

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

<u>New Global Settings for Crawl Exclusion Lists</u> <u>Vulnerability Severity Customization for Information Gathering Findings</u>

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.

web Application Scanning	i 👻	Help 🗸 Irina starsky 🖌 Log or						
Dashboard Web Applica	ations Scans Burp Reports Configuration KnowledgeBase							
Configurations	Option Profiles Bruteforce Lists Search Lists Parameter Sets DNS Override Appliances Global Se	ettings						
Edit Setting	Crawl Exclusion Lists	Cancel Save						
Crawling >	White List							
	Set up a while list to allow links to be scanned even if a black list would normally block it. If you define a while list and no black list, then a default black list equivalent to "block	ck all URLs" is assumed.						
	VRLs							
	http://www.mywhitelist.com							
	Regular Expressions							
	PatchServer							
	Check guide on how to format your regular expressions.							
	Black List							
	Set up a black list to prevent those URLs or their sub-directories from being scanned. Any link that matches a black list entry will not be scanned unless it also matches a white list entry.							
	URLs							
	Regular Expressions							
	✔ Ps							
	IP List:							
	192.167.2.34							

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

teb Application Scattin	1 v	討 👺 Help 🗸 Irina starsky 🗸							
shboard Web Applic	ations Scans Burp Reports Configuration KnowledgeBase								
Configurations	Option Profiles Bruteforce Lists Search Lists Parameter Sets	DNS Override Appliances Global Settings							
dit Setting	Crawl Exclusion Lists	Cancel							
Crawling >	Global exclusion lists will be applied to all web applications in your subscription. You can also choose to amend or ignore this list when creating or editing a web application.								
	White List								
	Set up a white list to allow links to be scanned even if a black list would normally block it. If you define a whit	ite list and no black list, then a default black list equivalent to "block all URLs" is assumed.							
	URLs	Select the checkbox							
	http://www.mywhitelist.com	to specify the URLs							
		and							
	Regular Expressions	Regular Expression							
	PatchServer								

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.

Status	QID 🔺	Name	Grou	ıp	Last Dete	cted	Age	Patch	Severity	
-	6	DNS Host Name	Qui Viev	ick Actio	ons		91			Information Gathered - level 5
-	6	DNS Host Name	lgno Acti	ore ivate			122			(Qualys standard level 1)
-	6	DNS Host Name	Inst Rer	all Patch nove Pa	tch		89			
-	6	DNS Host Name	Edit Res	Severity store Sta	/ ndard Severity		233			
-	6	DNS Host Name	Car	est icel Rete	est		163			

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.

Veb Application Scann	ing 🗸					i 🔁	Help 🗸 🛛 Irina	starsky 🗸 🛛 L
shboard Web App	lications Scans Bur	p Repo	rts Configuration	KnowledgeBase				
Web Applicatio	Web Application E	dit: Trair	ning Video		Turn help	tips: On Off Launch help	×	
Irch Results	Edit Mode	S	Setup Inclusion and E	Exclusion Lists			y Scann	ed Update
lter Results	Asset Details ⊗	> C	rawl exclusion lists have b xclusion settings by adding	een set up as global settings. Gi 1 specific conditions by clicking a	obal settings can be igno Idd Exclusions.	(*) REQUIRED FIEL red or used with additional	.DS –	08 Jul 20
×	Application Details	\rightarrow	Use Global Settings assi	gned View Select t	o implement gl	obally defined	-	08 Jul 20
Information	Scan Settings	>	V ereneration		Crawl Exclusio	on List		
icanned lot Scanned	DNS Override	> %	White List					
dule Information	Crawl Settings	> ai	nd no black list, then a defa	ault black list equivalent to "bloc	all URLs" is assumed.			
cheduled lot Scheduled	Redundant Links	>	URLs					
ner Appliance	Authentication	>	Regular Expressions					
	Crawl Exclusion Lists	В	Black List					
Scan Status	Malware Monitoring	> S	et up a black list to prevent	t those URLs or their sub-directo	ries from being scanned.	hite list entry		
ubmitted tunning	Comments	>		and only with the bolt damed a		nite not entry.		
inished oHostAlive oWebService	Action Log	>	ORLS				Action	IS 💙 🛛 View R
ervice Errors Detected ime Limit Reached anceled rror	Cancel					Save As Save		NO SCREENS
ings	# vulnerabilities		High Severity	Medium Severity		Low Severity		AVAILABLI
ulnerabilities	Tags: -		Scheduled Scanner E	No External				

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.

QUALYS' EXPRESS				
Web Application Scanning	~	🗐 🦉 Help 🗸	Irina starsky 😽 🛛	.og out
Dashboard Web Applicati	ions Scans Burp Report	s Configuration KnowledgeBase		
📄 Web Application Ma	anagement Web Application	s Authentication Detections Catalog Maps		
Search Results	Web Application Edit: Tra	aining Web Application Turn help tips: On Off Launch help 🗙	2 🕨 🏵	٥×
▲ Filter Results	Edit Mode	Set up black and white lists	Scanned Updated	1 -
Tags	Asset Details 🔇 >	URLs	– 08 Jul 201	16
Scan Information	Application Details >	Regular Expressions		
Scanned Not Scanned	DNS Override >	POST Data Black List Set up a list of regular expressions to block any form submission for URLs matching any of these entries.		
Schedule Information	Crawl Settings	Regular Expressions		
Scanner Appliance	Redundant Links >	Logout Regular Expression		
	Authentication >	Set up a regular expression to indentify logout link. This link will not be crawled by WAS scanner		
Last Scan Status	Crawl Exclusion Lists	Regular Expression		
Submitted	Malware Monitoring >		Actions 🗸 View Re	eport
Finished No Host Alive	Comments >			
No Web Service Service Errors Detected Time Limit Reached	Action Log >	Check guide on how to format your regular expressions.	NO SCREENSHOT AVAILABLE	
Canceled .	Cancel	Save As Save		v
POWERED BY QUALYS	-	/	bout Terms of Use Su	upport

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.

Information Gathered Details							
1	50021 Scan Diagnostics						
Finding # Group CWE <u>OWA SP</u> WA SC	448615* (38800926) Information Gathered - -		Web Application Authentication Detection Date	API test for rdt and comment Not Used 20 Jul 2016 7:15PM GMT+0530			
Details					Show		
Results							
Highli New - Modif: Remove Loaded 0 HTML form Collected Total req Average s Most rece First col Special c -TO: The -CE: The 403 https 404 https Collected	<pre>.ght changes from previous scar this link was not found in the ied - this result was found by ed - this link was not found, 1 blacklist entries. whitelist entries. authentication unavailable, n 2 links overall. uests made: 24 erver response time: 0.70 secont links: umm indicates HTTP response co ases: request timed out request timed out request timed out request timed out ://10.11.69.21/WAS-2930/redund ://10.11.69.21/favicon.ico 1 links overall.</pre>	<pre>> previous scan the previous scan but ut was reported in the > WEBAPP entry found nds ie, > connection error): antLinks/ antLinks/mobile\$20</pre>	its value was dif e previous scan	ferent	Export		