Acunetix Web Vulnerability Scanner

Getting Started

V9

By Acunetix Ltd.

Starting a Scan

The Scan Wizard allows you to quickly set-up an automated security scan of your website. The security scan provides a comprehensive understanding of the web vulnerabilities present in your website, and gives you the opportunity to review the individual alerts returned.

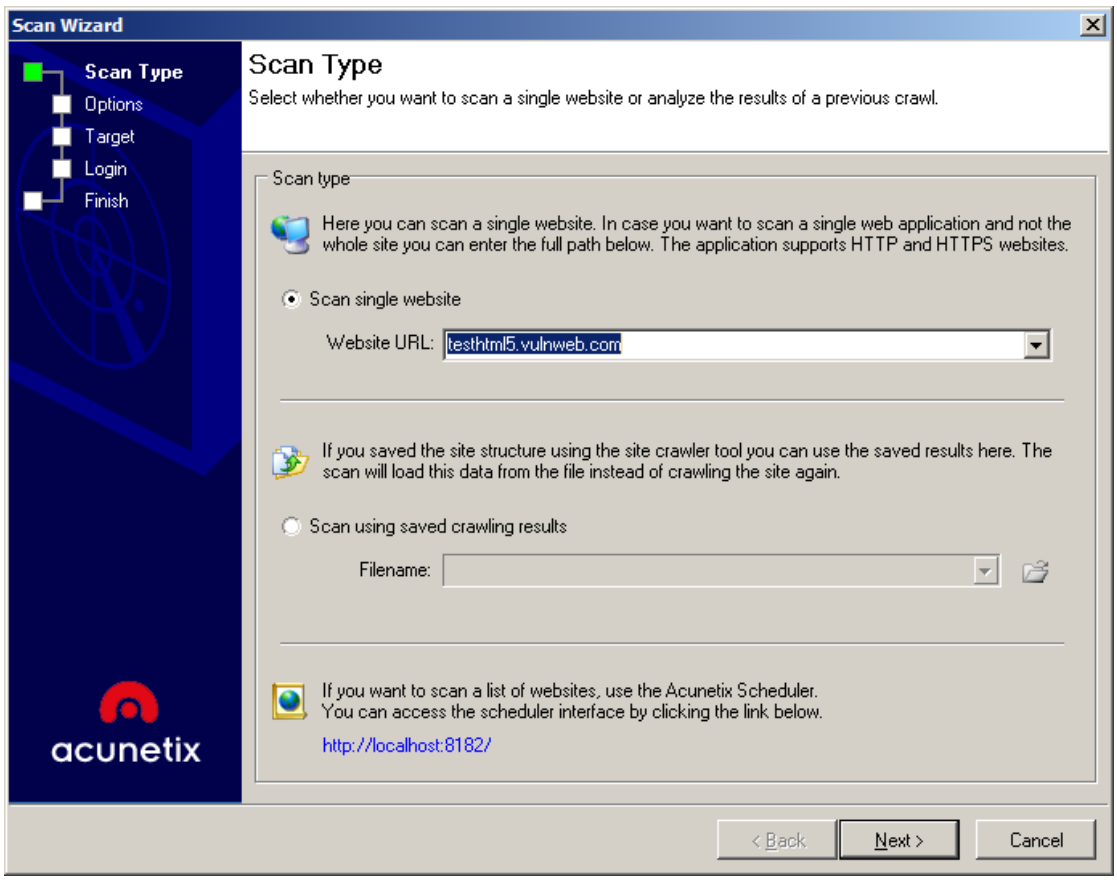
This Getting Started Guide explains the process of launching a security audit of your website through the Scan wizard.

IMPORTANT NOTES:

- DO NOT SCAN A WEBSITE WITHOUT PROPER AUTHORISATION!
- Avoid scanning your main website. Ideally you should scan a test copy of your website as the scan might lead to unexpected behavior of the site.

Step 1: Select Target to Scan

1. Click on 'File > New > Website Scan' to start the Scan Wizard or click on 'New Scan' button from the Acunetix WVS menu bar.



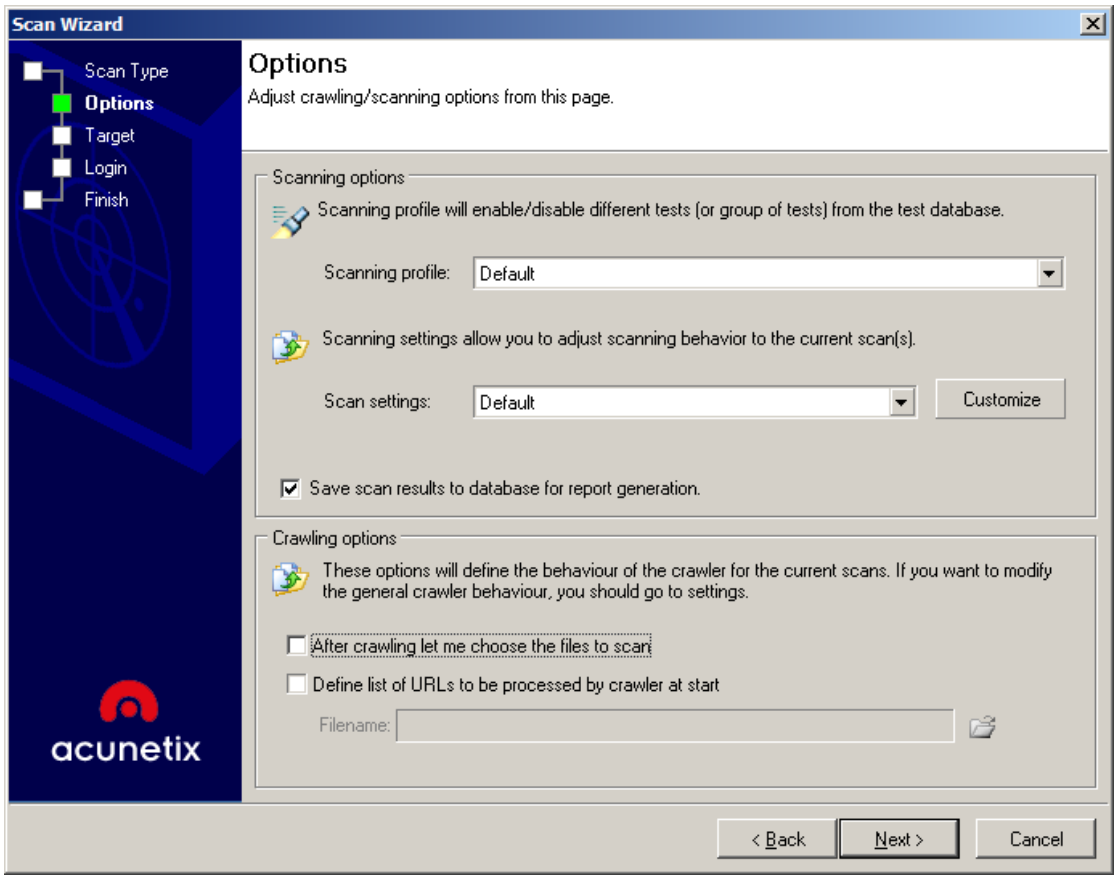
Screenshot 1 – Scan Wizard: Provide Website to Scan

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

- **Scan single website** - e.g. http://testphp.acunetix.com
- **Scan using saved crawling results** - If you previously crawled a website, you 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 – Scan Wizard: Configure Scanning and Crawling options

Scanning Profile

Select a scanning profile (e.g. SQL Injection or XSS) to be used when scanning the target website. A scanning profile defines which vulnerability checks will be launched against your website. The Default scanning file 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

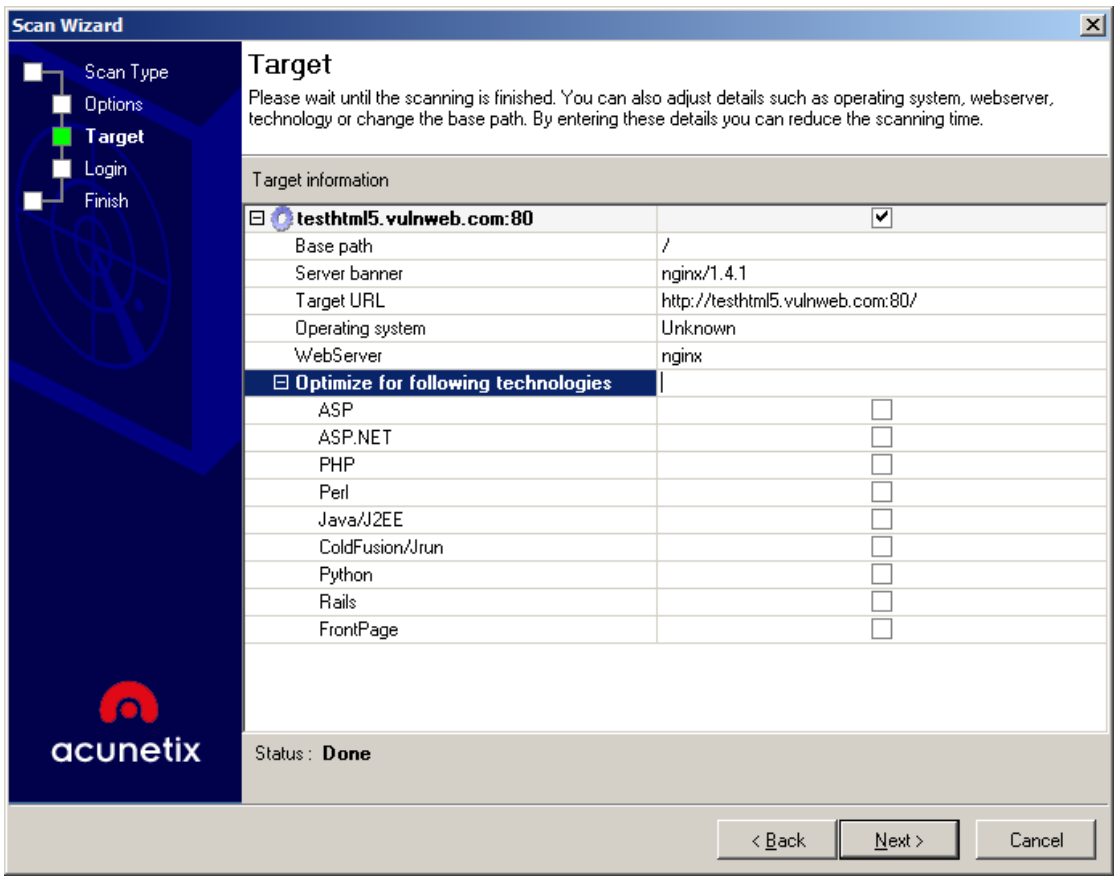
The Scan Settings template will determine what Crawler (HTTP protocol, advanced crawling) and scanner settings to be used during a scan. You can customize the scan settings using the 'Customize' button. Any changes made will affect only the current scan. If you wish to save the changes to be used for future scans, you can select to save the template at the end of the Scan Wizard. For more information, please refer to the 'Scan Settings Template' section in the user manual.

Crawling Options

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

You can also select to have the crawler process URLs which might not be linked from the main URL by using the **Define list of URLs to be processed by crawler at start** option.

Step 3: Confirm Targets and Technologies Detected



Screenshot 3 – Scan Wizard: Confirm Targets and Technologies

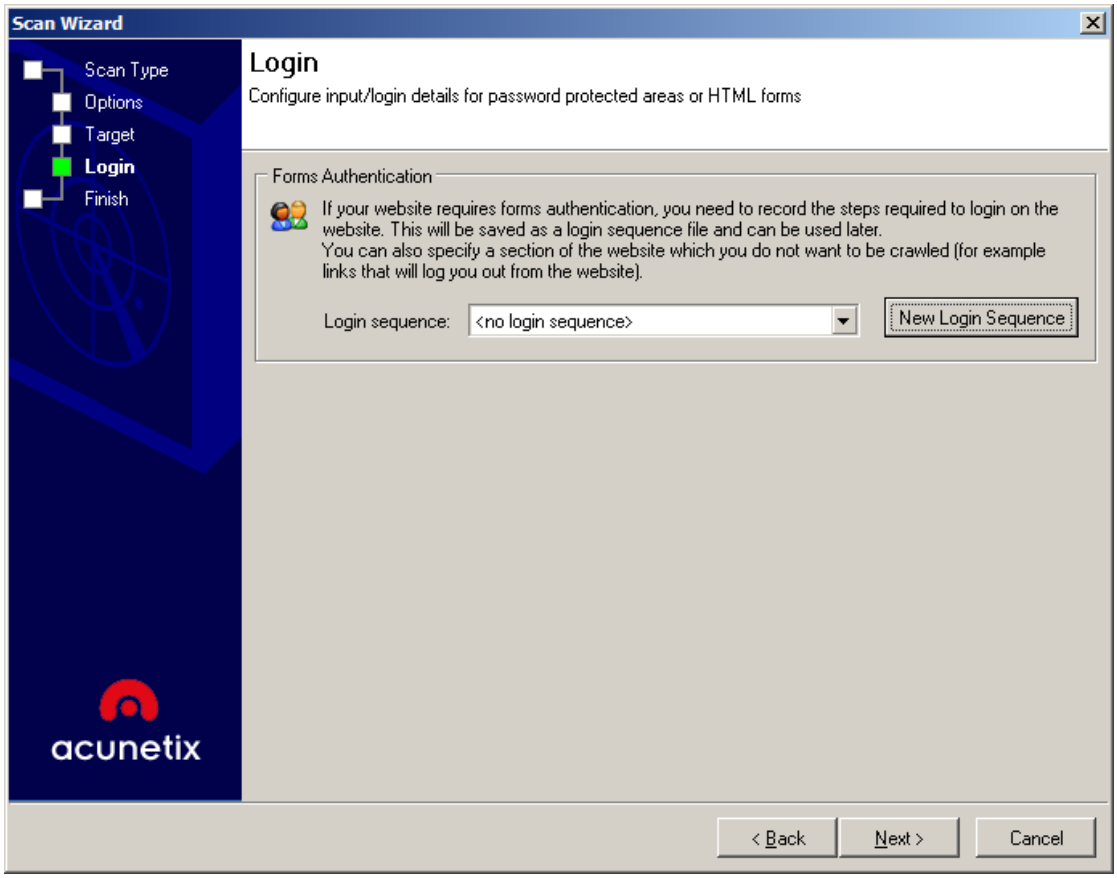
Acunetix WVS will automatically fingerprint the target website for basic details and will automatically determine if a custom 404 error-page is being used. For more information, please refer to 'Custom 404 Pages' section in the user manual.

The web vulnerability scanner will optimize and reduce the scan time for the selected technologies by reducing the number of tests performed. Use the checkboxes next to the web technologies to enable or disable scanning for specific technologies. If a specific web technology is not listed, then that technology is supported by there are no vulnerability tests exclusive to that technology.

Step 4: Configure Login for Password Protected Areas

There are 2 common types of Authentication mechanisms used authenticate.

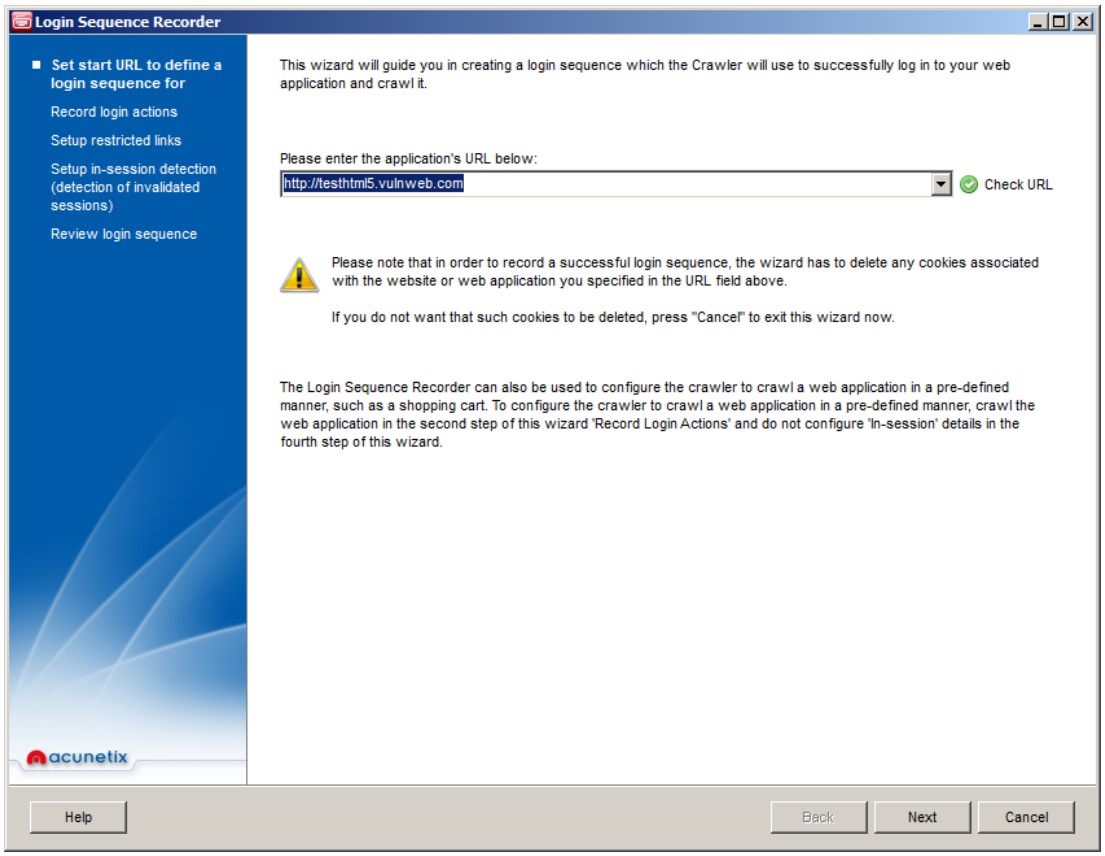
- **HTTP Authentication** - This type of authentication is handled by the web server, where the user is prompted with a password dialog. If you scan an HTTP password protected website, you will prompted to specify the username and password after going through the scan wizard, unless these are predefined in the Application Settings. For more information, please refer to the 'Scanning a HTTP password protected area' section in the user manual.
- **Forms Authentication** - This type of authentication is handled via a web form. The credentials are sent to the server for validation by a custom script. The rest of this section shows how to scan a site which uses this type of authentication.



Screenshot 4 – Scan Wizard: Login Details Options

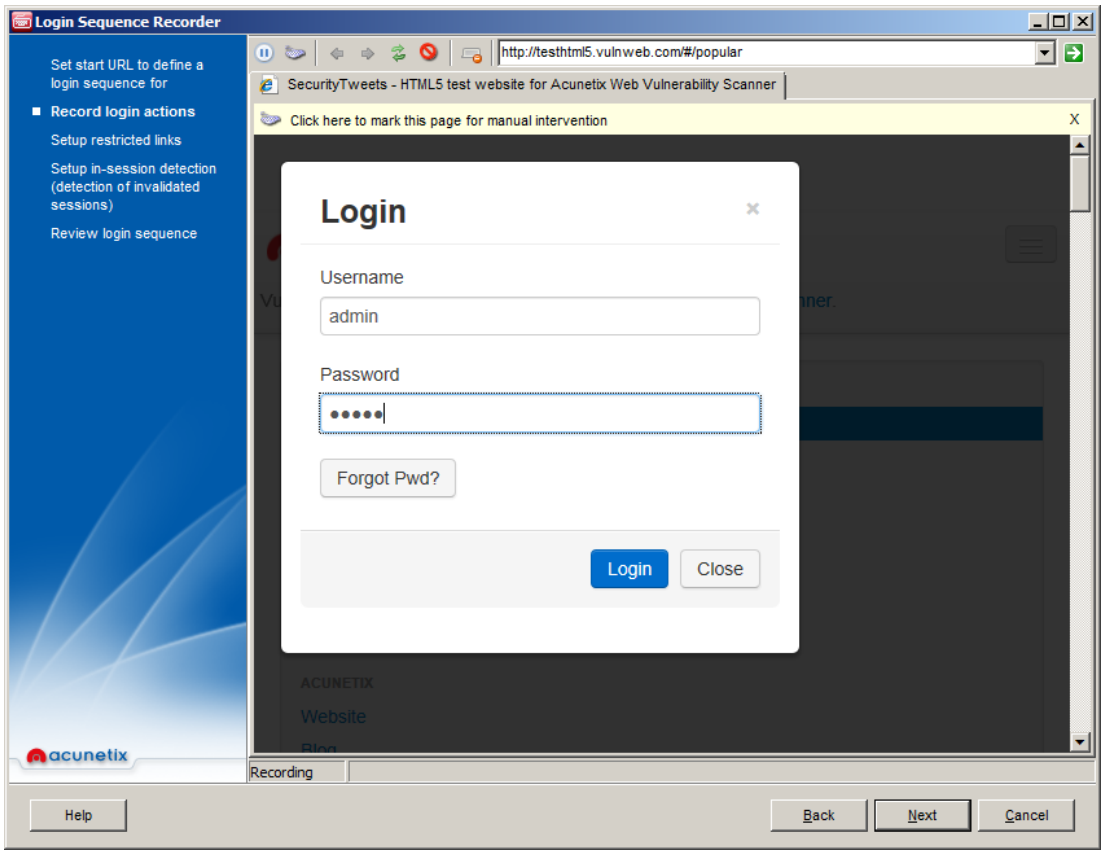
Scanning a form based password protected area

1. Click 'New Login Sequence' to launch the Login Sequence Recorder. By default the URL of the target website is automatically used. Click Next to proceed.



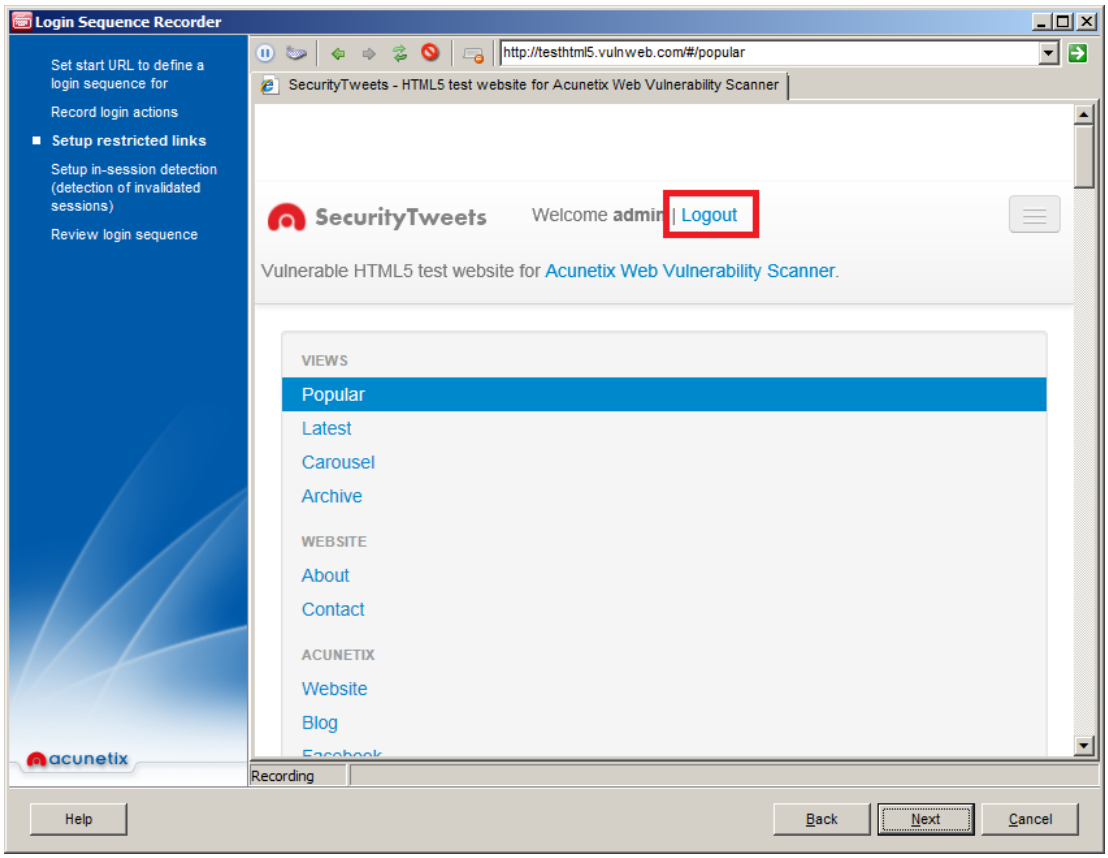
Screenshot 5 – Login Sequence Recorder: Confirm URL

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



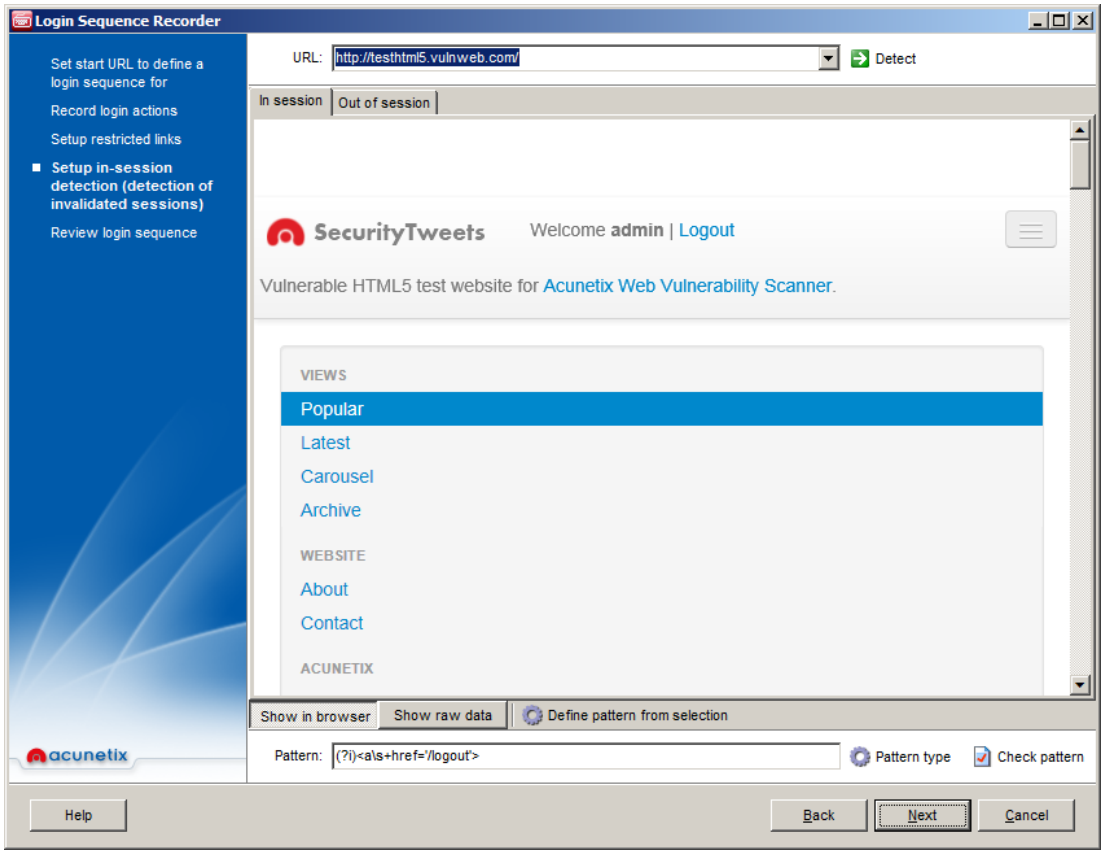
Screenshot 6 – Login Sequence Recorder: Record Login Actions

3. 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 on the logout link. If the logout link is not in the same page, click on 'Pause' in the top menu, navigate to a page where the logout link is found, resume the session and click on the logout link. Click 'Next' to proceed.



Screenshot 7 - Login Sequence Recorder: Specify restricted links

4. In this step, you can specify ‘In Session’ or ‘Out of Session’ detection patterns. Session detection allows the crawler to detect that it is still logged in. f the session expires during a crawl, the Crawler will automatically login again. Click the Detect button so the Login Sequence Recorder will try to automatically detect the pattern.
Note: if the automatic detection does not work, you would need to specify the pattern manually. For more information, please refer to the 'Scanning a HTTP password protected area' section in the user manual.



Screenshot 8- Login Sequence Recorder: Session Detection

5. In the last step of the wizard, you can review the recorded sequence. One can change priority of URLs, edit requests and add or remove requests. Click ‘Finish’ to finalize the login sequence recording.

For more information, please refer to the ‘Login Sequence Recorder’ section in the Acunetix WVS user manual.

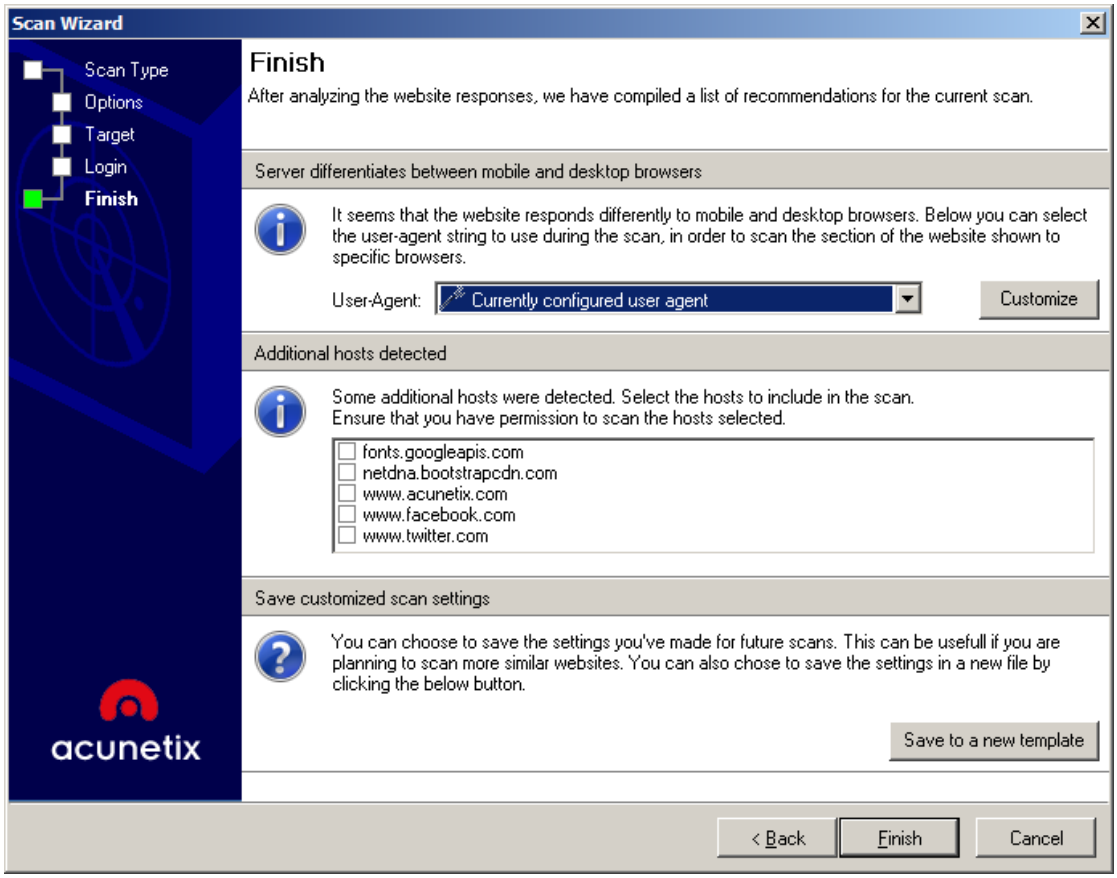
Step 5: Final wizard options

In the final step, the Scan Wizard will make an initial analysis of the web site and you might be alerted to the following:

- 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 is enabled, you will be prompted with the option to configure AcuSensor on the website. For more information, please refer to the 'Installing the AcuSensor Agent' section in the Acunetix WVS user manual.

- If the website responds differently to a mobile browser, in which case you will be presented with the option to scan the site as a normal browser or as a mobile browser
- Acunetix WVS will also alert you if additional hosts are discovered; i.e. when your website links to other websites. By default these are not scanned, but you will be given to option to include these in the scan. Remember that you need permission to scan these hosts too.

You will also be given the option to save the scan options to a new scanning template, so that the same scan settings can be re-used for future scans.



Screenshot 9 - Scan Wizard – Final Scan Configuration options.

Step 6: Completing the scan

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