Ivan Marchany CYB660 Penetration Testing Dr. Knapp

Tool Demonstration: BurpSuite

Introduction: BurpSuite is a web penetration testing tool that can be used to intercept web traffic and find vulnerabilities. This tool allows you to intercept data being sent between your browser and your web application. The data that can be intercepted can include such as usernames and passwords. In this demonstration, I'll be going through the steps of getting started using the interface and test a webpage. The goal of this assignment is to show how easy and powerful BurpSuite is on intercepting credentials. As a Web Penetration Tester is important to test your client web server to see if there are malicious code on their web pages.

Table of Contents:

Introduction	1
Setting up BurpSuite	2
Using Burp Suite GUI	3
Intercepting traffic on a web page	6
Brute Force Attack using DVWA	9
References	16



Setting up BurpSuite:

If you have Kali Linux version 2 and up, BurpSuite should be included in your tool library. If you are using Ubuntu, you can download it using the following steps:

- a) Make sure you have java updated. Use the following command: sudo apt-get install openjdk-8-jre
- b) Click this link to download Burp Suite for Linux and Windows: <u>https://portswigger.net/burp/communitydownload</u>
- c) Once is downloaded on your computer, enter the following command: sudo bash path/to/download/file
- d) Then the BurpSuite wizard should appear and follow the steps to install it





Burp Suite Community Released 29 June 2018 v1.7.35 Release notes	Edition v1.7.35 Latest Stable	
Download		
E Download for Windows (64-bit)	View Checksums	Download
🕹 Download plain JAR file	View Checksums	Download
	Other Platforms \checkmark	

Using BurpSuite GUI:

The interface contains several options you can use while you are using the tool. As a beginner, is a better focus on the main tabs of the interface:



a) Use the temporary project since I'm using the free version

			Burp Suite Community Ed	ition v1.7.35	
?	Welcome to Burp Suite Community Edition. Use the options below to create or open a project. Note: Disk-based projects are only supported on Burp Suite Professional.				
	 Temporary project 				
	New project on disk	File: Name:			Choose file
	Open existing project		Name	File	
		File:	Pause Spider and Scanner		Choose file
					Cancel Next

b) Go to your browser and set your proxy to manual using the default settings listening to port 8080

	Preferences - Mozilla Firefox	•••
🗱 Preferenc	ices × +	
Firefox	about:preferences#advanced	+ ☆ ⊠ ≡
🛅 Most Visited	d~ 👖 Offensive Security 🌂 Kali Linux 🌂 Kali Docs 🌂 Kali Tools 🄅 Exploit-DB 📡 Aircrack-ng 🚺 Kali	Forums »
	Connection Settings	×
 ID General Q Search ID Conte Applic ↔ Privact G Securi G Sync Advan 	Configure Proxies to Access the Internet No proxy Auto-detect proxy settings for this network Use system proxy settings Manual proxy configuration: HTTP Proxy: 127.0.0.1 Use this proxy server for all protocols SSL Proxy: Port: ETP Proxy: Port: SOCKS Host: Port:	
	SOC <u>K</u> S v4 • SOCKS <u>v</u> 5 <u>N</u> o Proxy for:	bw
	localhost, 127.0.0.1	S
	Help Cancel OK	

c) Once is set, return to BurpSuite, go to your options on your interface to validate your proxy configuration

?	Proxy Liste	eners					
٢	Burp Proxy us	ses listeners to	o receive incoming HT	TP requests fro	om your browser. ו	You will need to configure your br	owser to use one of the listeners as its proxy server.
	Add	Running	Interface	Invisible	Redirect	Certificate	
		2	127.0.0.1:8080			Per-host	
	Edit						
	Remove						•

Intercepting traffic on a web page:

a) Go to the Proxy tab and under Proxy, go to Intercept tab and switch Intercept on to off. Then go to the browser and type in the URL: example.com



b) Return to the interface and then click on the HTTP history under Proxy and you should get information from example.com

Target Proxy Spider Scanner In	ntruder Re	epeater	Sequencer	Decoder	Compare	er Exter	nder P	Project options	User option	ns Alerts		
Intercept HTTP history WebSockets history Options												
Filter: Hiding CSS, image and general bina	ary content											
# 🔺 Host	Method	URL				Params	Edited	d Status	Length	MIME type	Extension	Title
1 http://detectportal.firefox.com	GET	/succe	ss.txt					200	379	text	txt	
2 http://detectportal firefox.com	GET	/succe	ss txt					200	379	text	txt	
3 http://example.com	GET	/favico	n ico					404	1603	HTMI	ico	Example Domain
4 http://example.com	GET	/favico	n ico					404	1603	нтмі	ico	Example Domain
•											,	
							_					
Request Response												
Raw Headers Hex												
GET /favicon ico HTTP/1 1												
Sch / Tarlon Lto miny Li												
User-Ademit Mozilla/5.0 (X11: Linux x86 64: rv:52.0) Gecko/20100101 Firefox/52.0												
Accept: */*	Accept: */*											
Accept-Language: en-US,en;g=0.5												
Accept-Encoding: gzip, deflate	ccept-Encoding: gzip, deflate											
Connection: close												

- c) Here it shows a lot of information about the web page such as the URL, method and raw information that contains your Operating System. This is a basic example of how you can retrieve information about a web page which can be HTTP or HTTPS.
- d) Now click the Intercept tab under Proxy and turn on the Intercept to test a web page that can be intercepted.

Target P	roxy Spider	Scanner	Intruder	Repeater
Intercept	HTTP history	WebSocke	ts history	Options
Forward	d C	Drop	Intercep	t is on
Raw Hex	c			

e) Go to Firefox and enter in the URL: youtube.com



Connecting	× +
(julia) youtube.com	
📷 Most Visited 🗸 👖 C	ffensive Securit

- f) The reason the page is not loading is that the website is being intercepted by the Burp Suite.
- g) If you click the Forward bottom, the web page will continue to load until it reaches to the web page.

Forward	Drop	Intercept is on	Action		
Raw Params	Headers Hex				
POST /GTSGIAG3 H Host: ocsp.pki.g User-Agent: Mozi Accept: text/htm Accept-Language: Accept-Encoding: Content-Length: Content-Type: ap Connection: clos	TTP/1.1 lla/5.0 (X11; Lir l,application/xh1 en-US,en;q=0.5 gzip, deflate 75 plication/ocsp-re- e	nux x86_64; rv: tml+xml,applica equest	:52.0) Gecko/201001(ation/xml;q=0.9,*/*	01 Firefox/52. ;q=0.8	0
010G0E0C0A0	Ω∴+₀⊳⊴ơ"∴⊵ზ ₿cb2 (00500u00⊴J ⊳ 0l0	⊵ౖౖౖౖౖౖౖౖౖౖౖౖౖౖౖౖౖౖౖౖౖౖౖౖౖౖౖౖౖౖౖౖౖౖౖౖ	⊴√K20r\$0i	
			 YouTube ♦ ● https:// Most Visited ▼ 	× www.youtube.c	+ com curity 🌂 Kali Lir
			🔲 🕒 YouTu	ıbe	Search
			Power on	TV and watch STARZ® w	n new epi rith YouTu
			TRY IT NOW	extra charge. Power © 201	8 Starz Entertainment, LLC

h) At this point, you have successfully intercepted the web traffic from the user which allows you to view additional information that may be useful for manipulating or exploiting vulnerabilities.

This is how you use BurpSuite as a beginner to intercept traffic on web pages. If you are a web penetration tester, this tool can be useful to test web applications on your target or the company that you are auditing to find vulnerabilities that are critical to their web server. This tool can go further in details of what you can do with the information you obtain from the web page. I'll be using this tool for my demo with some tricks that this tool can do. I plan to intercept DVWA web server and try to brute force it.

Brute Force Attack using DVWA

Many hackers use brute force attacks on system logins that passwords are complex. For the ones that are not, they use a wordlist that contains weak and default passwords. In this tool demonstration, I'll be showing how to Brute force DVWA using BurpSuite.

I'll be using SamuraiWTF because DVWA and BurpSuite are already installed and configured. To install SamuraiWTF, go to: https://sourceforge.net/projects/samurai/files/SamuraiWTF%203.0%20Branch/ and download the latest

https://sourceforge.net/projects/samurai/files/Samurai/WTF%203.0%20Branch/ and download the latest version of Samurai-WTF as an iso. (If you have questions of how to install it on your VM, speak with me and I will give you guidance)

Once you are ready to use SamuraiWTF. Open Firefox and enter in the URL: dwva/login.php and you should see the login page of DVWA. Also, if you are already running BurpSuite, it already caught URL information on your Target tab of the interface. Login to DVWA, the username is **admin** and password is **password**.





Home	Welcome to Damn Vulnerable Web App!
Instructions Setup	Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.
Brute Force	WARNING!
Command Execution CSRF	Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing <u>XAMPP</u> onto a local machine inside your LAN which is used solely for testing.
Insecure CAPTCHA	Disclaimer
SQL Injection	We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to
SQL Injection (Blind)	prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.
Upload	General Instructions
XSS reflected XSS stored	The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.
DVWA Security	
PHP Info About	You have logged in as 'admin'
Logout	

Now you are logged in as admin. Go to DVWA Security and make sure the security level is low which it should be set to low already. Now, let's go to Brute Force.

Home	Vulnerability: Brute Force
Instructions	Login
Setup	Username:
Brute Force	Password:
Command Execution	
CSRF	Login
Insecure CAPTCHA	

In here, you will have to make up a username and password for Brute Forcing. Now, go back to BurpSuite and turn to Intercept on to capture the login. Enter the username **admin**, for password enter **password** and click login.

Target Brown Spider Scanner Intruder Reprater Sequencer Decoder Comparer Extender Options Alerts CO2 Intercest HTTP history WebSockets history Options Request to http://dwails0.1027.42.84.21 Forward Drop Intercept is on Action	Damn Vulnerable Web App ① × ← → × ✿ ③ ♪	+ ✓ dwwa/vulnerabilities/brute/ ··· ♥ 1 date. An update is required to stay secure. Update Now
Ram Params Headers Hex ET /vulnerabilities/brute//username=admin&password&Login=Login HTTP/1.1 bost: dva ker-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:59.0) Gecko/20100101 Firefox/59.0 ccept: Language: en-US,en;q=0.5 ccept:-Language: en-US,en;q=0.5 ccept:-Encoding; gzip, deflate #ferer: http://dva/vulnerabilities/brute/ sofice: PHPSESDDevcsgq6feceSdinom8mjk2jpt1; security=low onnection: close bgrade-Insecure-Requests: 1	Home Instructions Setup Bruti: Force Command Execution CSRF Insecure CAPTCHA	Vulnerability: Brute Force

Now look both and see that BurpSuite has successfully intercepted the Brute Force Credentials and you notice that the DVWA web page is still loading the page. Now to Action tab and send it to the Intruder.

Request to http://dvwa:80 [127.42.84.2]	
Forward Drop Intercept is on Action)
RawParamsHeadersHexSend to Spide Do an active sJET /vulnerabilities/brute/?username=admin&Send to Intruedost:dvwaSend to Intruelost:dvwaSend to RepeJser-Agent:Mozilla/5.0 (X11; Ubuntu; LinuxAccept:text/html,application/xhtml+xml,appAccept-Language:en-US,en;q=0.5Accept-Encoding:gzip, deflateRequest in brBlazer - AMF1Blazer - AMF1Blazer - AMF2Donnection:close	er Scan der Ctrl+1 ater Ctrl+R encer Darer der owser Festing XML Export e/Disable Security Manager

Then go to the Intruder tab and then click Positions

Target	Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Options	Alerts	CO2		
1 ×	2 ×]												
Target	Position	s Payl	oads Opt	ions										
P Co as	Payload Positions Start attack Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.													
At	tack type:	Sniper											•	
G H U A A R C C U	ET /vuli ost: dvi ser-Age ccept: ccept-L ccept-E eferer: ookie: I onnecti pgrade-	nerabil wa nt: Moz text/ht anguage ncoding http:/ PHPSESS on: clo Insecur	ities/br :illa/5.0 :ml,appli : en-US, : gzip, : gzip, //dvwa/vu SID= <mark>Svcs(</mark> >se re-Reques	rute/?us 0 (X11;) ication/: ,en;q=0. deflate ulnerabi gq86fec9 sts: 1	ername= <mark>5</mark> a Ubuntu; L Khtml+xml 5 Lities/br 5dinom8mj	dmin§&pass inux i686; ,applicati ute/ <mark>k2jpt1§</mark> ; s	sword= <mark>Spa</mark> rv:59.0 on/xml;c security=	assword§&L 0) Gecko/2 1=0.9,*/*; = <mark>§low§</mark>	ogin= <mark>§Lo</mark> 0100101 q=0.8	gin§ HTT Firefox∕	P/1.1 759.0			Add § Clear § Auto § Refresh

The intruder allows you to edit the parameters of the request. While you edit the parameters, you can manipulate it and then get the results you are looking for. What is highlighted are all the payloads from the request. The payloads that need to be highlighted only are the username and the password. The first

thing you do is click Clear \$ to remove what is highlighted. Then highlight the payloads which are admin and password and manually add them one by one.



Now they are highlighted, the request is ready for the next step. Make sure you change the attack type to Cluster bomb because you are using two values for the attack which is the username and password. Once is set, go to the Payloads tab.

Tar	jet Positions	Payloads	Options		
?	Payload Se You can define payload types	ts e one or mor are available	e payload se for each pa	ts. The number of payl yload set, and each pay	pad sets depends on the attack type defined in the Positions tab. Various vload type can be customized in different ways.
	Payload set:	1		Payload count:	5
	Payload type:	Simple list		Request count:	0
?	Payload Op This payload t Paste	otions [Sin ype lets you admin administrate root	nple list] configure a s or	simple list of strings th	at are used as payloads.
	Remove Clear	test userl			▶
	Add]
	Add from list	(Pro vers	ion only]	7	

In this tab, you will set your payloads using set 1 and 2. Set 1 will be for your username. You will use the Simple list and under payload options, you can add or load a simple list of usernames. For this demonstration. I added 5 common usernames. Now switch the payload set to 2.

Tar	get Po	sitions	Payloads	Options			
?	Paylo You car	ad Set	s	e pavload s	ets. Th	e number of pavl	oad sets depends on the attack type defined in the Positions tab. Various
	payload	types a	are available	for each p	ayload	set, and each pa	yload type can be customized in different ways.
	Payload	d set: (2		V	Payload count:	6
	Payload	type: (Simple list		V	Request count:	30
?	Paylo This pa	ad Op yload ty	tions [Sim pe lets you admin	nple list] configure a	simple	list of strings th	at are used as payloads.
	Load		administrato root test	or			
	Rem	ove	userl password				•
	Clea	ar					
	Ad	d]
	Add fr	om list	(Pro versi	ion only]		1	

In payload set 2, you will add the password list. You can load them from a wordlist like rockyou as an example. For this demonstration, I added 6 common passwords manually. Now that both payloads are set, you can click the intruder tab on the very top left of your interface and start the attack. There will be a popup of Burp Intruder that the attack will be slow since I'm using the free version. Just click ok to continue.

50

Intruder attack 2

Results Target Positions Payloads Options

Filter:	Showing	all	items

Attack Save Columns

Filter: Showing all items								?
Request 🔺	Payload1	Payload2	Status	Error	Timeout	Length	Comment	
0			200			5086		
1	admin	admin	200			5035		
2	administrator	admin	200			5035		
3	root	admin	200			5035		
4	test	admin	200			5035		
5	userl	admin	200			5035		
6	admin	administrator	200			5035		
7	administrator	administrator	200			5035		
8	root	administrator	200			5035		
9	test	administrator	200			5035		
10	userl	administrator	200			5035		
11	admin	root	200			5035		
12	administrator	root	200			5035		
13	root	root	200			5035		
14	test	root	200			5035		
15	userl	root	200			5035		
16	admin	test	200			5035		
17	administrator	test	200			5035		
18	root	test	200			5035		
19	test	test	200			5035		
20	userl	test	200			5035		
21	admin	userl	200			5035		
22	administrator	userl	200			5035		
23	root	userl	200			5035		
24	test	userl	200			5035		
25	userl	userl	200			5035 🖌		
26	admin	password	200			5086		
27	administrator	password	200			5035		
28	root	password	200			5035		
29	test	password	200			5035		
30	userl	password	200			5035		
Request Response								
Raw Par	rams Headers Hex							
GET /vuln	erabilities/brute/?use	nname=admin&password=	asswords	Login=L	nain HT	TP/1 1		
Upot, dur			00000000	Login-L	ogin m	117/111		5
Hose Ares	a . Marilla/E O (Milia)	humbur Linux icoc	FO 0) C-	-lie (DOI)		i nafau (Er		
User-Agen	τ: Mozilla/5.0 (XII; ι	buntu; Linux 1686; rv	:59.0) Ge	CK0/2010	JOIOI H	iretox/59	9.0	
Accept: t	ext/html,application/>	html+xml,application/	kml;q=0.9	,*/*;q=0	0.8			
Accept-La	nguage: en-US,en;q=0.5	5						
Accept-En	coding: gzip, deflate							
Referer:	http://dvwa/vulnerabil	.ities/brute/						
Cookie: P	HPSESSID=vcsqq86fec950	linom8mik2ipt1: securi	tv=low					
Connectio	n: close	,,,,	-,					
Upgnede T	n. ccose							
upgrade-1	nsecure-Requests: I							
? <	+ > Type a search	h term						0 matches
Finished								
_								

This page displays the results of the Brute Force. Look closely at the length of each attempt. Most of them are 5035 and some of them have different length, but there is one that has a unique length. The attempts of 5086 are most likely the correct username and password because the length is unique from others. To prove the credentials is correct, you can test it out on your target and see if it works.

Vulnerability: Brute Force

Login	
Username:	
admin	
Password:	
Login	
Welcome to the password protected area admin	

This test shows that the credentials you typed in the have logged in successfully.

Now that the attack is performed, and we saw the correct password login, this is how easy you can brute force a web page login. If I was using Google Hacking Database and Shodan to find security cameras or servers that are out there in the public with default passwords, I could probably brute force easily using BurpSuite. Although, if you get a traceback, you can go to jail for breaking in. This tool is very powerful and friendly to use. You must have a mindset of what are you trying to accomplish. Using it properly, you will gain access to the system that you want to get in. As a Web Penetration Tester is important to test Brute Force on your client's web page to see if their password is in a word list like rockyou. If so, you must report it to your client and provide recommendations of security best practice to make sure your web server or web page is not compromised.

References:

Bisht, S. (August 27, 2017) how to install burp suite in Linux/Ubuntu 16.04. Bitforestinfo

HackerSploit (February 26, 2018) Web App Penetration Testing - #1 - Setting Up Burp Suite. YouTube

(February 16, 2014) Burp Suite. Kali Tools

HackerSploit (March 19, 2018) Web App Penetration Testing - #3 - Brute Force Attacks With Burp Suite. *YouTube*