

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:

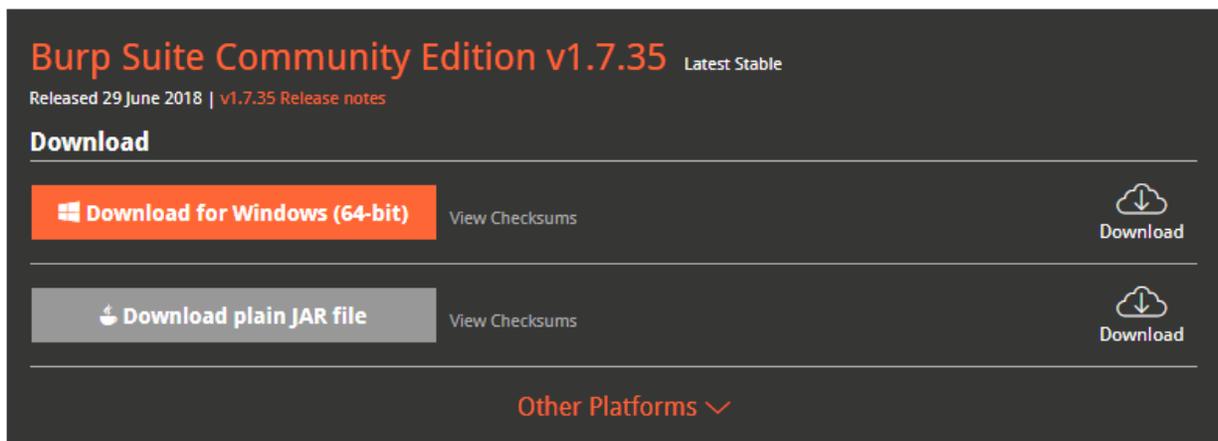
Introduction - - - - -	1
Setting up BurpSuite - - - - -	2
Using Burp Suite GUI - - - - -	3
Intercepting traffic on a web page - - - - -	6
Brute Force Attack using DVWA - - - - -	9
References - - - - -	16



Setting up BurpSuite:

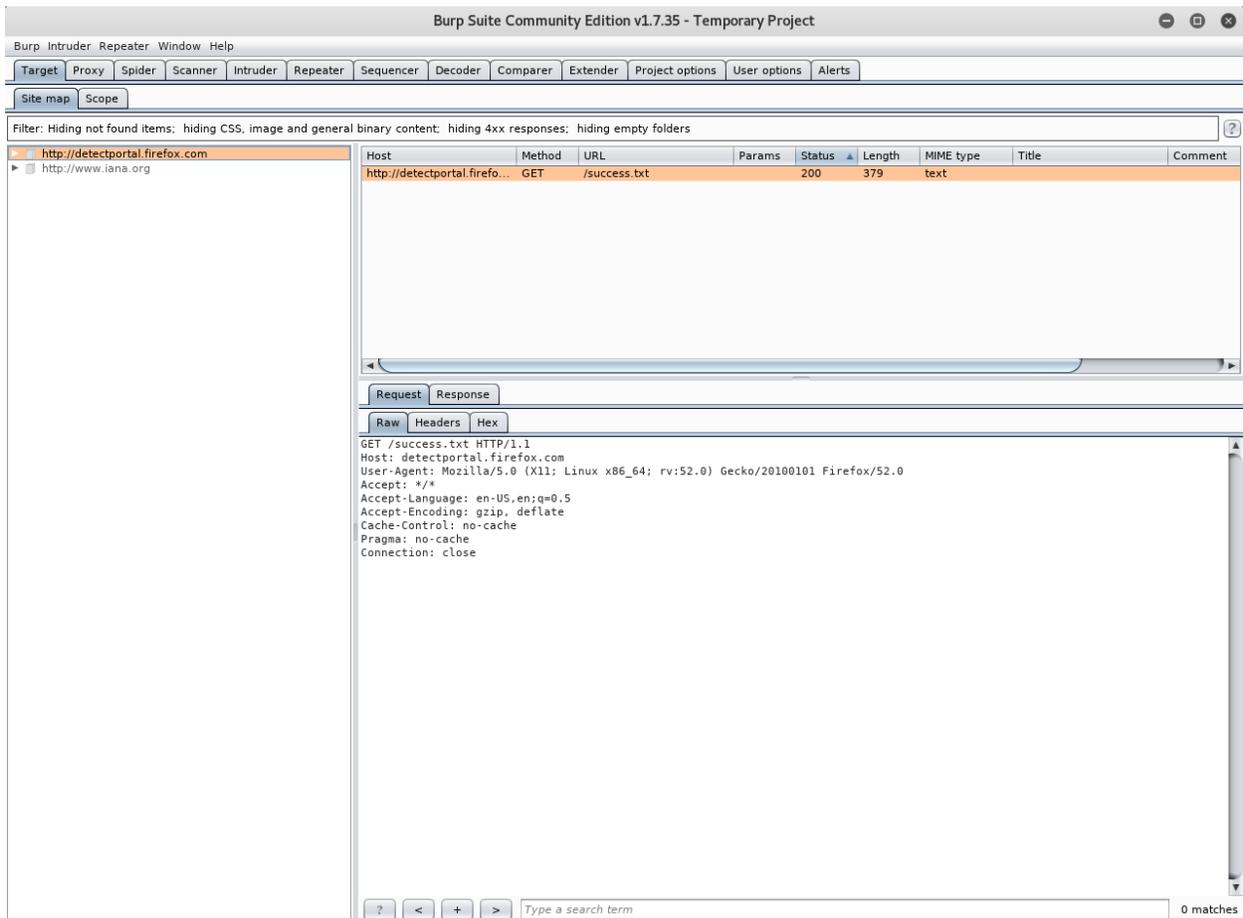
If you have Kali Linux version 2 and up, BurpSuite should be included in your tool library. If you are using Ubuntu, you can download it using the following steps:

- 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:
<https://portswigger.net/burp/communitydownload>
- 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

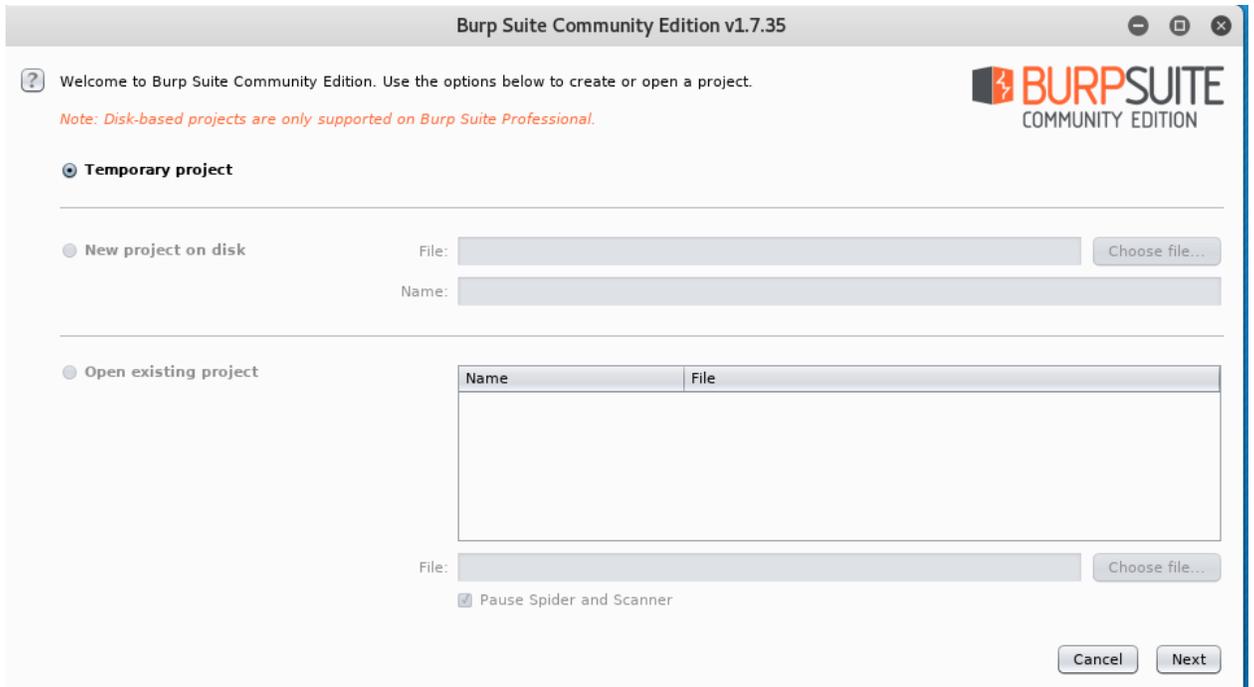


Using BurpSuite GUI:

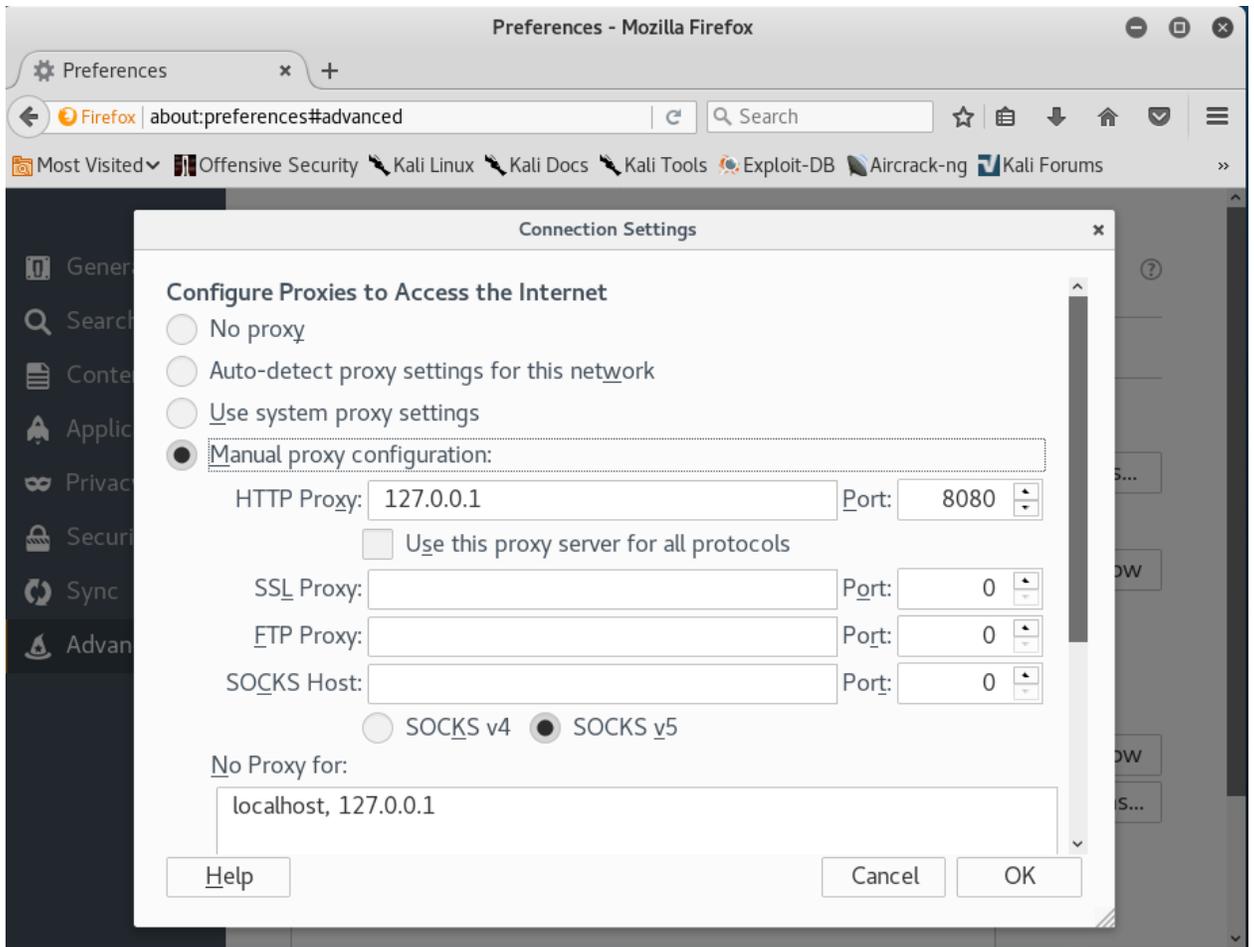
The interface contains several options you can use while you are using the tool. As a beginner, is a better focus on the main tabs of the interface:



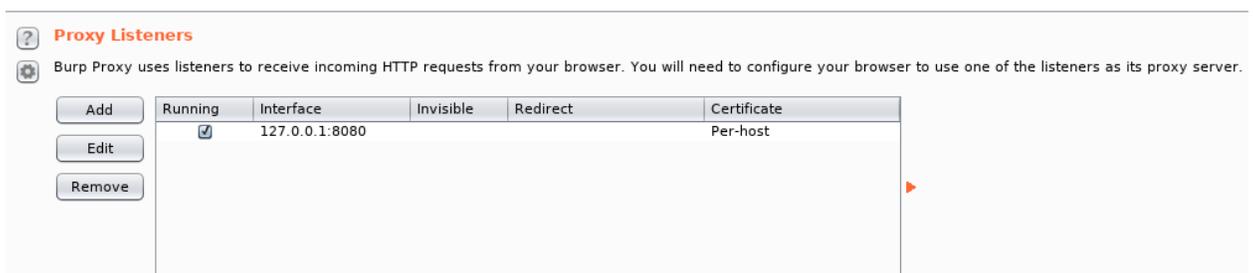
- a) Use the temporary project since I'm using the free version



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

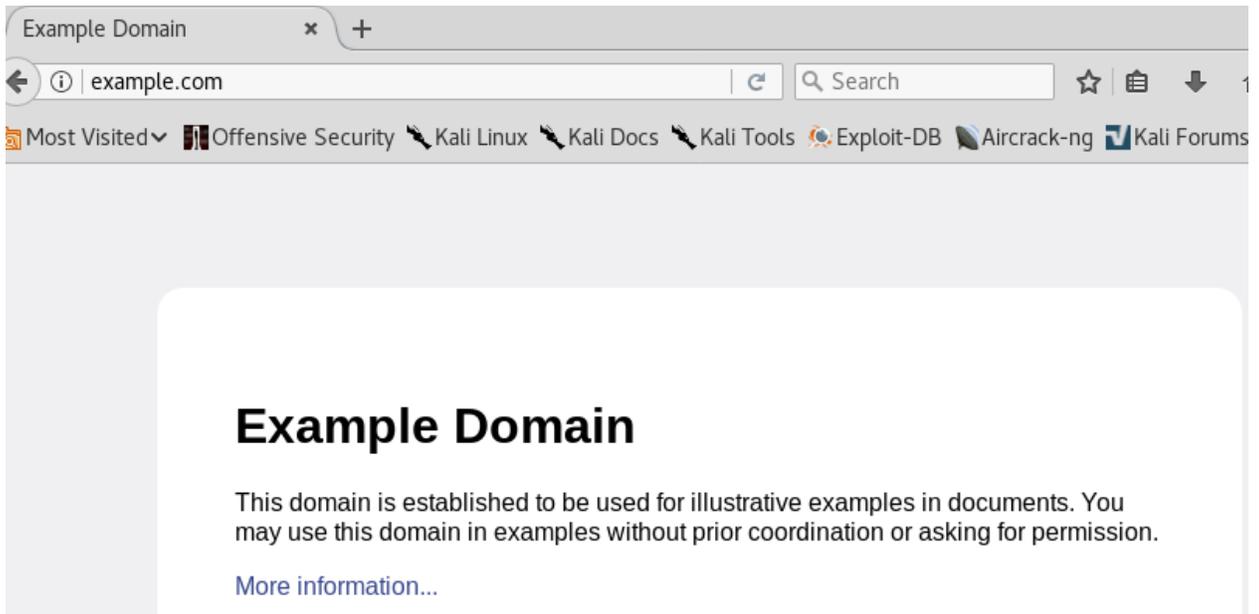


- c) Once is set, return to BurpSuite, go to your options on your interface to validate your proxy configuration

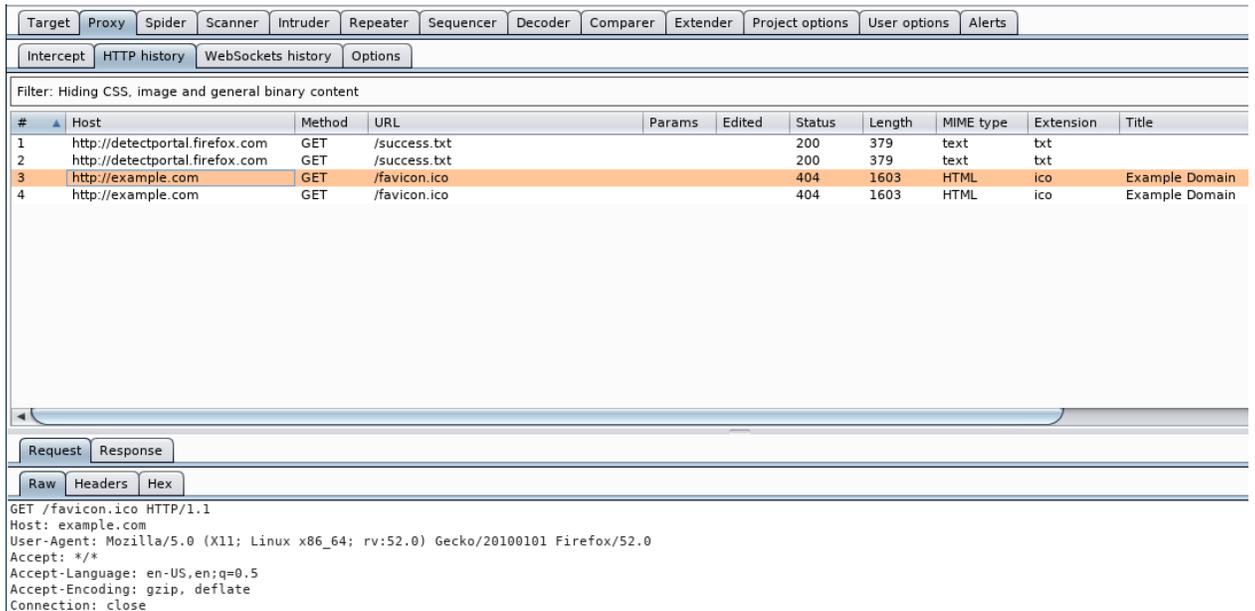


Intercepting traffic on a web page:

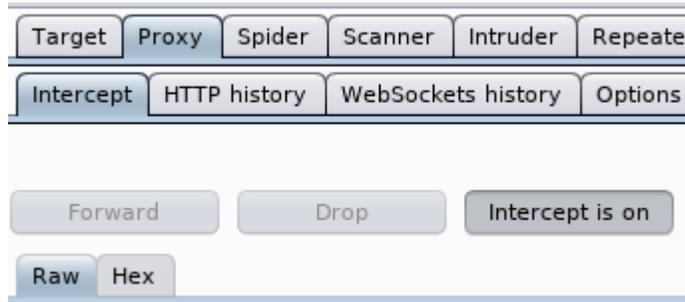
- a) Go to the Proxy tab and under Proxy, go to Intercept tab and switch Intercept on to off. Then go to the browser and type in the URL: example.com



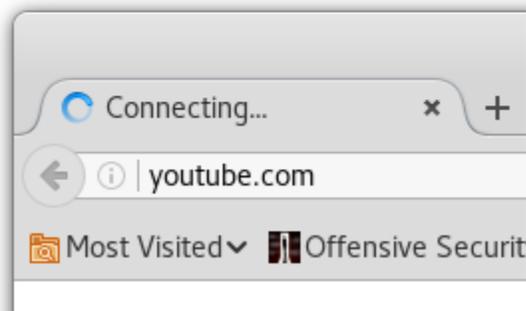
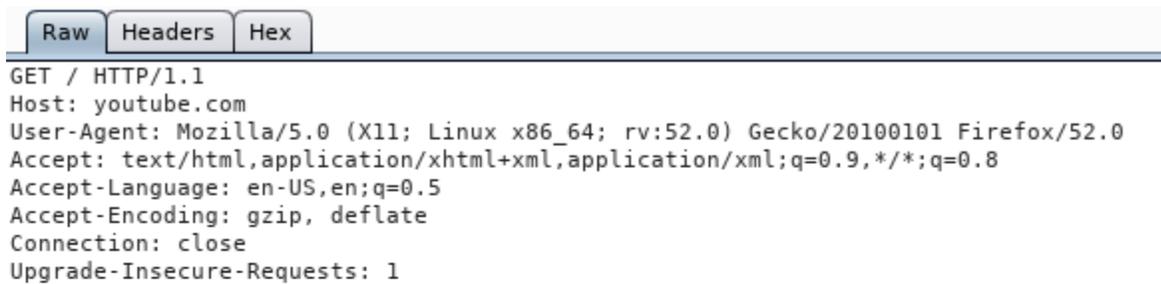
- b) Return to the interface and then click on the HTTP history under Proxy and you should get information from example.com



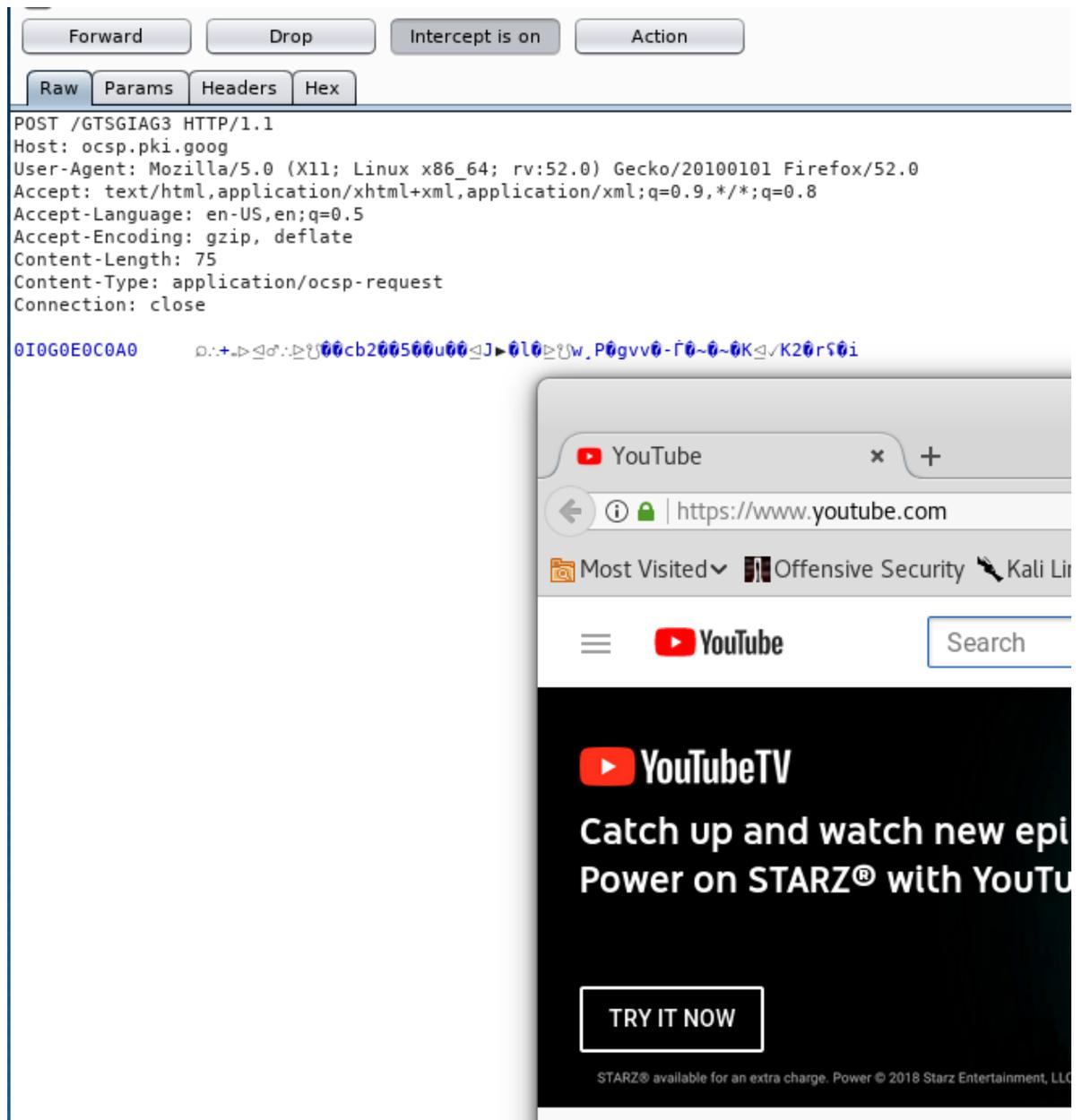
- c) Here it shows a lot of information about the web page such as the URL, method and raw information that contains your Operating System. This is a basic example of how you can retrieve information about a web page which can be HTTP or HTTPS.
- d) Now click the Intercept tab under Proxy and turn on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



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



- 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 button, the web page will continue to load until it reaches to the web page.



- 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 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**.



Username

Password

 This connection is not secure. Logins entered here could be compromised. [Learn More](#)



- Home
- Instructions
- Setup

- Brute Force
- Command Execution
- CSRF
- Insecure CAPTCHA
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored

- DVWA Security
- PHP Info
- About

- Logout

Welcome to Damn Vulnerable Web App!

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.

WARNING!

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 [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

Disclaimer

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 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.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'

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
- Instructions
- Setup

- Brute Force
- Command Execution
- CSRF
- Insecure CAPTCHA

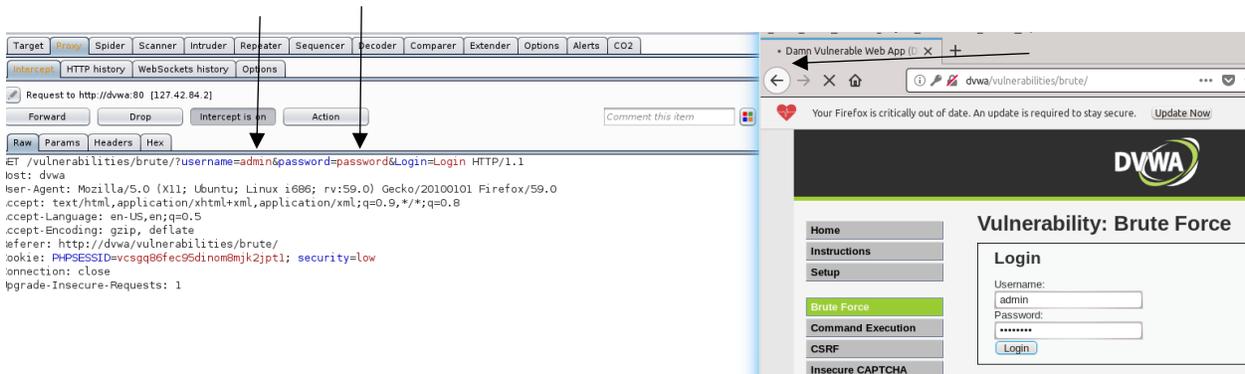
Vulnerability: Brute Force

Login

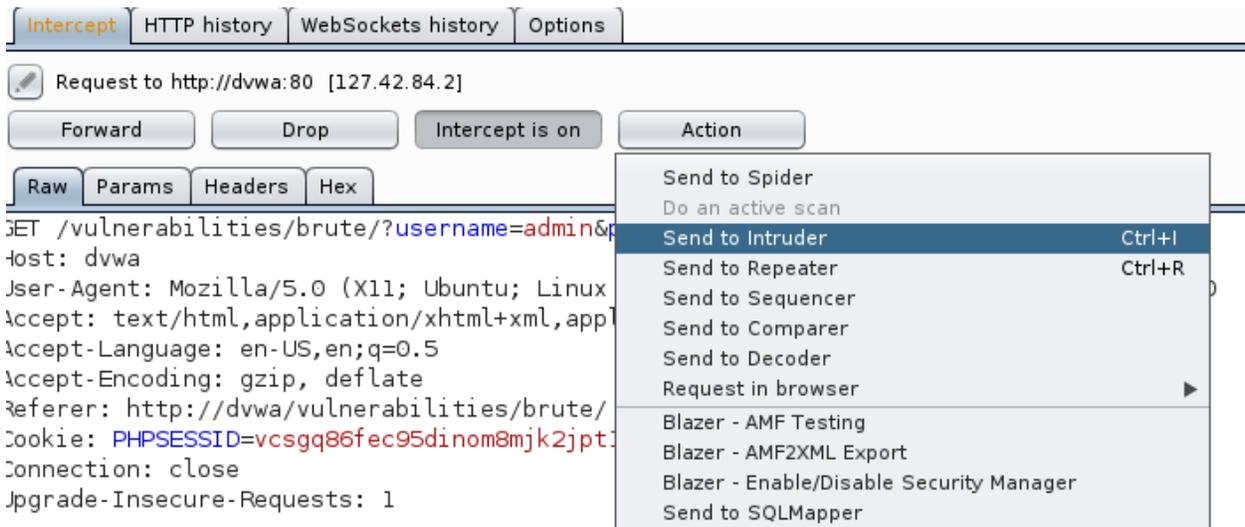
Username:

Password:

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.



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.



Then go to the Intruder tab and then click Positions

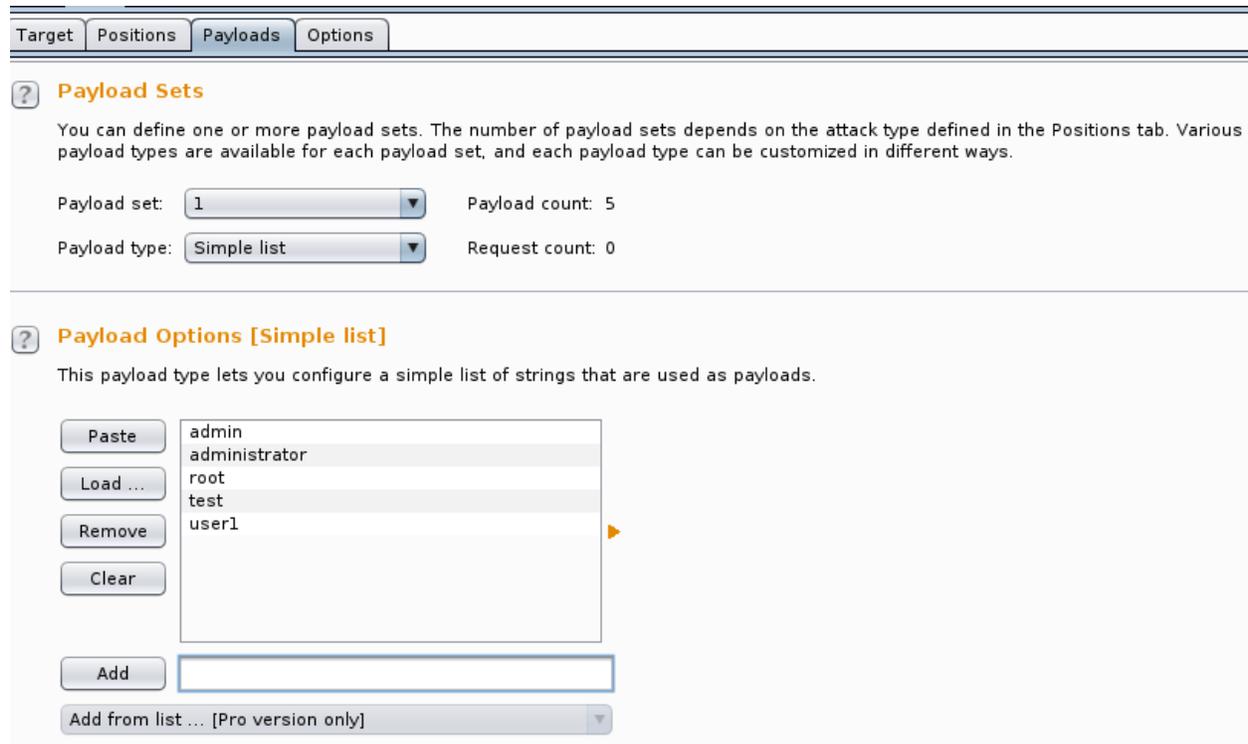


The intruder allows you to edit the parameters of the request. While you edit the parameters, you can manipulate it and then get the results you are looking for. What is highlighted are all the payloads from the request. The payloads that need to be highlighted only are the username and the password.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



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.

Target Positions **Payloads** Options

? **Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: Payload count: 6

Payload type: Request count: 30

? **Payload Options [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear

admin
administrator
root
test
user1
password

Add

Add from list ... [Pro version only]

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.

Intruder attack 2

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			200	<input type="checkbox"/>	<input type="checkbox"/>	5086	
1	admin	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
2	administrator	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
3	root	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
4	test	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
5	user1	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
6	admin	administrator	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
7	administrator	administrator	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
8	root	administrator	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
9	test	administrator	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
10	user1	administrator	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
11	admin	root	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
12	administrator	root	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
13	root	root	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
14	test	root	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
15	user1	root	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
16	admin	test	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
17	administrator	test	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
18	root	test	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
19	test	test	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
20	user1	test	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
21	admin	user1	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
22	administrator	user1	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
23	root	user1	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
24	test	user1	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
25	user1	user1	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
26	admin	password	200	<input type="checkbox"/>	<input type="checkbox"/>	5086	
27	administrator	password	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
28	root	password	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
29	test	password	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	
30	user1	password	200	<input type="checkbox"/>	<input type="checkbox"/>	5035	

Request Response

Raw Params Headers Hex

```
GET /vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.1
Host: dvwa
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:59.0) Gecko/20100101 Firefox/59.0
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
Referer: http://dvwa/vulnerabilities/brute/
Cookie: PHPSESSID=vcsqg86fec95dinom8mjk2jpt1; security=low
Connection: close
Upgrade-Insecure-Requests: 1
```

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:

Password:

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*