scan** option.

If you would like to crawl a specific URL any other, select the **Define list of URLs to be processed by crawler at start** option.

Step 3: Confirm Target and Technologies Detected



Screenshot 3 – Scan Wizard Selecting Targets and Technologies

Acunetix WVS will automatically fingerprint the target website for basic details and automatically detect and determine if a custom 404 error-page is being used. For more information please refer to Section 'Custom 404 Error Pages' of the manual.

The web vulnerability scanner will optimize and reduce the scan time for the selected technologies by reducing the number of tests performed. If you would like to add or remove scans for specific technologies then click on the relevant field and change the settings from the provided check boxes. If a specific web technology is not listed, then that technology is supported but there are no vulnerability tests exclusive to that technology.

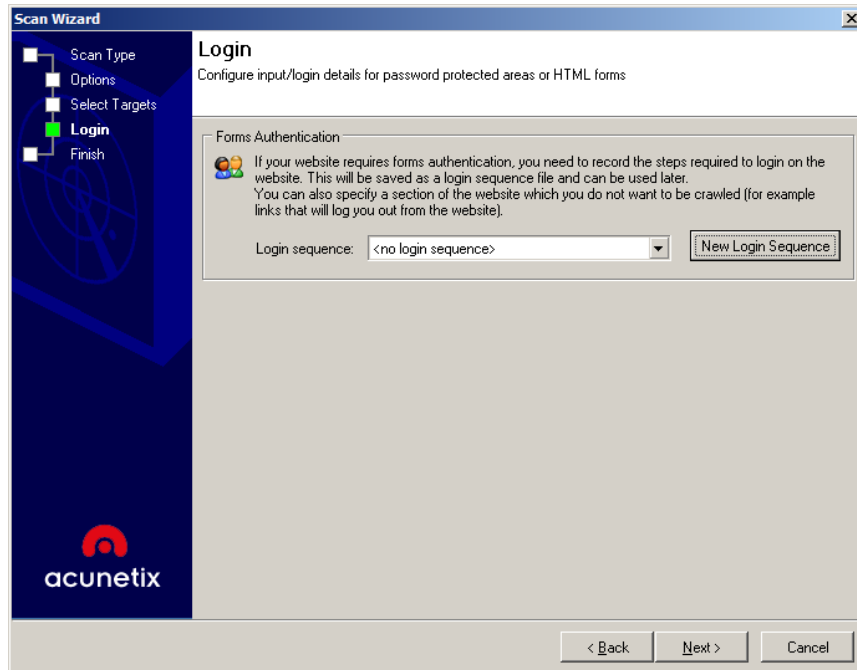
Step 4: Configure Login for Password Protected Areas

HTTP Authentication - This type of authentication is handled by the web server, where the user is prompted with a password dialog.

Scanning a HTTP password protected area:

If you scan an HTTP password protected website, you will be automatically prompted to specify the username and password, unless they are predefined. For more information please refer to Section "Scanning a HTTP password protected area" of the manual.

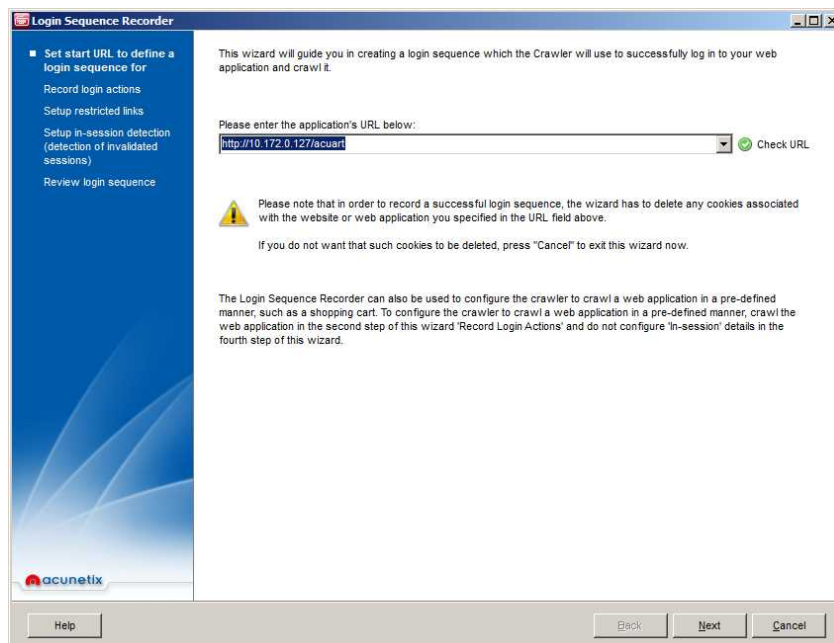
Forms Authentication - This type of authentication is handled via a web form not via HTTP. The credentials are sent to the server for validation by a custom script.



Screenshot 4 - Login Details Options

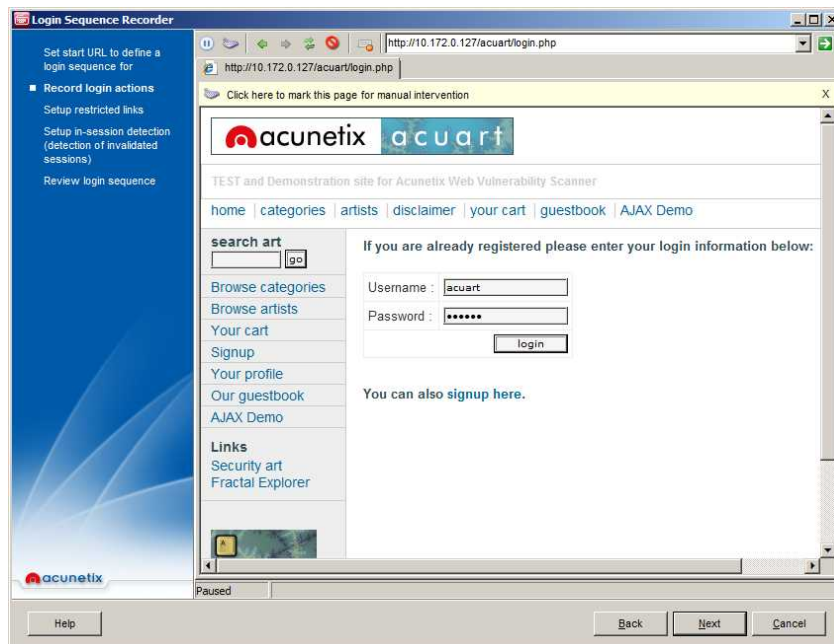
Scanning a form based password protected area:

1. Click New Login Sequence to launch the Login Sequence Recorder



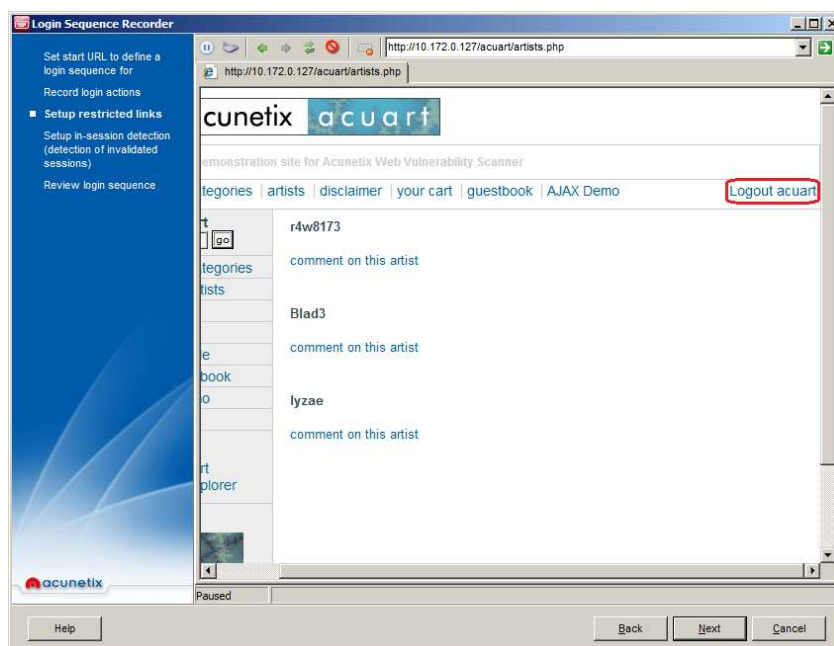
Screenshot 5– Login Sequence Wizard

2. Enter the URL of the website for which you would like to record a login sequence. By default the URL of the target website is automatically populated. Click **Next** to proceed.



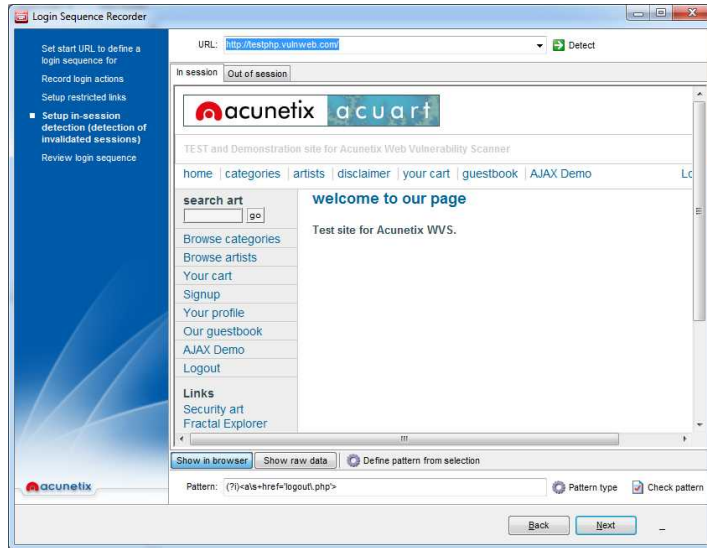
Screenshot 6 – Login Sequence Recorder

3. On the second page of the wizard, browse the website's login page and submit the authentication credentials in the login form in order to log in. Wait for the page to fully load, indicating that you are logged in. Click **Next** to proceed.



Screenshot 7 – Specify an excluded link

4. Once logged in, you also need to identify the logout link so the crawler will ignore it to prevent ending the session. In the 'Setup restricted links' step of the wizard, click the logout link for it to be ignored. If the logout link is not on the same page, click the Pause button in the top menu, navigate to a page where the logout link is found, resume the session and then click on the logout link. Click Next to proceed.



Screenshot 8 – Specify an ‘In session’ or ‘Out of session’ pattern

5. In this step, you have to specify In Session or Out of Session detection patterns. For the In Session detection, specify a pattern which allows the crawler to detect the session is still valid. If the session expires during a crawl, the Crawler will automatically log in again. Click on Detect so Acunetix WVS will try to automatically detect the pattern.

Note: If the automatic detection does not work, you must specify the pattern manually. For more information please refer to “Scanning a HTTP password protected area” section in the Acunetix WVS user manual.



Screenshot 9 – Specify an ‘In session’ or ‘Out of session’ pattern - Drop down menu

6. In the last step of the wizard, you can review the recorded sequence. You can change priority of url’s, edit requests and add or remove requests. Click ‘Finish’ to save the recorded session.

Step 6: Final wizard options

The final step of the scan wizard, includes an overview of the scan options and alerted if further actions are required. Below is a list of all possible options you might be presented with:

- If an error is encountered while connecting to the target server, you will be alerted with the complete details of the error.
- If Acunetix WVS is unable to automatically detect a pattern for the custom 404 error page automatically, you will have to configure a custom 404 error page rule. For more information please refer to the “Custom 404 Error Pages” section in the Acunetix WVS user manual.
- If the target server is using CASE insensitive URLs, you will also be alerted with the option to force case insensitive crawling.
- If AcuSensor Technology is enabled, you will be prompted with the option to configure AcuSensor technology. Click the Customize button to install AcuSensor on the target server. For more information please refer to “Installing the acusensor agent” section in the Acunetix WVS user manual.
- Acunetix WVS will also alert you if additional hosts have been discovered; i.e. other websites which your website links to. By default, Acunetix WVS will not crawl and scan additional hosts / FQDN's which are linked from your website.

Step 7: Completing the scan

Click on Finish to start the automated scan. Depending on the size of the website, scanning profile, and the server response time, a scan may take up to several hours. These factors cannot be controlled by Acunetix WVS.