

# 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.

→ (i) 10.10.35.14:8080/WebServiceRestful_Ser	ver/RequestForm.jsp	C <sup>d</sup> Q Search		☆	Ê	
	Create Rest Request					
URL	http://10.10.35.14:8080/WebServiceRestful_Server/rest/student/savetoFile					
Method	PUT		•			
Post Data	{"command":" ping -c2 -i localhoss]","content":"10.10.35.14Text"}					
	Send					
Response	Bad option -c2. Usage: ping [-t] [-a] [-n count] [-I size] [-f] [-i TTL] [-v TOS]       [-r count] [-4]         host-list] [ -k host-list]       [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_nameOptions:         specified host until stopped.       To see statistics and continue - type Control-Break;         stop - type Control-C.       -a       Resolve addresses to hostnames.       -n count       Number         to send.       -l size       Send buffer size.       -f       Set Don't Fragment flag in packet (IPv4-0         Time To Live.       -v TOS       Type Of Service (IPv4-only. This setting has been deprecated         has no effect on the type of service field in the IP Header).       -r count       Record route for contonly).        s count       Timestamp for count hops (IPv4-only).       -i host-list       Lose source rout         (IPv4-only).       -k host-list       Strict source route along host-list (IPv4-only).       -w timeout Tim         milliseconds to wait for each reply.       -R       Use routing header to test reverse route along host-list routes along only).       Per RFC 5095 the use of this routing header has been       deprected	s count] [[-j t Ping the To of echo requests pnly)i TTL and ount hops (IPv4- e along host-list eout in o (IPv6- ated. Some				

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

inte	rcept HTTP metary WebSockets h	istory Options	]					_					
	Hiding CBS, image and general binar	ry containt											
	Hust	Method	URL	Parallia	Edited	1564	Length	MM	101	P.	Cooties	Time .	Listener port
F	Mg/310 10 35 14 9080	GET	WebSeviceRealty_SeverRequesForm.jsp	10		200	9393	HTML	8	10.10.35.14	J9E390N/D+84	14:47:37.6	0080
	Max / Kax progresses.com	GET.	ajavito40quero/3.1.00quero.min.ja	6	6	200	86975	scree.		216.58.194.202		1447.375	8085
	htp://10.10.35.14.8080	P007	WebServiceRealful_ServertreatIstudentIchangemajor	60	- 63	200	202	144		10.10.25.14		14.48.135	9080
	http://10.10.35.14.9090	POST	WebServiceRealful_Serverireatistudent/updatei#	100	- 6	200	180	test	8	10.10.35.14		14.48515	8080
	http://10.10.3514.9090	POST	WebServiceRealty_ServectesStatuderBupdatei#	66	10	200	180	text .		10.10.35.14		14.48585	8080
	Mp #10 10 35 14 8080	PUT	WebSeviceResBull Sevenestistudent/savetoFile	56	10	200	179	JBON		10.10.35.14		14 49 50 5	8080
	http://10.10.35.14.9080	PUT	WebSeviceRestful Senectes/shudentsavetoFile	10	- 63	200	546	HTML	ē	10.10.35.14		14:50:40:5	6080
	http://10.10.35.14.8080	PUT	WebServiceReptbal ServerheststudentssivetoFile	1	- 63	200	140	HTML		10 10 35 14		1451235	6080
	http://10.10.3/5.14.0000	PUT	WebSeviceReattul_Sevenest/student/add	10	- 63	200	234	test	8	10.10.35.14		1452-275	6080

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

Target Press Spider Scanner	a hutury Coptons	Sequencer   Decoder   Comparer   Edender   1	Project california	Case options	Alerts	WAS EA	ension [ V	VAS Exter	nalion	-				
Filter: Hilding CSS, image and general b	many content									_				
Processor         Processor <t< td=""><td>Si Silet a for Lori y: in Pitare S Pitare 2</td><td>Pas.</td><td></td><td>1124cm 2000 2000 2000 2000 2000 2000 2000 20</td><td>Langth 8393 80976 202 180 180 140 146 254</td><td></td><td></td><td>6 CECCECSC 2</td><td>10.70.28 14 20.70.28 14 2016 06 194.2002 70 10.2016 14 70 10.2016 14 70 10.2016 14 70 10.2016 14 70 10.2016 14 70 10.2016 14 70 10.2016 14</td><td></td><td>1447 325 1447 325 1448 123 1448 123 1448 125 1448 125 1448 125 1448 125 1448 125 1448 125 145 125 145 125 145 125 145 125</td><td>Latane po 2000 2000 2000 2000 2000 2000 2000 20</td></t<>		Si Silet a for Lori y: in Pitare S Pitare 2	Pas.		1124cm 2000 2000 2000 2000 2000 2000 2000 20	Langth 8393 80976 202 180 180 140 146 254			6 CECCECSC 2	10.70.28 14 20.70.28 14 2016 06 194.2002 70 10.2016 14 70 10.2016 14 70 10.2016 14 70 10.2016 14 70 10.2016 14 70 10.2016 14 70 10.2016 14		1447 325 1447 325 1448 123 1448 123 1448 125 1448 125 1448 125 1448 125 1448 125 1448 125 145 125 145 125 145 125 145 125	Latane po 2000 2000 2000 2000 2000 2000 2000 20	
			files game files of∑ox	Durg, Rett, All Films	File.ord						([gas]) (	Cancel		
			a maneta a	ncode request	ts and test	onses								

## 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.

Web Application Creation	8
Select the starting point for your web application.	
Blank Allows you to build the new web asset from scratch	Existing Asset Select from previously created web assets

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

Web Applicat	ion Creatio	n	Turn help tip	s: On   Off Launch help 🗙
Step 1 of 10		Tell us about the asset you wan	it to scan	
1 Asset Detai	ils 🛞 🖌	REST-Service-Courses		
2 Application	n Details	Target Definition		
3 Scan Settir	igs	Web Application URL*		
4 Crawl Setti	ngs	http:// 10.10.35.14:8080/Webs It is your responsibility to verify that you have	ServiceRestfi permission to scan all web applications that you spe	ecify as scan targets.
5 Redundant	Links	Custom Attributes		
6 Authentica	tion	Provide attribute information that will help	) you categorize this web application within you	r subscription.
7 Crawl Excl Lists	usion	Name	Value Enter one or many lines	Add
9 Comments	Uptions	Tags		
10 Review An	d Confirm	Select tags to apply to the web applicat	íon	Select   Create   Remove All
		(no tags selected)		
Cancel				Continue

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

Web	Application Creati	Turn help tips: On   Off Launch h	elp (
Step	o 2 of 10	Tell us about the web application you want to scan	
1	Asset Details 🛞 🛷	Target Definition (') REQU	RED FIEL
2	Application Details 🛛 🛷	Web Application URL	
3	Scan Settings	Limit at or below URL hostname	
4	Crawl Settings	Explicit URLs to Crawl / REST Paths and Parameters / SOAP WSDL Location	_
5	Redundant Links		
6	Authentication	Burp Log File	
7	Crawl Exclusion Lists	You have the option to upload a Burp Log File with your scan tests. Once uploaded we will parse it to create requests and then crawl and test those requests.	
8	Advanced Options	Upload Burp Log File	
9	Comments		
10	Review And Confirm		
Can	icel	Previous	ontinu

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

tep	2 of	10	Tell us about the web application you wan	nt to scan
1	Asset [	Details 🕥 🚽	Target Definition	(*) RECUIRED F
2	Applic	Import File		8
3	Scan	Import a file f	rom your computer	
	Crawl	Select a file from	n your computer.	(*) REQUIRED FIELDS
	Redu	Choose File	No file chosen.	
	Authe			
	Crawl Lists		Drop file here	
	Advar			
	Comn			Cancel
	Revie			

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.

Web	Application Creatio	n		Т	urn help tips: On   Off	Launch help	×
Ste	p 2 of 10	Tell us about the web app	lication you want to	scan			
1	Asset Details 🚷 <	Crawl Scope* Limit at or below URL hostna Explicit URLs to Crawl / REST Pati	ame hs and Parameters / SOAP	VSDL Location			
3	Scan Settings Crawl Settings						
5	Redundant Links	Burp Log File	luro Log File with your sc	an tests. Once uplo	aded we will parse it		
6 7	Authentication	to create requests and then crawl	and test those requests.				
8	Lists Advanced Options	68_39_3004_get_post_p	out_404		Download	🙁 Remove	
9	Comments	Report Date	Burp Version	# Items	Size		
10	Review And Confirm	03 Feb 2017	1.7.15	4	7.1 KB		
Car	ncel				Previo	ous	nue

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).

Option Profile Creation		Turn help tips: On   Off Launch help 🗙
Step 2 of 5	Please define how the	scan will perform
1 Profile Details ✓	Document Type	
3 Search Criteria	SmartScan Support	
4 Comments	When enabled we'll perform a for a number of actions per pay technologies.	dvanced scanning, using enhanced AJAX/SPA deep crawling and vulnerability testing, i.e. This option is recommended for scanning sites with advanced frameworks and
5 Review And Confirm	<ul> <li>Enable SmartScan Support</li> <li>You can customize the numbe the scan duration.</li> <li>SmartScan Depth*</li> </ul>	r of actions that can be tested per page. Note the higher the number you set, the longer
	Behavior Settings	
	These settings define the thres will keep running no matter ho	hold to be reached before stopping the scan. If you deactivate these settings, the scan w many errors it will find.
	Timeout Error Threshold	100
Cancel		Previous

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

Last updated: April 30, 2018