WAS - Web Application Scanning 4.9

Release Notes

This new release of the Web Application Scanning (WAS) 4.9 includes improvements to global settings and Web Application enhancements. Looking for our user guides? Just log in to your account and go to Help > Resources.

Feature highlights for Qualys WAS 4.9

New Global Settings for Crawl Exclusion Lists
Vulnerability Severity Customization for Information Gathering Findings

Web Application Enhancements

Crawl Exclusion List for a Web Application
Exclude Links from Crawling

Reporting Enhancement

Compare scan report results for Information Gathering

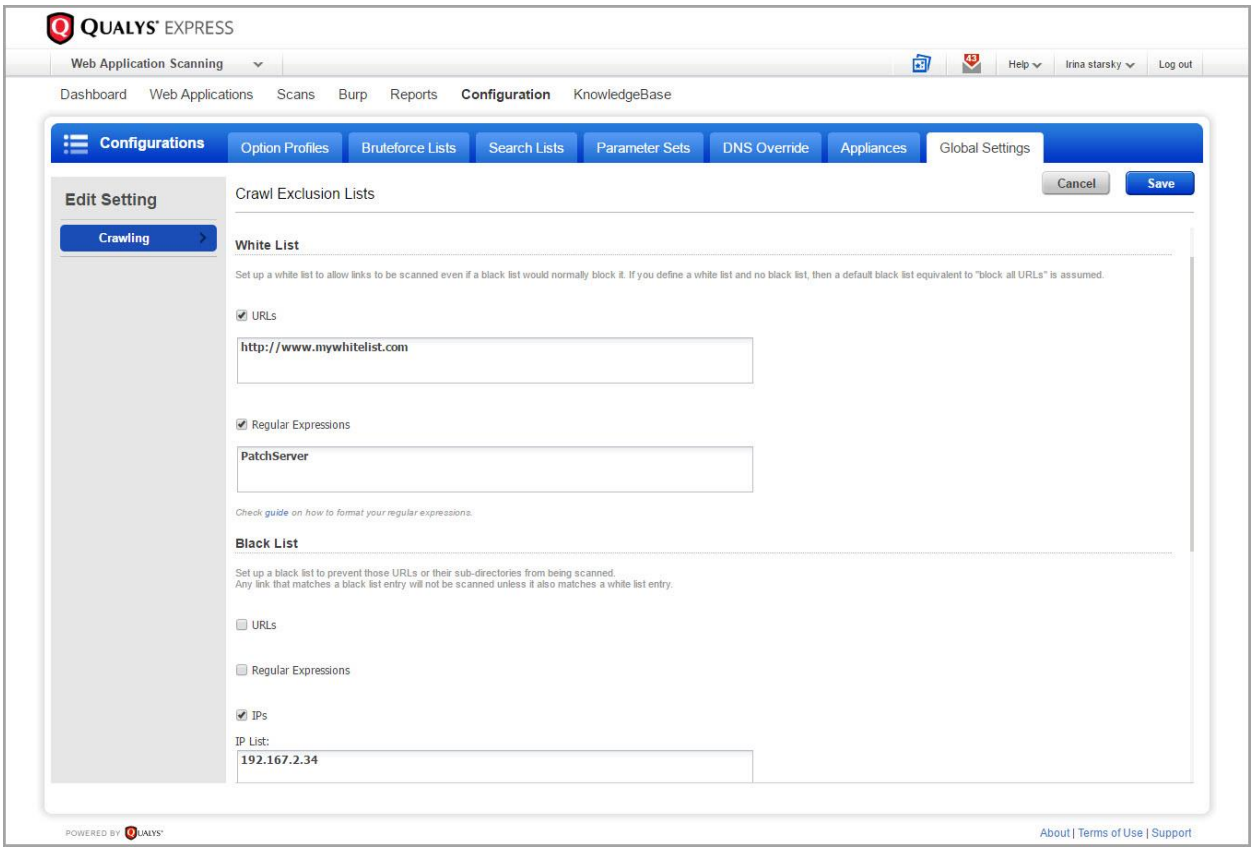
New Global Settings for Crawl Exclusion Lists

Want to allow or block IPs, URLs from being scanned at a global level?

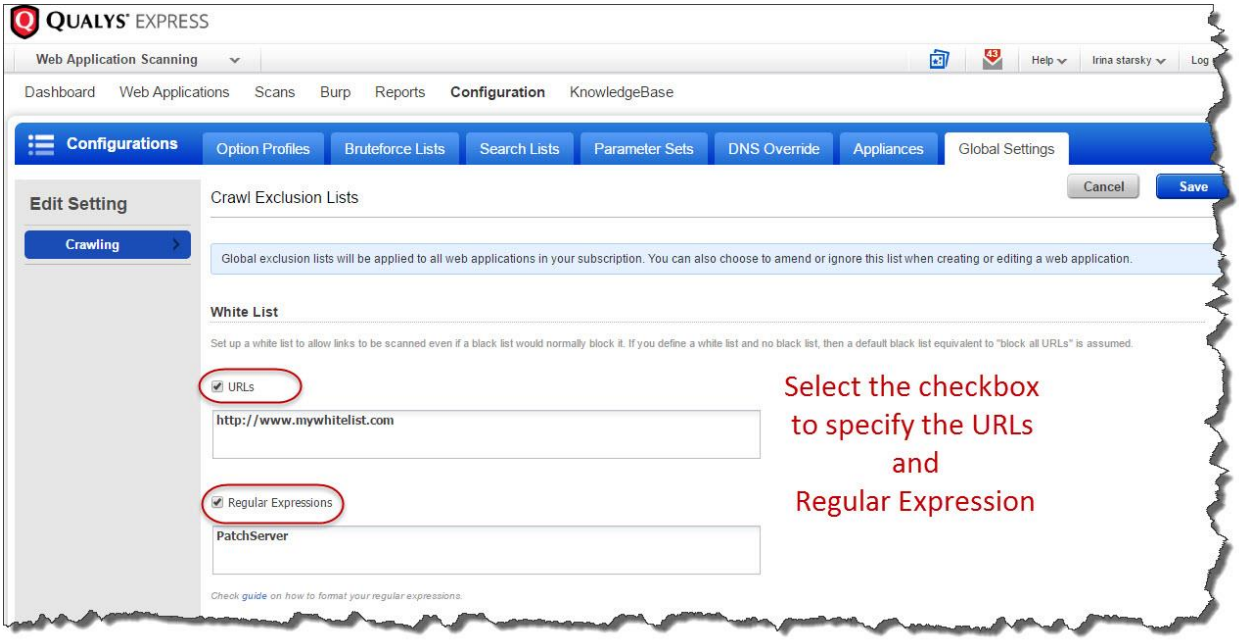
You can now configure what should be allowed or blocked from scanning. The new options in Global Settings allow you to define crawl exclusion list for the entire subscription (all web applications).

Go to Configuration > Global Settings > Crawling and view the global settings configured.

Click Edit to configure the crawl exclusion list. You can specify URLs, regexes or IPs (specific IPs or a range of IPs or a subnet) to be included or excluded from scanning. Select the checkbox to specify the details.



White List implies the list of items to be included in the scan.



Similarly, you can also configure the following for all web applications at one go:

Black List (list of items to be excluded from all scans),

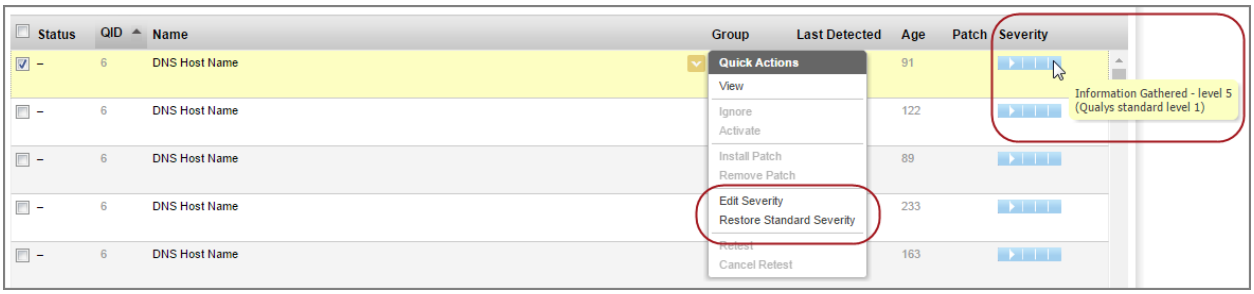
POST Data Black List (regular expression for URLs to be blocked from form submission),

Logout Regular Expression (regular expression to identify the logout links you want to exclude from scanning).

Vulnerability Severity Customization for Information Gathering Findings

You now have the ability to customize the vulnerability severity of information gathering findings reported in your web applications.

You can easily specify comments for every change and actions are logged to track changes made on the severity level. The mouse-over shows what the Qualys severity level of the finding was prior to being updated. The severity level change has an impact on the dashboard stats, web application reports and when viewing detections.

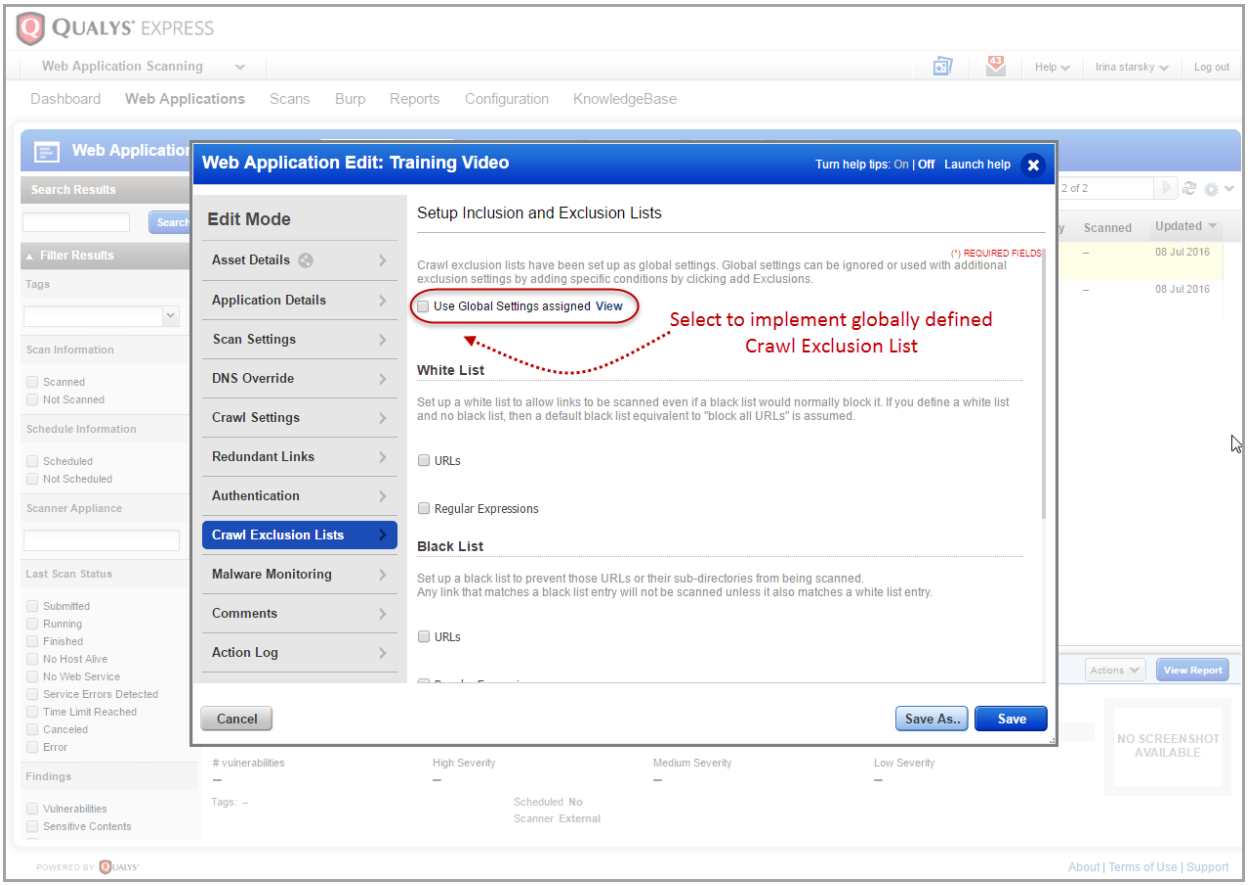


Simply navigate to Web Applications > Detections and select Edit Severity from the quick actions menu for the desired vulnerability. Here you can choose to increase or decrease the severity of the finding. Click Restore Standard Severity to revert to the Qualys standard severity level.

Crawl Exclusion List for a Web Application

You can also define the crawl exclusion list for exclusive for the web application. You can chose to implement the globally defined crawl exclusion list or customize the crawl exclusion list for the web application.

Edit the web application to configure the URLs and regexes to be included or excluded from scanning.



Select the required checkbox to specify the details. You can define:
White List (items to be included in the scan)

Black List (items to be excluded from all scans),

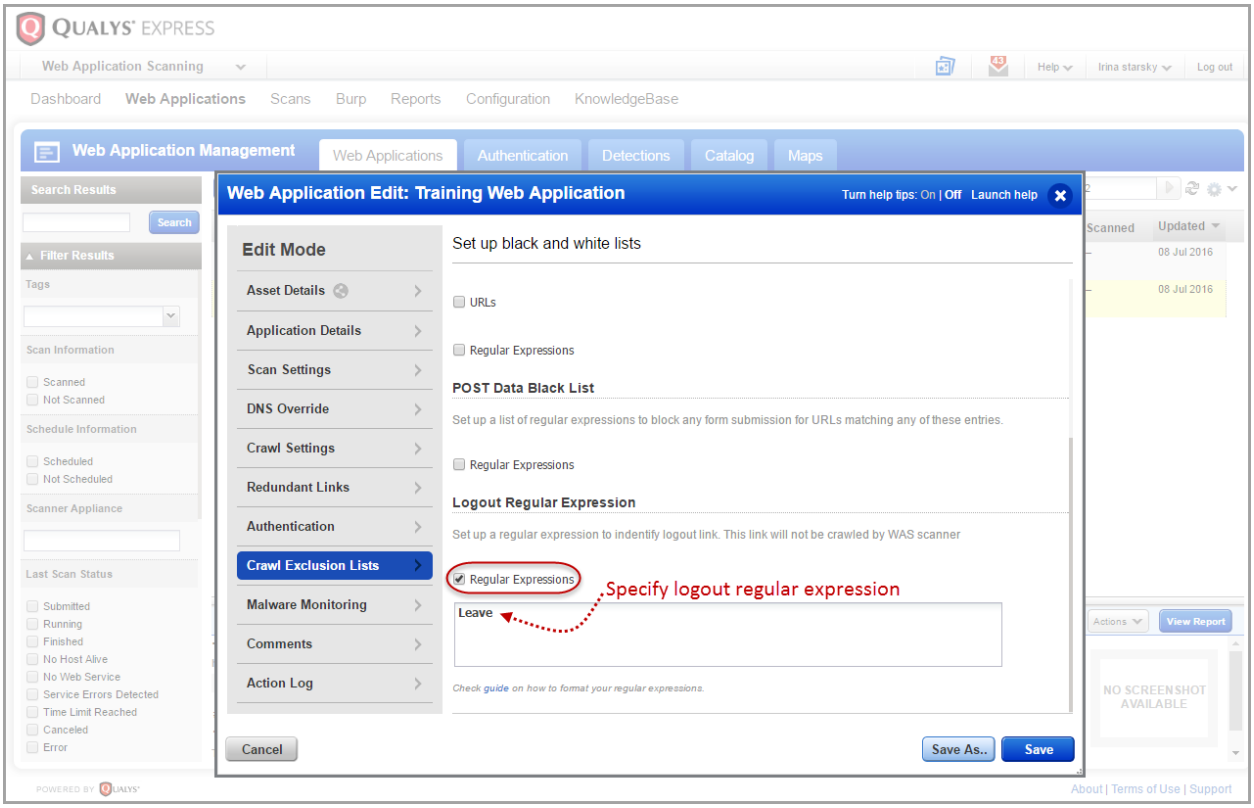
POST Data Black List (regular expression for URLs to be blocked from form submission),

Logout Regular Expression (regular expression to identify the logout links you want to exclude from scanning).

If you define crawl exclusion list for a web application and also enable the global settings for crawl exclusion list, the globally defined settings are implemented for the web application.

Exclude Links from Crawling

You can now define the logout links to be excluded from scanning by specifying the logout regular expression details while creating or updating the web application.



If you do not explicitly specify the links to be excluded from crawling, the default logout regular expression is applicable.

Reporting Enhancements

Compare scan report results for Information Gathering

You can view comparative analysis of changes in scan results between incremental scan reports.

Simply navigate to the Information Gathered section in a scan report. When you expand the Results section you can see the changes from previous scans highlighted in multiple colors. Disable the Highlight changes from the previous scan option to hide the comparative analysis. By default this option is enabled.