

# Using Burp to Capture REST API Endpoints for WAS Scanning

Qualys Web Application Scanning (WAS) supports REST API security testing using Burp, plus new support for Swagger.

## Did you know we've added Swagger support?

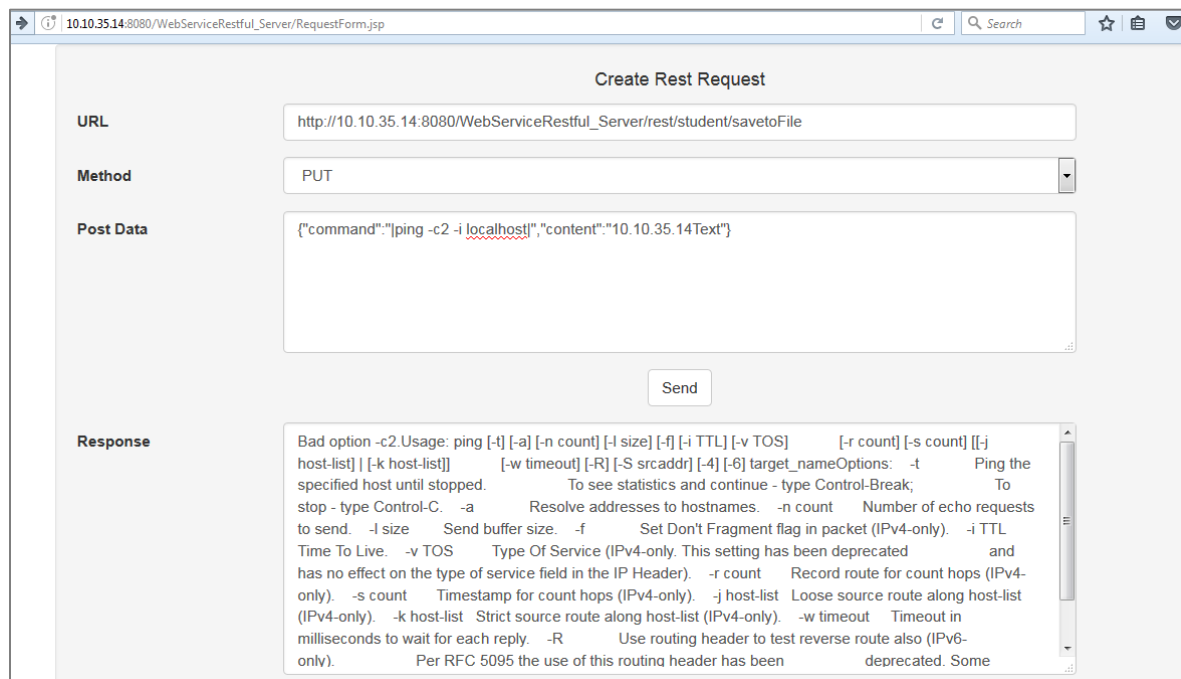
If you have a Swagger file then we recommend that you use Swagger instead of Burp for your REST API security testing. [Learn more on the Qualys Blog](#)

## Get Started using Burp

Scanning a REST service is a multi-step process which involves capturing requests using burp and configuring your web application to scan. We'll help you with these steps.

## Record requests to the REST service using BURP proxy tool

The first thing you'll need to do is enable proxy on your browser. Then, on the browser where you enabled proxy, make a request to the RESTful API service, as shown below.



Make all the required requests to the REST service. They'll be listed in the burp tool like this:

#	Host	Method	URL	Status	Length	MM	SSL	IP	Cookies	Time	Listener port
57	http://10.10.35.14:8080	GET	WebServiceRestful_ServeRequestForm.jsp	200	9393	HTML		10.10.35.14	JSESSIONID=84...	14:47:37.5	8080
59	https://api.googleapis.com	GET	ajax.googleapis.com/ajax/libs/jquery/3.1.0/jquery.min.js	200	86979	script		216.58.194.202		14:47:37.5	8080
62	http://10.10.35.14:8080	POST	WebServiceRestful_ServeRestStudentChangeMajor	200	202	text		10.10.35.14		14:48:13.5	8080
63	http://10.10.35.14:8080	POST	WebServiceRestful_ServeRestStudentUpdateData	200	180	text		10.10.35.14		14:48:51.5	8080
64	http://10.10.35.14:8080	POST	WebServiceRestful_ServeRestStudentUpdateData	200	180	text		10.10.35.14		14:48:58.5	8080
65	http://10.10.35.14:8080	PUT	WebServiceRestful_ServeRestStudentAvatarFile	200	179	JPG		10.10.35.14		14:49:50.5	8080
66	http://10.10.35.14:8080	PUT	WebServiceRestful_ServeRestStudentAvatarFile	200	146	HTML		10.10.35.14		14:50:40.5	8080
67	http://10.10.35.14:8080	PUT	WebServiceRestful_ServeRestStudentAvatarFile	200	146	HTML		10.10.35.14		14:51:23.5	8080
68	http://10.10.35.14:8080	PUT	WebServiceRestful_ServeRestStudentAvatarFile	200	234	text		10.10.35.14		14:52:27.5	8080

Select the items you want to scan. Right click and save all of the items.

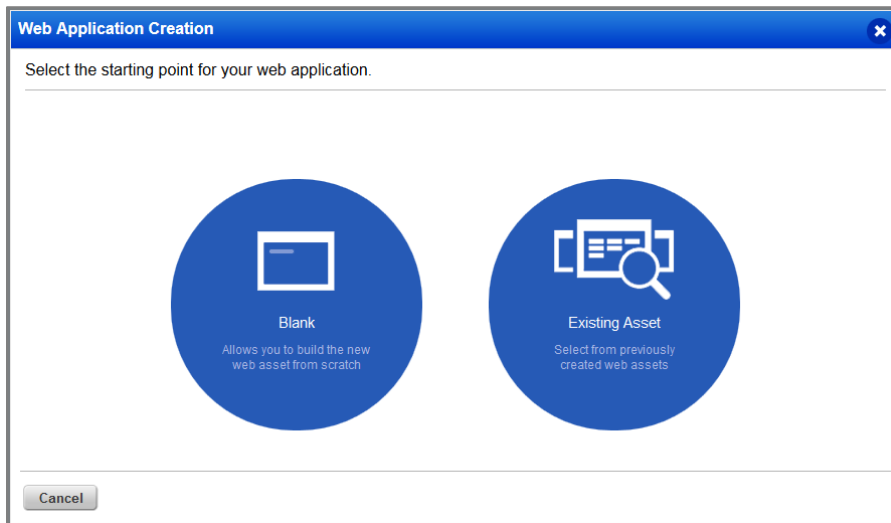
The screenshot shows the Burp Suite interface with the HTTP history table highlighted in orange. A right-click context menu is open over the table, and the 'Save All' option is selected. A 'Select a file' dialog box is open, showing the file name 'Burp\_Rest\_File.txt' and 'Files of Type' set to 'All Files'. The dialog box also has a 'Base64-encode requests and responses' checkbox checked.

## Configure your web application to launch WAS scan

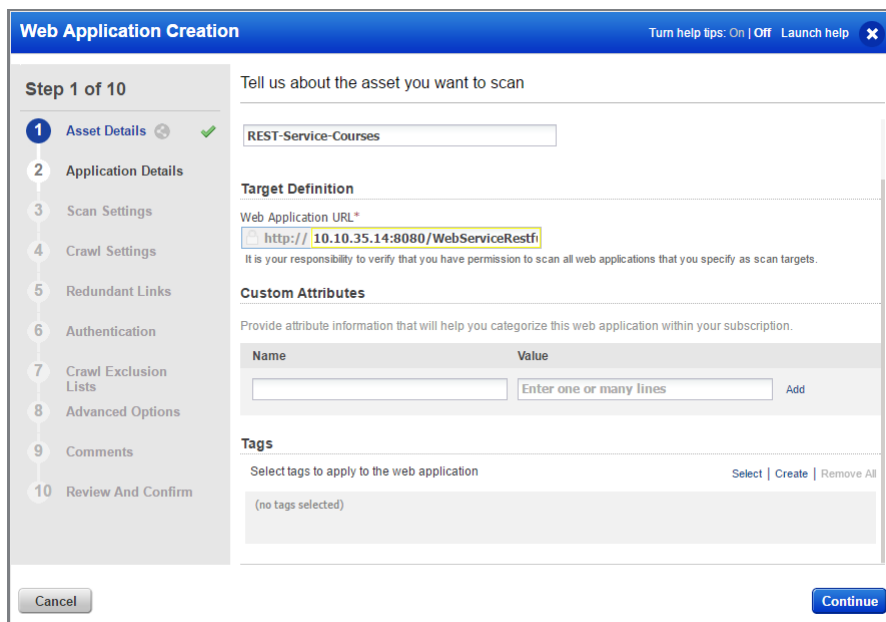
Log in to Qualys and choose Web Application Scanning (WAS) from the module picker.

The screenshot shows the Qualys module picker interface. The 'Web Application Scanning' dropdown is selected. The 'Active Modules (12)' list includes: PCI Compliance, AssetView, Cloud Agent, Vulnerability Management, Continuous Monitoring, Threat Protection, Policy Compliance, Security Assessment Questionnaire, Web Application Scanning (WAS), and Web Application Firewall. The 'Web Application Scanning (WAS)' module is highlighted with a red circle.

Click the Add Web Application button on your Dashboard or go to Web Applications > New > Web Application. Then choose your starting point. Select Blank and you'll be able to build your new web asset from scratch.



Give your web application a name and enter the URL to the RESTful API service.



Select the crawl scope and enter explicit URIs, if required. Then click Upload Burp Log File.

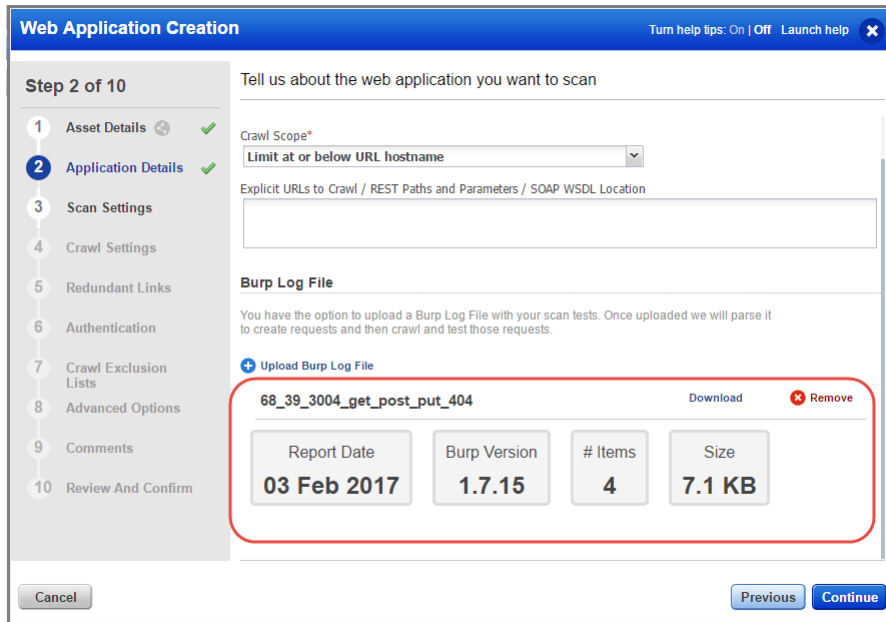
The screenshot shows the 'Web Application Creation' wizard at Step 2 of 10. The left sidebar lists steps from 1 to 10, with 'Application Details' (Step 2) selected. The main content area is titled 'Tell us about the web application you want to scan' and contains a 'Target Definition' section. Under 'Crawl Scope\*', a dropdown menu is open, showing 'Limit at or below URL hostname' selected. Below this is a text input field for 'Explicit URLs to Crawl / REST Paths and Parameters / SOAP WSDL Location'. In the 'Burp Log File' section, there is a button labeled 'Upload Burp Log File' with a plus icon, which is circled in red. At the bottom, there are 'Cancel', 'Previous', and 'Continue' buttons.

Click Choose File and browse to the burp file captured to upload it.

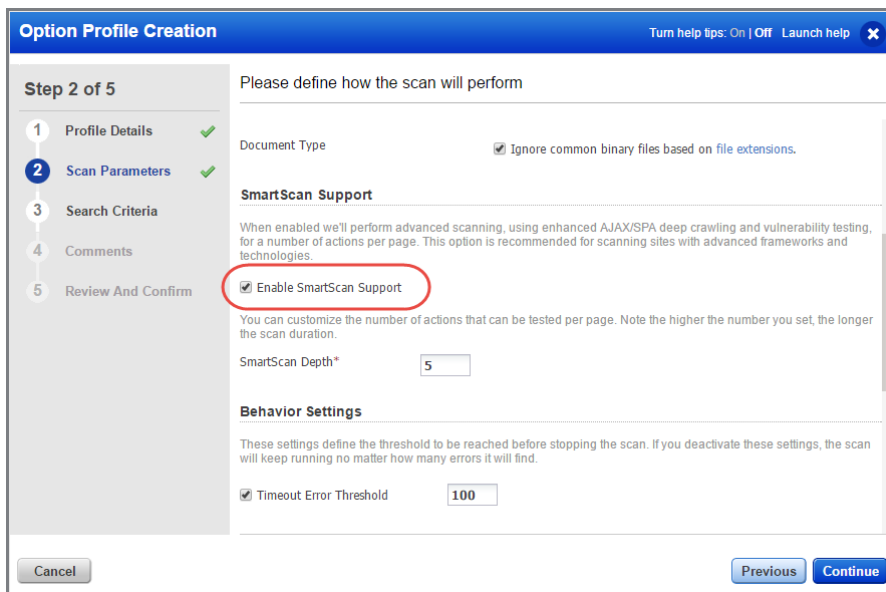
The screenshot shows the same 'Web Application Creation' wizard, but with an 'Import File' dialog box overlaid. The dialog has a title bar 'Import File' and a close button. It contains the text 'Import a file from your computer' and 'Select a file from your computer.' Below this is a 'Choose File' button and the text 'No file chosen.' There is a large grey area with a cursor icon and the text 'Drop file here'. At the bottom right of the dialog is a 'Cancel' button. The background wizard is dimmed, showing the 'Upload Burp Log File' button still highlighted.

When the Burp log file is successfully uploaded, you'll see file details on the screen, including the report date, version, number of items captured and the size. We will parse the file to create requests and then crawl the web application.

Note that you can upload only one Burp file with a maximum size of 5MB at a time. If you upload a second file, the new file will replace the old file.



Click Continue and walk through the remaining steps to save your new web application. You'll be prompted to choose an option profile (under Scan Settings), crawl settings, authentication options, etc. Note - The option profile you choose must have SmartScan enabled (see below).



That's it! Your web application is configured and ready to scan.

Last updated: April 30, 2018