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?

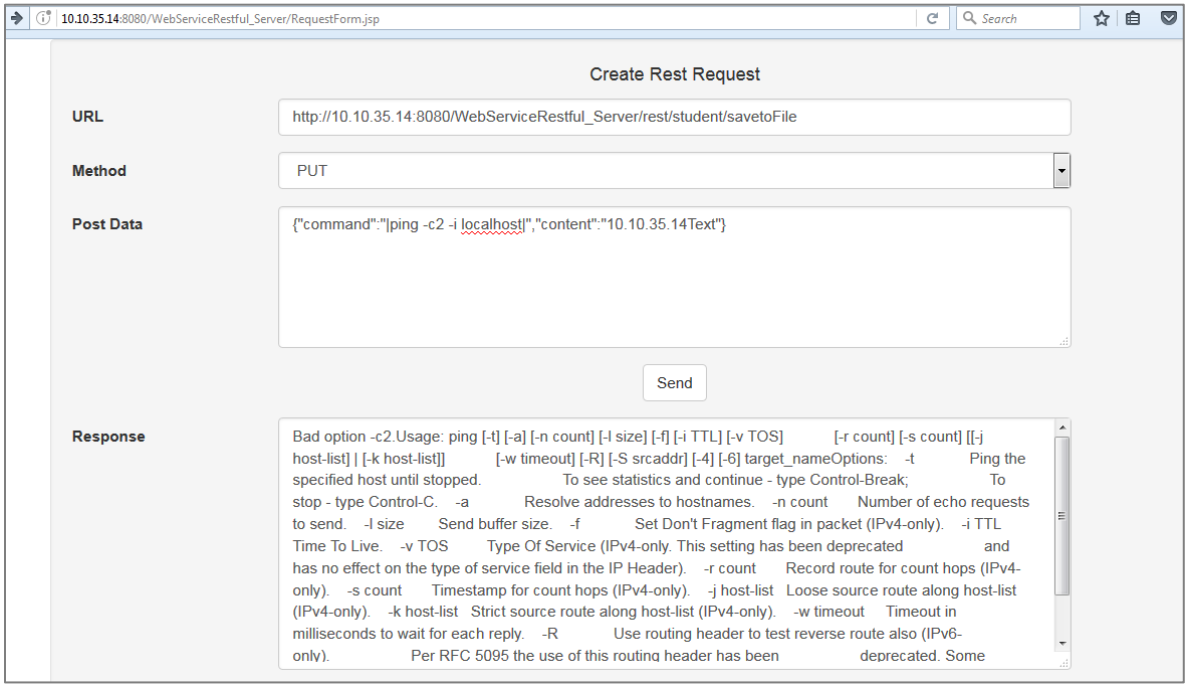
If you have a Swagger file then we recommend that you use Swagger instead of Burp for your REST API security testing. Learn more on the Qualys Blog

Get Started using Burp

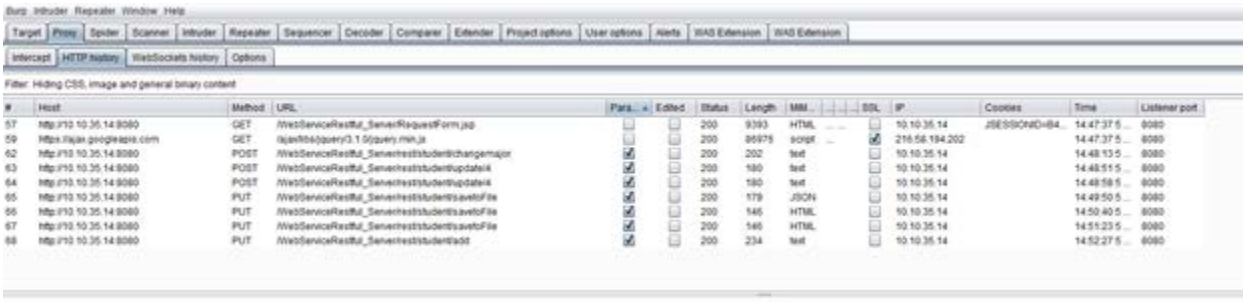
Scanning a REST service is a multi-step process which involves capturing requests using burp and configuring your web application to scan. We'll help you with these steps.

Record requests to the REST service using BURP proxy tool

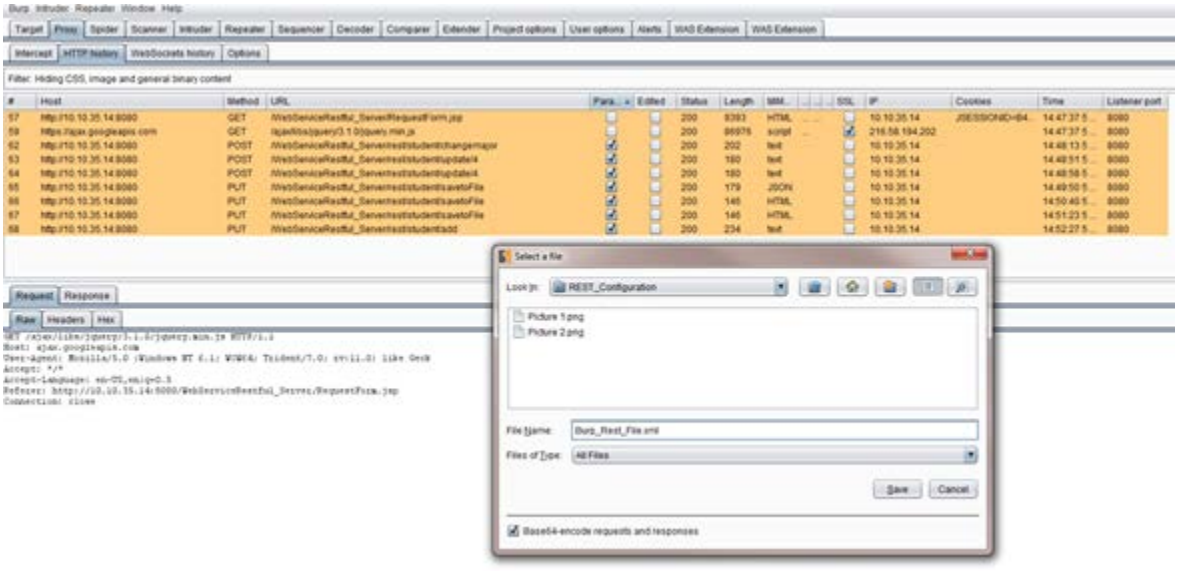
The first thing you'll need to do is enable proxy on your browser. Then, on the browser where you enabled proxy, make a request to the RESTful API service, as shown below.



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



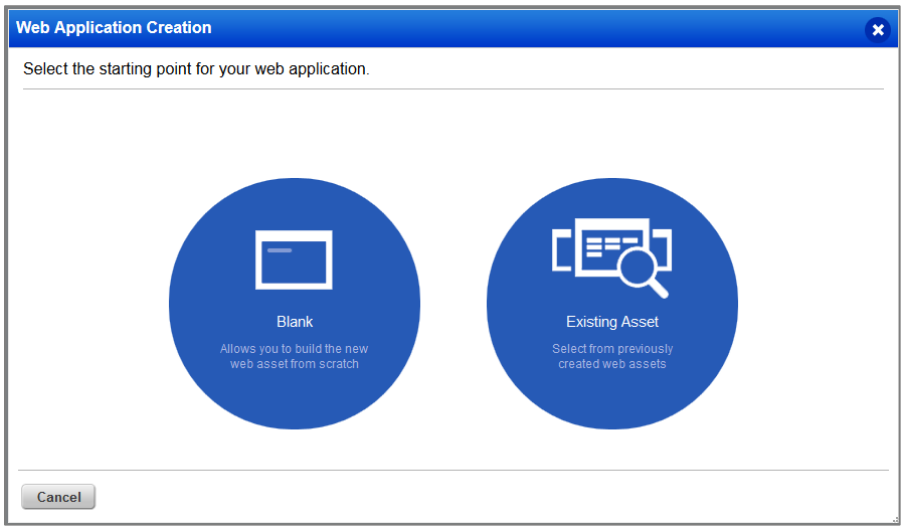
Select the items you want to scan. Right click and save all of the items.



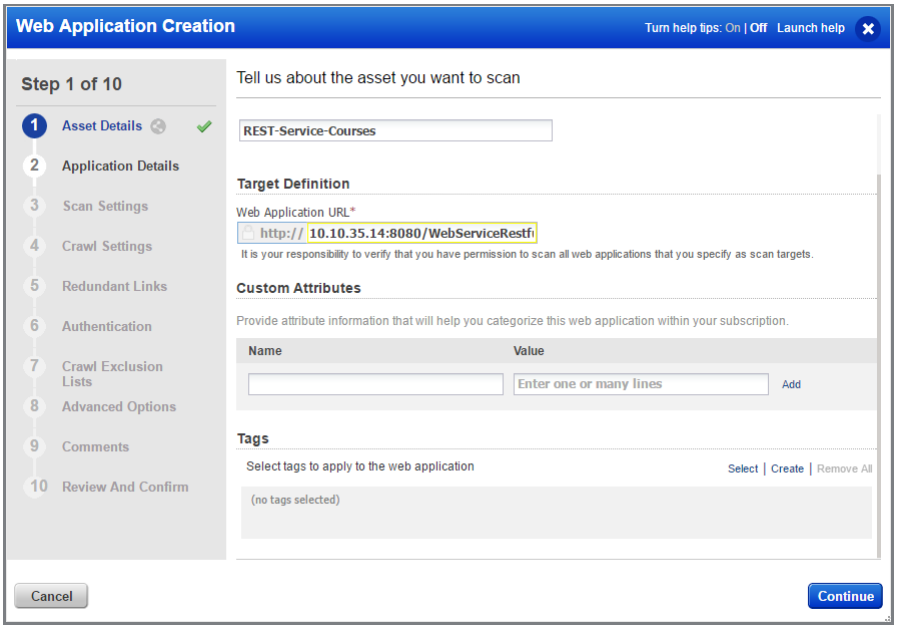
Configure your web application to launch WAS scan

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

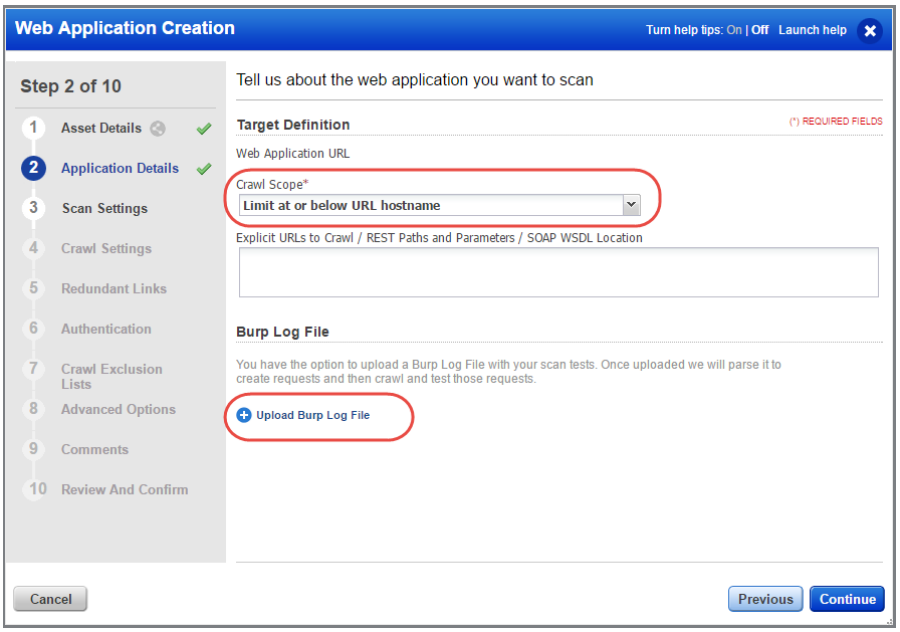
Click the Add Web Application button on your Dashboard or go to Web Applications > New > Web Application. Then choose your starting point. Select Blank and you'll be able to build your new web asset from scratch.



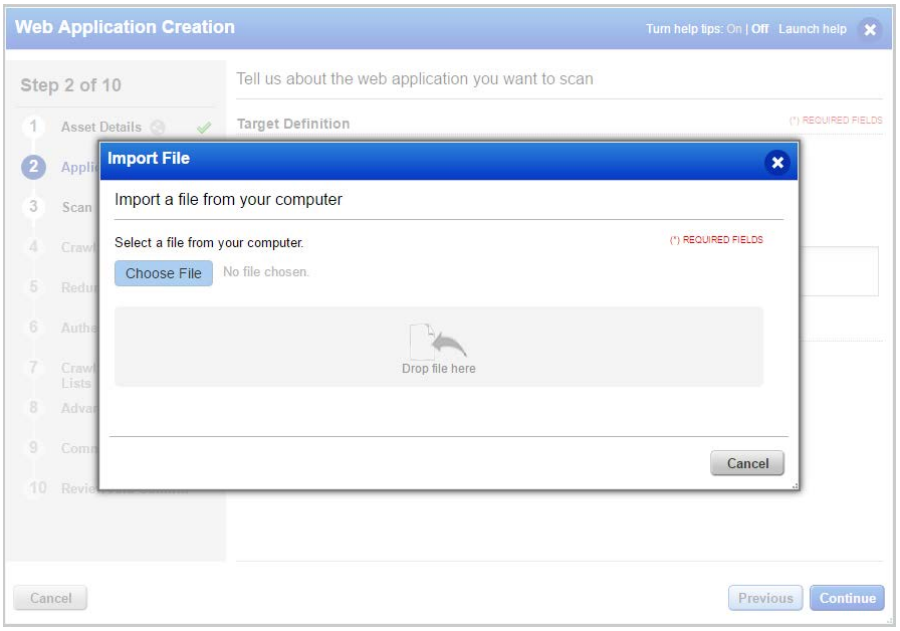
Give your web application a name and enter the URL to the RESTful API service.



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

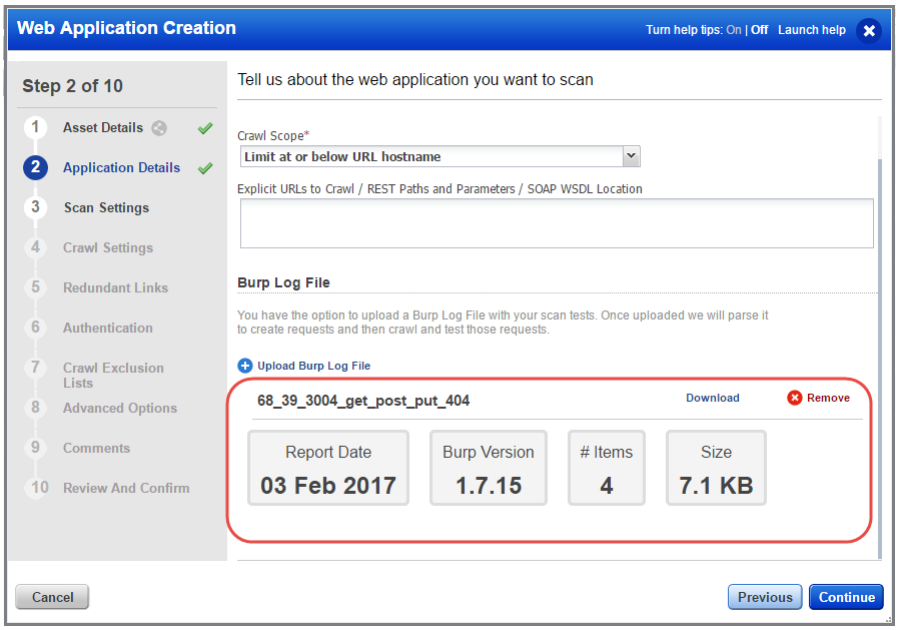


Click Choose File and browse to the burp file captured to upload it.

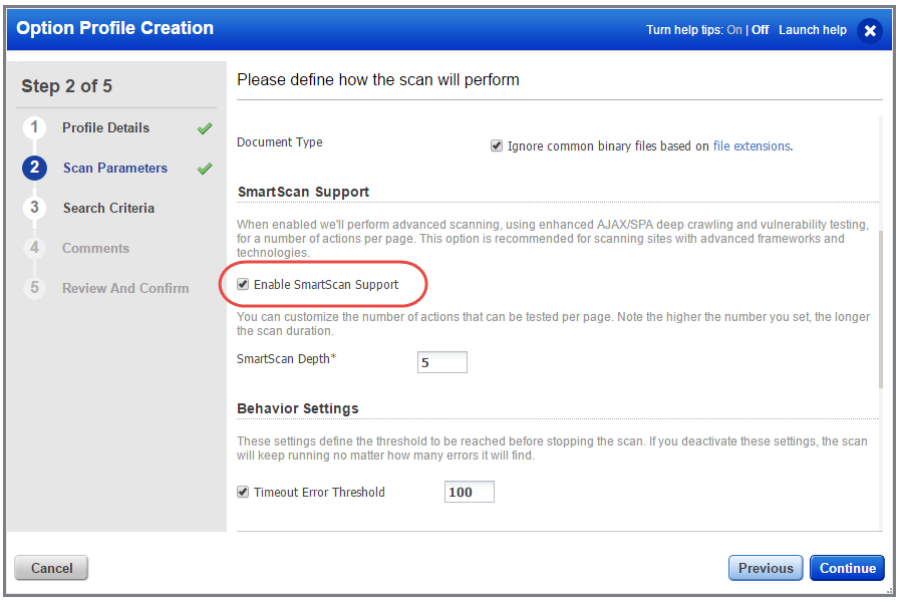


When the Burp log file is successfully uploaded, you'll see file details on the screen, including the report date, version, number of items captured and the size. We will parse the file to create requests and then crawl the web application.

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