Claranet Cyber Security

Burpsuite Configuration Guide

Burpsuite Configuration

Step 1: Open a Command Prompt Terminal and type "burpsuite" as shown below:



Step 2: Ignore any warning or update notification and select Temporary Project as shown below and click Next.

root@/# bur	psuite				
1 1	Burp Suite Community Edition v2020	.9.2			- 🗆 X
(?	Welcome to Burp Suite Commu Note: Disk-based projects are	unity Edition. I	Use the options below to create ad on Burp Suite Professional.	or open a project.	BURPSUITE
	 Temporary project 				
	New project on disk	Name:			
		File:			Choose file
	Open existing project		Name	File	
		File:			Choose file
			Pause Automated Tasks		
					Cancel Next



Step 3: Keep the default selection , " Use Burp defaults" and click on "Start Burp".

root@/# burp	suite					
🚯 Bu	rp Suite Community Edition v2020.9.2		- 🗆 X			
?	Select the configuration that you would like to) load for this project.	COMMUNITY EDITION			
	Use Burp defaults					
	Use options saved with project		C3			
	Load from configuration file	File				
	File:		Choose file			
	 Default to the above in future Disable extensions 					
			Cancel Back Start Burp			

Step 4: Burp Suite has now been started and you should have the below window. Click on the "Proxy" Tab highlighted below in red.

Burp Suite Community Edition v2020.9.2 - Temporary Project		- 🗆 X
Burp Project Intruder Repeater Window Help		
Dashboard Target Proxy Intruder Repeater Sequencer	ecoder Comparer Extender Project options User options	
Tasks 🕀 New scan 🕀 New live task 🕕 🚱 🥐 🖉	Time to level up? Catch more bugs with Burp Suite Pro	Find out more
Filter Running Paused Finished	Issue activity [Pro version only]	? ₄ ^
1. Live passive crawl from Proxy (all traffic)	Filter High Medium Low Info Certain Firm	Tentative Search
Add links. Add item it 0 items added to site map	Issue type Host	Path
Capturing: 0 responses processed	i Suspicious input transformation (reflected) http://insecure-bank.co	/url-shorten
0 responses queued	SMTP header injection http://insecure-website	/contact-us
	Serialized object in HTTP message http://insecure-bank.co	/blog
	Cross-site scripting (DOM-based) https://insecure-bank.c	
	XML external entity injection nttps://vulnerable-web	/product/stock
	Web cache poisoning	/product
Event log	Advisory	
Filter Critical Error Info Debug Search		
Time Type Source Message		
17:24:57 6 Oct 2020 Error Proxy Failed to start p	y l	
17:24:57 6 Oct 2020 Info Suite Using SOCKS	(



Step 5: Under the Proxy tab confirm the below default settings. Use the "Edit" button in case you wish to change the default settings. By default Burp is configured to listen over the localhost interface of port 8080. Feel free to change it to another port number and update the browser settings.

Burp F	Project Int	uder Repeate	er Window	Help						
Dash	board T	rget Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options
Interce	Intercept HTTP history WebSockets history Options									
() () ()	Proxy Listeners Surp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as									
	Add	Running	Interface	- I	nvisible R	edirect	Ce	rtificate	TLS Pro	tocols
			127.0.0.	1:8080			Pe	r-host	Default	
	Edit									
	Remove									

Step 6: Now , open your firefox browser as shown below.

🍅 New Tab 🛛 🗙 🗙	+										
\leftarrow \rightarrow C $rac{1}{2}$	Q Search with Google or e	、Search with Google or enter address									
		Search the Web	_								
		Search the web									
	Top Sites >										
	🏷 Highlights →										



Step 7: Press the "ALT" key in windows/linux or "Option" for mac users to enable viewing of the Browser Tool tab.Click on Edit and Preferences as shown below. Alternatively press the below keys in quick succession \rightarrow "ALT/Option + E + N".

×	Options	× +							
\rightarrow	C 🕜	Sirefox about:preferences#general	☆	lii\					
			₽ Find in Options						
⋪	General	General							
6	Home	Startup							
٩	Search	Restore previous session Warn you when guitting the browser							
	Privacy & Security	Always check if Firefox is your default browser							
C	Sync	😢 Firefox is not your default browser	Make <u>D</u> efault						
		Tabs ✓ Ctrl+Iab cycles through tabs in recently used order ✓ Open links in tabs instead of new windows When you open a link in a new tab, switch to it immediately Show tab previews in the Windows taskbar							

Step 8: Click on "Advanced" -> Network -> Settings

← → ⊂ ŵ	Sirefox about:preferences#general	☆ II\ 🗉
		ions
🔅 General		
Home Home	Browsing	
Q Search	✓ Use <u>a</u> utoscrolling	
	Use smooth scrolling	
	Show a touch keyboard when necessary	
Sync Sync	Always use the cursor keys to navigate within pages	
	Search for text when you start typing	
	✓ Enable picture-in-picture video controls Learn more	
	✓ <u>R</u> ecommend extensions as you browse <u>Learn more</u>	
	Recommend <u>f</u> eatures as you browse Learn more	
	Network Settings	
Extensions &	Themes Configure how Firefox connects to the internet. Learn more	S <u>e</u> ttings
⑦ Firefox Suppo	nt	



Step 9: Enter the information as shown below. Here we are configuring Firefox to communicate with Burpsuite over port 8080.Click OK and then in new tab open notsosecureapp.com

	Connection Settings			×
			,	^
General	Configure Proxy Access to the Internet			H
Home	🔘 No ргоху			H
nome	Auto-detect proxy settings for this network			H
Search	Use system proxy settings			
Drivoov & Socurity	<u>Manual proxy configuration</u>			
Privacy & Security	HTTP Proxy 127.0.0.1	<u>P</u> ort	8080	H
Sync	\checkmark Also use this proxy for FTP and HTTPS			L I
	<u>H</u> TTPS Proxy 127.0.0.1	P <u>o</u> rt	8080	L I
	ETP Proxy 127.0.0.1	Po <u>r</u> t	8080	H
	SO <u>C</u> KS Host	Por <u>t</u>	0	H
	● SOC <u>K</u> S v4 ○ SOCKS <u>v</u> 5			11
	<u>A</u> utomatic proxy configuration URL			11
		Rele	oad	11
	No proxy for			
	localhost, 127.0.0.1			11
Extensions & Themes				~
Firefox Support	OK Cancel		<u>H</u> elp	



Step 10: Once you have configured your browser, the next step is to test that it is working properly. Go to any HTTP site. If everything works well, you'll see an HTTP request in the intercept tab as shown in the following screenshot. Congratulations you have just configured Burpsuite successfully! You are now ready to intercept each HTTP/HTTPS request that the browser is sending to the server(s).

\rightarrow X	۵	Q notsos	ecureapp.con	۱								
	🚯 Burp Suite C	ommunity Edit	tion v2020.9.2 -	Temporary Pr	oject							
	Burp Project	Burp Project Intruder Repeater Window Help										
	Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options											
	Intercept H	TTP history	WebSockets I	nistory Opt	ions							
	Request to	http://notsose	cureapp.com:	30 [52.6.3.46)]							
	Forward	D	rop	ntercept is or	n Act	ion	Open Brows	er				
	Raw Paran	ns Headers	Hex									
	Pretty Raw	\n Acti	ons 🗸									
	<pre>I GET / HTTP/1.1 GET / HTTP/1.1 Host: notsosecureapp.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: close Cookie: PHPSESSID=i37bogtn2n0127328gtf6hc5m2 Upgrade-Insecure-Requests: 1 </pre>											

Step 11: Navigate to the "Target" tab , select the url "http://XXXXXXXXX.com" , right click on "Add to scope" as shown below. Scope defines to focus our testing to scoped items only, we can use/filter scoped items to Burp components such as interception, proxy history, scanner etc. However, we need to configure few components such as proxy history which is described in next steps.

Burp Project Intruder Repeater Window Help										
Dashboard Target Proxy	Intruder Repeater	Sequencer	Decoder	Compar	er Extender	Project options	User opt	ions		
Site map Scope Issue defin	itions									
Filter: Hiding not found items: hiding CSS, image and general binary content: hiding 4xx responses: hiding empty folders										
All https://incoming.telemetry.ml	ozilla.org	Host	,	Method	URL	Param	S Status	Length	MIME type	Title
Interpretation in the second secon	0	http://notsose	cureapp	GET	1		200	4475	HTML	NotSoSecure - Web
http://notsosecureapp.com https://snippets.cdn.mozilla	http://notsos	ecureapp.com	1	1	/about.php		200	4634	HTML	NotSoSecure - Web
► Inttps://tlscommunity-uat.can	Add to scope				/index.pnp /phpinfo.php		200	4475 77536	HTML	phpinfo()
https://www.google.com	Scan				/register.php		200	5646	HTML	NotSoSecure - Web
https://www.notsosecure.com	Engagement to	ools [Pro version	n only]	•	/DTD/xhtml1-tra	nsition				
	Compare site	maps			/changelog.php					
	Expand branch	ı			/changelog.php	?v=1.0 ✓				
	Expand reques	sted items					_			J.+
	Delete host									
	Copy URLs in	this host					Respo	nse		
	Copy links in th	nis host		Тн	xe		Raw	Headers	Hex	
	Save selected items									
Show new site map window					1		Pretty Raw Render In Actions V			
	Site map documentation									
						A	1 HTT	P/1.1 2	COULOK	000 10 10 01 cmm



© Claranet Cyber Security 2021. All rights reserved

Step 12: You can also select "Advanced Options" from "Scope" configuration. Add regex[.***\.webhacklab\.com\$**] to Host or IP Range field, this allows all subdomains of webhacklab.com with all ports.

Das	hboard Tar	get Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	
Site	map Scope	e) Issue de	efinitions								
 Target Scope Define the in-scope targets for your current work. This configuration affects the behavior of tools throughout the suite. The easiest way to configure use the context menus in the site map to include or exclude URL paths. Use advanced scope control Include in scope Add Enabled Specify a regular expression to match each URL component, or leave blank to match any item. An IP range can be specified instead of a hostname. 										onfigure scope	
	Remove			Protocol:	Any				T	•	
	Paste URI			Host or IP ra	ange: .*\.web	hacklab\.cor	n\$				
	Load			Port:	Enter	egex or leav	/e blank				
	Exclude from	scope		File:	File: Enter regex or leave blank						
	Add	Enabl	ed								
	Edit			Paste UF	RL			ОК	Cancel		

Step 13: Now click on the "Filter" row right below the SiteMap tab in the above image and select the option as "Show only in-scope items" as shown below and then click on the Proxy tab

Burp P	Burp Project Intruder Repeater Window Help											
Dashb	oard Target Proxy Intruder	Repeater	Sequencer	Decoder	Compa	rer Ex	xtender	Project options	User options			
Site m	ap Scope Issue definitions											
Filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders												
(?)	Filter by request type	Fil	ter by MIME ty	ре		Filter by	status co	de Folde	ers	MI		
() ()	Show only in-scope items Show only requested items	6	✓ HTML ✓ Script	✓ Other te ☐ Images	xt	✓ 2xx ✓ 3xx	x (succes x (redirec	s] 🗹 tion]	Hide empty folders			
	 Show only parameterized required Hide not-found items 	uests	Z XML CSS	FlashOther bit	nary	 4xx [request error]✓ 5xx [server error]						
	Filter by search term [Pro only]	F	Filter by file extension			Filt	Filter by annotation					
			Show only	asp,aspx,	jsp,php	p,php Show only commented iter			nmented items			
	Case sensitive Negative	search	Hide: js,gif,jpg,png,css			Show only highlighted items						
	Show all Hide all Revert changes											
			1 GET / 1	HTTP/1.1					1 HTTP/1.1	301 M		



Step 14: Under the Proxy tab click on the "HTTP history" tab and then again click on the same "Filter" button and select "Show only in-scope items". This way you'll be able to view only requests/responses related to our target application in the HTTP History.

Dashb	oard Target I	Proxy Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options		
Intercept HTTP history WebSockets history Options											
Filter: Hiding out of scope items; hiding CSS, image and general binary content											
(?)	Filter by request type		Fi	Filter by MIME type		Filt	Filter by status code				
ĘC3	Hide items without responses Show only parameterized requests		s quests	Script	 Other te Images Flash Other b 	inary	3xx [succe 3xx [redire 4xx [reque: 5xx [server	ction] st error]			
	Filter by search term [Pro only]			Filter by file extension			Filter by annotation			Filter by listener	
	 Regex Case sensitive Negative search 		search	Show only: asp,aspx,jsp,php Hide: js,gif,jpg,png,css			Show only commented items Port Show only highlighted items			Port	
Show all Hide all Revert changes											
Pretty Raw In Actions V Pretty Raw Render In Actions V											
1 GET 2 Hos	/robots.txt t: www.notsos	HTTP/1.1 secure.com			1 HTTP/1.1 301 Moved Permanently 2 Date: Tue, 06 Oct 2020 12:08:42 GMT						

