

## **BurpSuite**

#### The Swiss army knife of security tools

#### **Glancing Blow** Burp Intruder Repeater Window Help Target Proxy Spider Scanner Intruder Repeater Sequencer | Decoder | Comparer | Extender | Options | Alerts Site map Scope Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders ? nttps//polansistaging.yammer.com Method URL Params Status Length MIME type Title Comment Host http://privacy.microsoπ.com A h tps://questions-staging.heroku.com https://www. ienie van ner con THEFT erpri... A h tps://r.casalemedia.com https://www.taging.vernmer.com //securitvinnovation.c 3020 https://www.taging.yammer.com 2894 http://repo.manjaro.org https://www.taging.yammer.com A h tps://s-passets.pinimg.com https://www.taging.yammer.com ► A h tps://s-static.ak.facebook.com A h tps://s.adroll.com https://www. ading yammer.com HTML Yammer ► A h tps://s0.staging.assets-yammer.com https://www.itaging.yammer.com ▶ A h tps://s3.amazonaws.com https://www.taging.yammer.com count... https://www.laging.yammer.com http://safebrowsing.clients.google.com 85426 count... https://www.\_\_\_\_g...g., \_..... A h tps://sb-ssl.google.com -► 🔒 h tps://secure.adnxs.com 4 l e ► A h tps://secure.fastclick.net Request Response A h tps://segment-pixel.invitemedia.com A h tps://sendto.mozilla.org Raw | Params | Headers | Hex ► A h tps://services.addons.mozilla.org Value http://sizzleis.com Name ► 🤒 h tps://ssl GET /HTTP/1.1 h tps://ssl.google-analytics.com Host ► A h tps://ssl.gstatic.com Mozilla/5.0 (X11; Linux x86\_64; rv:26.0) Gecko/20100101 Firefox/26.0 User-Agent A h tps://stagexdrproxy.yammer.com text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8 Accept ► http://staging.sched.do en-US,en;q=0.5 Accept-Language ► A h tps://staging.yammerusercontent.com gzip, deflate Accept-Encoding DNT 1

#### The Tab Functionality

Burp Intruder F	lepeater	Window He	lp							
Target Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Options	Alerts
Site map Sco	pe									

Tiltan Lliding pat found itamas biding CCC image and general hippopresentants biding Austreeneness. biding emoty folders

#### Proxy – Where It Starts

- A proxy is a piece of software (it could be hardware)
- It sits between one thing and another and behaves as the middleman
- Example
  - You are at your browser communicating with a web app
  - You decide you want a proxy sitting between your browser and the app
  - So, you start a proxy server running and then you tell your browser to send requests to the proxy
  - The proxy receives requests from the browser and forwards them to the web app
  - When responses come back, the proxy routes them to you

#### Proxy – Where It Starts



#### Proxy – Why Would You Do This?

- Because the proxy provides a service you want
  - Encryption of traffic
  - Anti-virus scanning
  - Keeping track of sites visited
  - Stopping you from reaching some sites
  - Giving you control over what goes on
  - Allowing you to see what is going on in the exchange
  - Providing services to make your job easier
- The proxy can make your life much simpler



#### **Getting Burp Suite**

- There are two versions
  - Professional, about \$300/year
  - Not so professional, free, and missing some cool stuff
- Download it from <a href="http://portswigger.net">http://portswigger.net</a>
- It's Java App, so you just download the jar file
- Put it somewhere convenient
  - /home/opt/BurpSuite or C:/opt/BurpSuite or whatever
- To start it, use
  - java –Xmx1024m –jar <path to the jar file>
  - The amount of memory can be lower or larger, but 256m is about the min

#### How to Proxy with Burp

• Start up Burp Suite

	Burp Suite Professional v1.5.21 - lice	ensed to Security Innovation [10 user license]	↑_□×
Burp Intruder Repeater Window Help			
Target Proxy Spider Scanner Intruder Repe	ater Sequencer Decoder Comparer Extende	er Options Alerts	
Site map Scope			
Filter: Hiding not found items; hiding CSS, image and	general binary content; hiding 4xx responses; hidir	ng empty folders	?
	Host Method URL	Params Status 🔺 Length MIME type Title	Comment Time reque
		_	
	Request Response		
	Raw Hex		
			Ê.
	2 < + > Type a search term		0 matchas
			offiaccies

#### How to Proxy with Burp

• Proxy -> Intercept



You might want to start with Intercept off, so click on it

#### How to Proxy with Burp

• Proxy -> Options

		Burp Suite Free Edition V1.5	
	Burp Intruder Repeater Window Help		
	Target Proxy Spider Scanner Intrude	r Repeater Sequencer Decoder C	omparer Options Alerts
	Intercept History Options		
	<ul> <li>Proxy Listeners</li> <li>Burp Proxy uses listeners to receive ind listeners as its proxy server.</li> </ul>	coming HTTP requests from your browser	. You will need to configure your b
	Add Running Interface	Invisible Redirect	Certificate Per-host
If running isr	't checked,		
check it.			

This is where your proxy listens. 8080 can be changed. Usually it listens on the system where it is running.

#### Setting Up Your Browser – Local Burp

- Firefox
  - Tools -> Options (Win) or Edit -> Preferences (Lin)
  - Advanced -> Connection -> Settings
  - Check Manual Proxy Settings - 23 **Connection Settings** Configure Proxies to Access the Internet No proxy – Use this proxy server ... Auto-detect proxy settings for this network Use system proxy settings Manual proxy configuration: 8080 🌲 HTTP Proxy: 127.0.0.1 Port: Change the port if desired Use this proxy server for all protocols SSL Proxy: 127.0.01 8080 🕀 Port: 127.0.0.1 TP Proxy: Port: 8080 🕀 SOCKS Host: 127.0.0.1 Port: 8080 🕀 SOCKS v4 SOCKS v5

#### Setting Up Your Browser – Local Burp

• IE

- Tools -> Internet Options -> Connections -> LAN Settings
- Configure Proxy Settings
- Check Manual Proxy Settings



#### Setting Up Your Browser – Local Burp

• Advanced tab, but the default is typically correct

Proxy Setti	ings			×
Servers				
	Туре	Proxy address to use		Port
	HTTP:	127.0.0.1	:	8080
	<u>S</u> ecure:	127.0.0.1	:	8080
	ETP:	127.0.0.1	:	8080
	So <u>c</u> ks:		:	
	🔽 <u>U</u> se the s	ame proxy server for all protocols		

#### **Testing Your Setup**

- Chromium and Safari left to the reader
- You are now set up.
- To test it, click on the Proxy -> History tab
- Then go to some URL in your browser

▼			Burp Suite Fre	e Edition v1.5	5			
Burp Intruder Repeater Window He	lp							
Target Proxy Spider Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Options	Alerts	
Intercept History Options								
Filter: Hiding CSS, image and general	binary co	ntent						
# 🔺 Host	Method	URL			Params	Modified	Status	Le
1 http://google.com	GET	1						
A	۲	18 X IV 193	<b>W</b> 2/8/232~1	z/~z/mx/x	V			

# The Setup

#### Simple form

#### and response

<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp	<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp				
http://127.0.0.1/cs476/sqli/form.html	http://127.0.0.1/csit.php?account=1234				
	<ul> <li>127.0.0.1/cs476/sqli/submit.php?account=1234</li> </ul>				
SI • Mail • System • water • NetDev • System • Movies •	SI • Mail • System • water • NetDev • System • Movies •				
Enter the account number 1994	select name, userid from accounts where account='1234'				
Enter the account number 1234 Submit	You are identified as				
	name userid				
	Joe B   joe				

#### Information in the History Tab

• First, there is a huge amount of information just in the History tab

15	http://127.0.0.1	GET	/cs476/sqli/			200	1451	HTML		Index of /cs476/sqlı		127.0.0.1	
16	http://127.0.0.1	GET	/cs476/sqli/form.html			200	555	HTML	html			127.0.0.1	
17	http://127.0.0.1	GET	/cs476/sqli/submit.php?account=	$\checkmark$		200	439	HTML	php			127.0.0.1	
													/ <b>&gt;</b>
Req	uest Response												
Raw	Headers Hex												
GET /c	s476/sqli/form.html HTTP/1	.1											
Host:	127.0.0.1 Marilla/5.0 (V11. Lin	N VOE EALEN	26 0) Cocke/20100101 Firefox/26 0										
Accep	t: text/html,application/xhtr	nl+xml,applic	ation/xml;g=0.9,*/*;g=0.8	>	— A	nyth	ing us	eful h	ere?			1	
Accep	Language: en-US,en;q=0	.5				-	-						
Accep	t-Encoding: gzip, deflate											ade	
Refere	r: http://127.0.0.1/cs476/sc	di/									~ Jas		
Conne	ction: keep-alive	114									atwe		
	·									ostt	110		
										neques			
										ITTP RCS			
									hat				
								is	the				
							17	nis					

# Request Headers

Request Response	
Raw Headers Hex	
Name	Value
GET	/cs476/sqli/ HTTP/1.1
Host	127.0.0.1
User-Agent	Mozilla/5.0 (X11; Linux x86_64; rv:26.0) Gecko/20100101 Firefox/26.0
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
DNT	1
Referer	http://127.0.0.1/cs476/
Connection	keep-alive + heads
	request r
	The



1 · · · ·		and the second	_	_					and the second sec	_		
16 http://127.0.0.1	GET	/cs476/sqli/form.html			200	555	HTML	html			127.0.0.1	
17 http://127.0.0.1	GET	/cs476/sqli/submit.php?account=	$\checkmark$		200	439	HTML	php			127.0.0.1	
•												
						_						
Request Response												
Raw Headers Hex HTML	Render											
HTTP/1.1 200 OK												
Date: Tue, 04 Feb 2014 12:21:18	GMT											
Server: Apache/2.2.25 (Unix) mo	d_ssl/2.2.25 C	)penSSL/1.0.1f DAV/2 PHP/5.5.8	_									
Last-Modified: Tue, 21 Jan 2014 1	9:49:34 GMT	•		_								
ETag: "b094-de-4f0804eb7ef80"					-> Δr	nvth	ing us	eful he	re?			
Accept-Ranges: bytes				/		iy ci i	ing us	crui ne				
Content-Length: 222												
Keep-Alive: timeout=5, max=10	)											
Connection: Keep-Alive												
Content-Type: text/html												
HTML												
<himl></himl>												
< BODA>									nse			
<form <="" formnome="geteeseunt" td=""><td>action - Icubr</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>aspu.</td><td></td><td></td><td></td></form>	action - Icubr								aspu.			
Enter the account number i	action="subn	xt" name="account">					5	-he l	Est			
<pre>cinput type="submit" yelue="\$u"</pre>	iput type= te bmit">	xt hame= account >						7110				
								\ ·				
· · · · · · · ·												
												-

# **Response Headers**

Request Response	
Raw Headers Hex HTML Render	
Name	Value
HTTP/1.1	200 OK
Date	Tue, 04 Feb 2014 12:21:18 GMT
Server	Apache/2.2.25 (Unix) mod_ssl/2.2.25 OpenSSL/1.0.1f DAV/2 PHP/5.5.8
Last-Modified	Tue, 21 Jan 2014 19:49:34 GMT
ETag	"b094-de-4f0804eb7ef80"
Accept-Ranges	bytes
Content-Length	222 aders
Keep-Alive	timeout=5, max=100
Connection	Keep-Alive
Content-Type	text/html

## Submit Request Params

Request	Response	
Raw Para	ams Headers	Hex
GET request	to /cs476/sqli/	submit.php
Туре	Name	Value
URL	account	1234

## Popup Menu Options

- Right-click
- This how you can pass a particular URL to one of the Burp Suite tool.
  - Repeater
  - Spider
  - Active Scan
  - Passive Scan
  - Intruder

Add to scope	
Spider from here	
Do an active scan	
Do a passive scan	
Send to Intruder	Ctrl+I
Send to Repeater	Ctrl+R
Send to Sequencer	
Send to Comparer (request)	
Send to Comparer (response)	
Show response in browser	
Request in browser	•
Generate Script	
Engagement tools	•
Show new history window	
Add comment	
Highlight	•
Delete item	
Clear history	
Copy JRL	
Convinte	

## A Live Example

## Homework 3

- http://www.hackthissite.org
- Go there and register
  - The passwords are a pain
  - Start with the basic mission and move on up
  - You should be able to get to through at least 3 of the Realistic Missions
  - We are going to talk about some of this next time

## Homework 4

• The topic is BurpSuite