

### Burp Suite Tutorial: Part 2 – Intruder and repeater tools

Karthik R, Contributor

Read the original story on SearchSecurity.in.

In <u>the first part of our Burp Suite tutorial series</u> we covered the basics of <u>Burp Suite</u> and presented an overview of some of the tools in the framework. In this second installment, we will describe two more important tools of the framework, viz. *intruder* and *repeater*.

#### **Burp intruder**

<u>Intruder</u> is used to automate customized attacks against Web applications. It has four panels – target, positions, payloads and options – as seen in Figure 1.

**Target:** This panel is used to specify the target host (the URL) and the port to use for the connection. There is an option for using SSL encryption, if required. Figure 2 shows the target panel.

**Positions:** This panel is very important in automating attack strings on the target. The types of attack vectors are sniper attack, battering ram attack, pitchfork attack and cluster bomb.

In this Burp Suite tutorial, Figure 3 shows that the payload positions are automatically highlighted with the **§** character. This is achieved by clicking on the *auto* button to the right. You can add markers and customize the scenario as required.

target proxy spitter i interner Wetuder repruder seguencer decoder comparer splinns alerts  1 2  Seguit peotions phyloids replans	
atlack type [shoes [v] 12 payoad positions [v] index.phg ?=Lt le=Signetial (Descloying Aset son=Souther) loging at yes=Singing aret write=Sile (balabant 1+7mig 1+) [ITTP/1.1] [+]	
Host: en.wikipedia.org User-Agent: Norilla/5.0 (Vindows NT C.1; cv:0.0.1) Geckn/I0300101 Firefox/8.0.1	AGE § clear § auto §
Proxy-Connection: keep-mlive Referr: http://m.wikipedim.org/w/index.php?tile=Special/BercLoginireturnto=Stikalahasti+Tempie Cocks: mediaWiki.user.bucketest.articlefeedback-tracking=Stikipores: mediaWiki.user.bucketest.articlefeedback-options=Stilambows: clicktracking-meanion=SpifistContentsticterentscons=Stikipores: mediaWiki.user.bucketest.articlefeedback-options=Stilambows: clicktracking-meanion=SpifistContentsticterentscons=Stikipores: mediaWiki.user.bucketest.articlefeedback-options=Stilambows: clicktracking-meanion=SpifistContentsticterentscons=StikiporesStilambows: Content-Longth: 105	sebash
vpEnne=SumernmenSaupFaseword=SphermwordScepLoginAttempt=SLogeinEcepLoginToken=ST685=EfteTimSt6401740i811070045c5	

Figure 1. Burp intruder (click to enlarge)



target positions payloads options
host en.wikipedia.org
port 80
use SSL

Figure 2. Target panel in Burp intruder

The sniper attack functions as a single payload set. Here, only one value is replaced for all the payload positions in sequence. This attack is generally used to test for common <u>SQL injection</u> and <u>XSS attacks</u> on the webpage.

A battering ram attack is another type of single payload attack. This is used when a single value is needed in the payload position and works fine when the password quality rules and policies set are weak. Considerable enumeration needs to be carried out before using this form of attack; it works in scenarios where, for instance, the username and password both have the same values.

The pitchfork attack or cluster bomb attack can be used when multiple payload sets are required. In a cluster bomb attack there are two lists, with each word in the first list running against a corresponding word in the second list. It is used when the target has a login form that has to be breached.

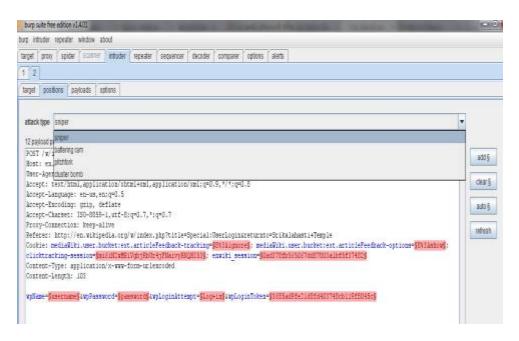


Figure 3. Positions panel, with different attack vectors (click to enlarge)



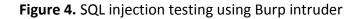
In this section of our Burp Suite tutorial, we shall attempt a SQLi attack on the demo page of etopshop at the following URL: <u>http://www.etopshop.com/demo/pcstore/admin.asp</u>.

### SQL injection testing using Burp intruder

After capturing the page as described in <u>Part 1 of this Burp Suite tutorial</u> series, choose the payload markers as username fields and password fields. Since the attack requires two parameters, we would need a multiple payload attack. We shall choose the pitchfork attack vector from the dropdown menu and the preset list for adding SQL attack strings to be tried out at the target. Figure 4 shows the options being set for the attack.

There are several options under this payload set. These include character based, number based, random characters based, brute force, dates, and so on. For this Burp Suite tutorial we have used the preset list. Once we set up options and payload here, we are ready to test the target. To do so, go to *intruder* in the menu bar and click on *start attack*.

target positions payloads options	
number of payloads: 2 number of requests: 1	
payload set 1 v preset list	•
' or '1'='1 admin'	
add	
add from list	·
load	paste
delete	clear
payload processing rules	
	edit
	remove
	up
	down
select rule type	add





Filter: sh	owing all items							
results	target positions	payloads o	ptions					
request	payload1	payload2	status	error	timeout	length	comment	
0	pajiodari		200			1585	baseline request	
1 (	' or '1'='1	' or '1'='1	200			1528		
		$\sim$						
request	response							
raw	params headers	hex						
POST /	demo/pcstore/ad	lmin.asp HTTP	9/1.1					
Host:	www.etoshop.com	1						
	gent: Mozilla/5	,						
Accept	: text/html,app	lication/xht	ml+xml,appl	icatio	on/xml;q=0	).9,*/*;	q=0.8	
Accept	-Language: en-u							
-								
-	-Encoding: gzip	,						
Accept	-Charset: ISO-8	859-1,utf-8;	q=0.7,*;q=0	.7				
Accept Proxy-	-Charset: ISO-8 Connection: kee	859-1,utf-8; p-alive						
Accept Proxy-( Referen	-Charset: ISO-8 Connection: kee r: http://www.e	859-1,utf-8; p-alive toshop.com/d	lemo/pcstore	/admin	-			
Accept Proxy-( Referen	-Charset: ISO-8 Connection: kee	859-1,utf-8; p-alive toshop.com/d	lemo/pcstore	/admin	-			
Accept Proxy-( Referen Cookie	-Charset: ISO-8 Connection: kee r: http://www.e	9859-1,utf-8; p-alive toshop.com/d SATDTSD=KKEJ	lemo/pcstore PHIBLGJJKLD	/admin EPFPEC	-			
Accept Proxy-( Referen Cookie Conten	-Charset: ISO-8 Connection: kee r: http://www.e : ASPSESSIONIDA	9859-1,utf-8; p-alive toshop.com/d SATDTSD=KKEJ	lemo/pcstore PHIBLGJJKLD	/admin EPFPEC	-			
Accept Proxy- Referen Cookie Conten Conten	-Charset: ISO-8 Connection: kee r: http://www.e : ASPSESSIONIDA t-Type: applica	9859-1,utf-8; p-alive toshop.com/d SATDTSD=KKEJ	lemo/pcstore PHIBLGJJKLD	/admin EPFPEC	-			
Accept Proxy-( Referen Cookie Conten Conten Connec	-Charset: ISO-8 Connection: kee r: http://www.e : ASPSESSIONIDA t-Type: applica t-Length: 73 tion: close	859-1, utf-8; p-alive toshop.com/d SATDTSD=KKEJ tion/x-www-f	lemo/pcstore PHIBLGJJKLD form-urlenco	e/admin EPFPEC oded	CPEB			
Accept Proxy-( Referen Cookie Conten Conten Connec	-Charset: ISO-8 Connection: kee r: http://www.e : ASPSESSIONIDA t-Type: applica t-Length: 73	859-1, utf-8; p-alive toshop.com/d SATDTSD=KKEJ tion/x-www-f	lemo/pcstore PHIBLGJJKLD form-urlenco	e/admin EPFPEC oded	CPEB	t nSubmi	t=Login	
Accept Proxy-( Referen Cookie Conten Conten Connec	-Charset: ISO-8 Connection: kee r: http://www.e : ASPSESSIONIDA t-Type: applica t-Length: 73 tion: close	859-1, utf-8; p-alive toshop.com/d SATDTSD=KKEJ tion/x-www-f	lemo/pcstore PHIBLGJJKLD form-urlenco	e/admin EPFPEC oded	CPEB	tnSubmi	t=Login	

Figure 5. SQL attack in progress with Burp intruder

Figure 5 shows the process of SQL injection. The *results* tab shows the payloads being sent to the target. The *request* tab shows the HTML source and how the payloads are placed at the chosen markers. The *response* tab shows that the injection succeeded; analyzing the HTML source shows a "welcome" message. In order to see the webpage, simply click on *render*.

Figure 6 of this Burp Suite tutorial shows the successful penetration of the Web application, using the SQL injection vulnerability. Similarly, XSS attack vulnerabilities can also be checked using the preset list to load XSS strings and probe the target.

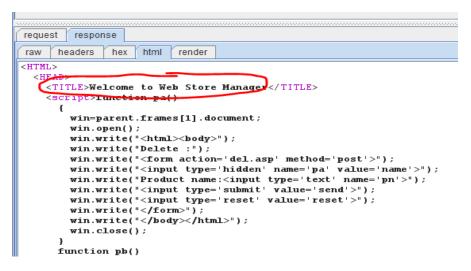


Figure 6. Successful SQL injection of the target

### **Burp repeater**

Let us now move to <u>Burp repeater</u> in this Burp Suite tutorial. Burp repeater is a tool used to manually modify the HTTP requests and test the responses given by the page. This can even lead to probing for vulnerabilities on the webpage. Basically, this is used to play back requests to the server.

#### **Understanding XSS with Burp repeater**

For this Burp Suite tutorial, we shall use a vulnerable Web application at <a href="http://www.steve.org.uk/Security/XSS/Tutorial/simple.html">http://www.steve.org.uk/Security/XSS/Tutorial/simple.html</a> for understanding and analyzing XSS (cross-site scripting) vulnerability in a webpage.

go cancel host www.steve.org.uk					
< > port 80 use SSL					
request					
raw params headers hex					
<pre>User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:8.0.1) Gecko/20100101 Firefox/8. Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-us,en;q=0.5 Accept-Encoding: gzip, deflate Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7 Proxy-Connection: keep-alive Referer: http://www.steve.org.uk/Security/XSS/Tutorial/simple.html Content-Type: application/x-www-form-urlencoded Content-Length: 47</pre>					
text Leave+a+message+for+another+user+%DD%OA					
+ < >					

Figure 7. Burp repeater panel



In Figure 7, the attack spot that takes the input on the webpage has been highlighted. We need to find out if the input is sanitized for code injections or not. First, we shall attempt a simple HTML injection on the webpage as shown in Figure 8. This tells us that HTML tags are not sanitized in the input. As before, use *render* to preview the webpage within the tool in its own panel.

Accept: text/html,application/shtml+sml,application/sml:q=0.9,*/*;q=0.8	
Accept-Language: en-us.en/g=0.5	
Accept-Encoding: grip, deflate	
Accept-Charset: ISO-8059-1,utf-8;q=0.7,*;q=0.7	
Proxy-Connection: keep-alive	
Referer: http://www.steve.org.uk/Security/XSS/Tutorial/simple.html Content-Type: application/x-www-form-urlencoded	
Content-Length: 32	
test-" (hi> HTML INJECTION (/hi>	
+ < +	
response	
raw headers her fitm render	
*	
UTAL INFECTION	
HTML INJECTION	
[Return to munple page [Return to index ]	
V second and a second data second and a second sec second second sec	

#### Figure 8. HTML injection

Next, we will try probing for XSS vulnerabilities. For this we need to pass a script tag. The attack string could be a simple JavaScript such as:

<iframe src="javascript:alert('Xss')";</iframe>



Figure 9. Iframe injection using repeater



www.steve.org.uk/Security/XSS/Tutoria	/simple.cgi			
	1			
		-		
			Xss	
			ок	
		-		

Figure 10. Confirming XSS vulnerability in the target

In figure 9 of this Burp Suite tutorial, we see that the iframe code is injected into the source of the webpage. Check the browser to confirm if there is an XSS bug present in the application. We see that there is a reflected XSS vulnerability on the target, as shown in Figure 10.

In this installment of our Burp Suite tutorial, we have covered the intruder and repeater tools in detail. We have also explained how to analyze the target for Web-related security bugs such as SQL injection and cross-site scripting. In the third and final installment, we shall cover the remaining tools of Burp Suite.

>>Read more about Burp Sequencer, decoder and comparer in the 3rd part of this series<<



**About the author:** *Karthik R* is a member of the NULL community. Karthik completed his training for EC-council CEH in December 2010, and is at present pursuing his final year of B.Tech. in Information Technology, from National Institute of Technology, Surathkal. Karthik can be contacted on rkarthik.poojary@gmail.com. He blogs at <u>http://www.epsilonlambda.wordpress.com</u>

You can subscribe to our twitter feed at @SearchSecIN. Read the <u>original</u> <u>story</u> on SearchSecurity.in.

