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:

Setting up BurpSuite:

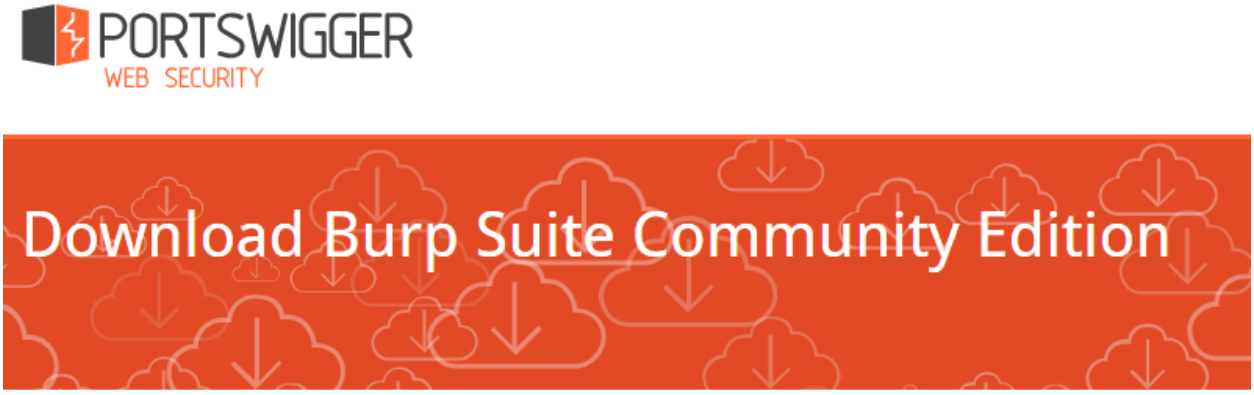
If you have Kali Linux version 2 and up, BurpSuite should be included in your tool library. If you are using Ubuntu, you can download it using the following steps:

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

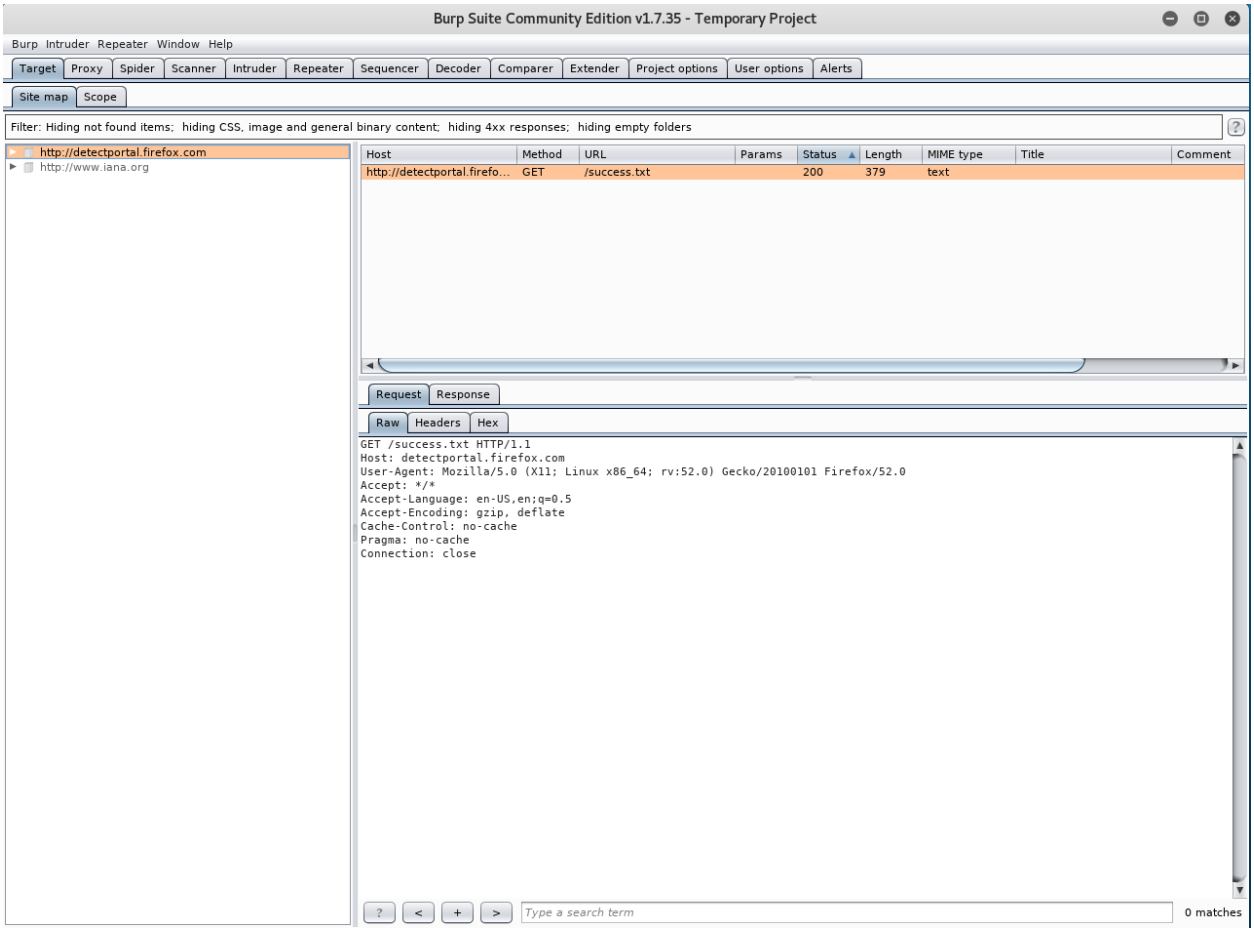
c) Once is downloaded on your computer, enter the following command: sudo bash path/to/download/file

d) Then the BurpSuite wizard should appear and follow the steps to install it

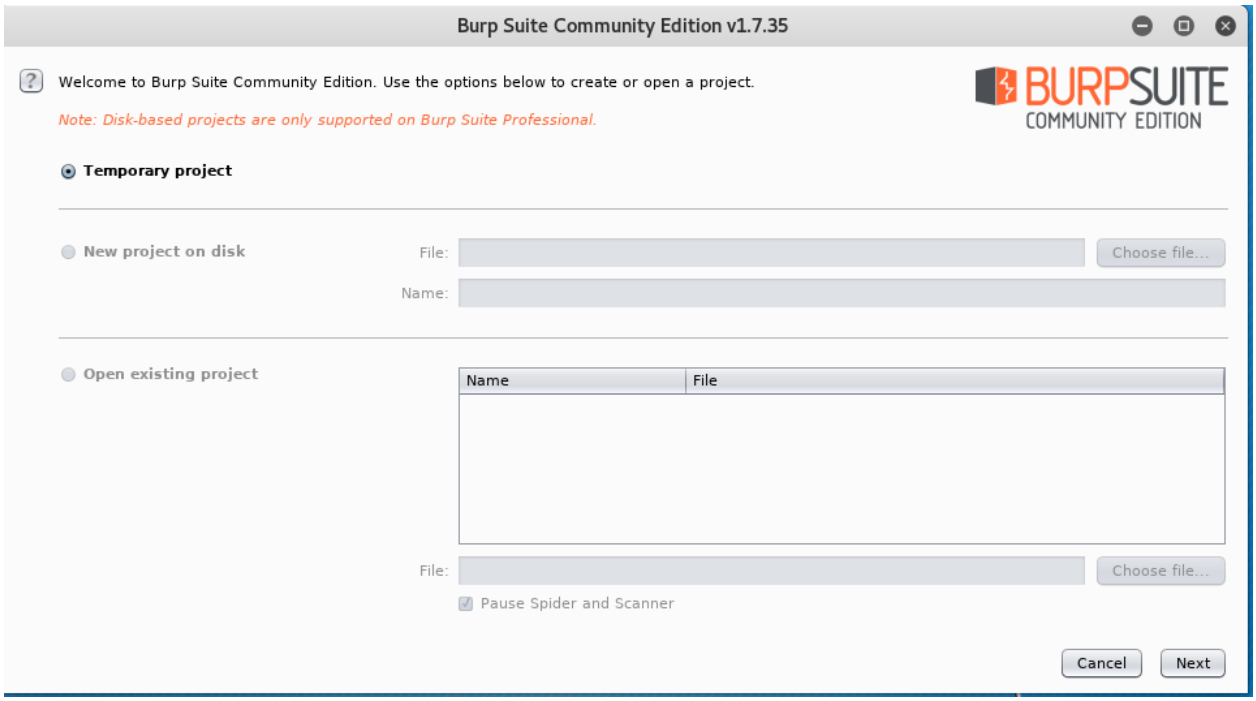


Using BurpSuite GUI:

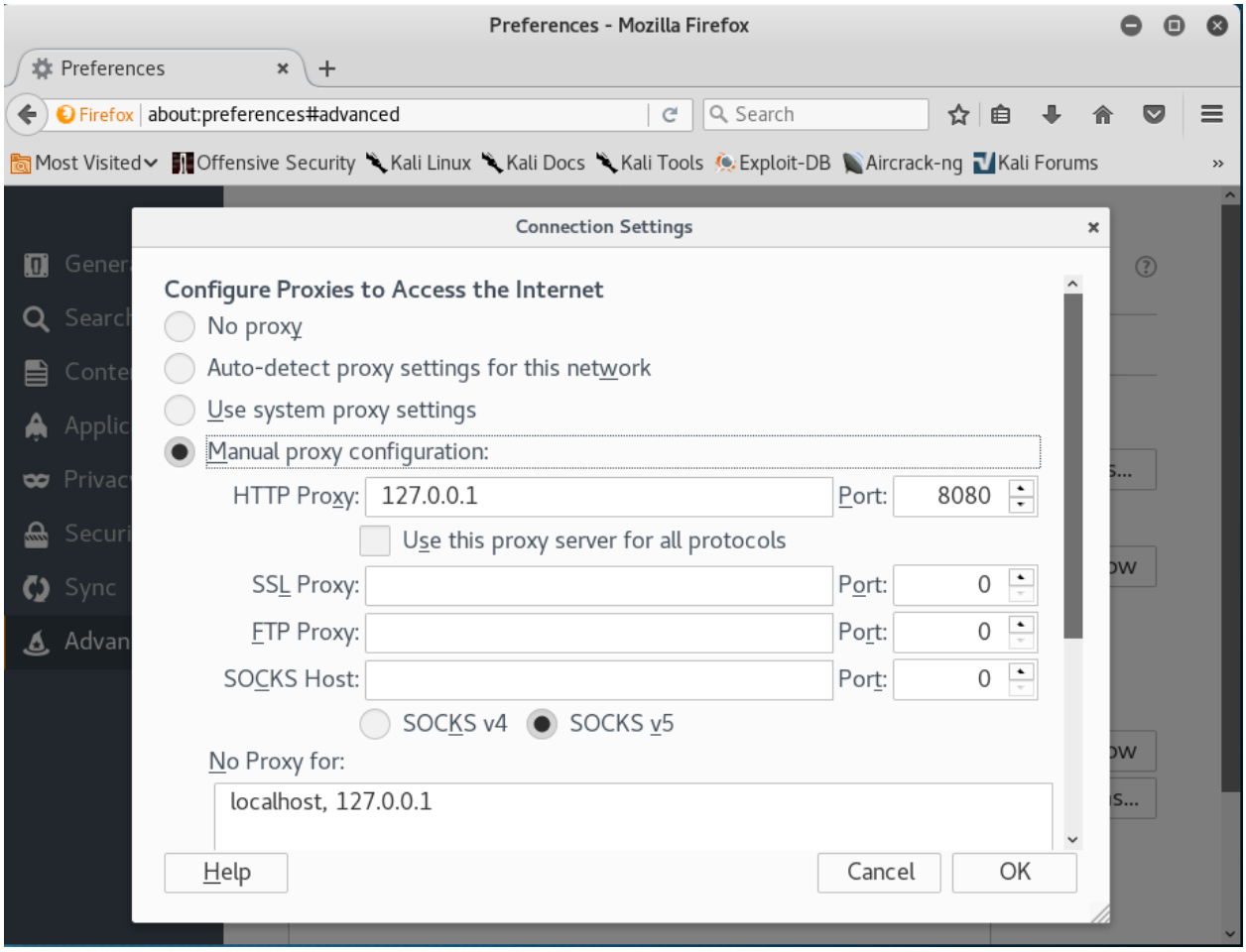
The interface contains several options you can use while you are using the tool. As a beginner, is a better focus on the main tabs of the interface:



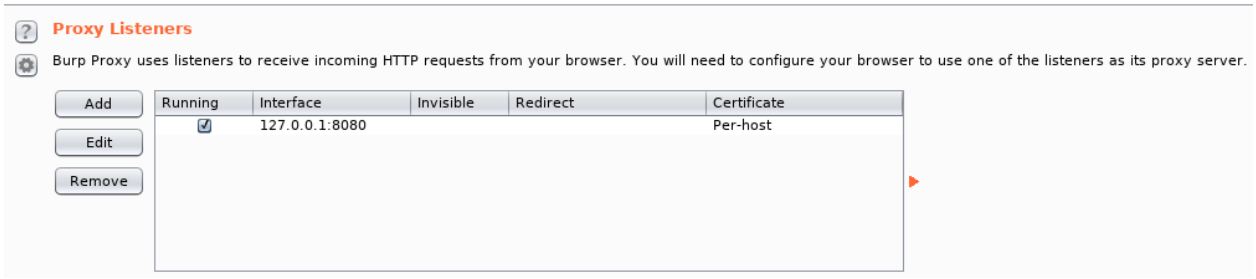
a) Use the temporary project since I'm using the free version



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

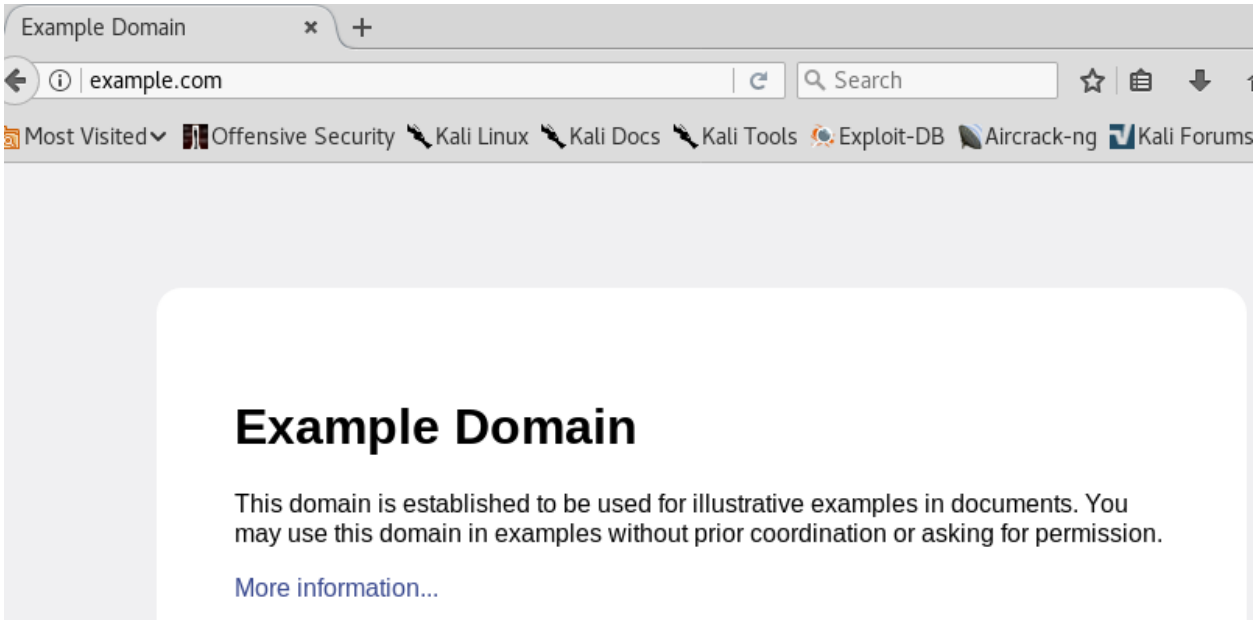


c) Once is set, return to BurpSuite, go to your options on your interface to validate your proxy configuration

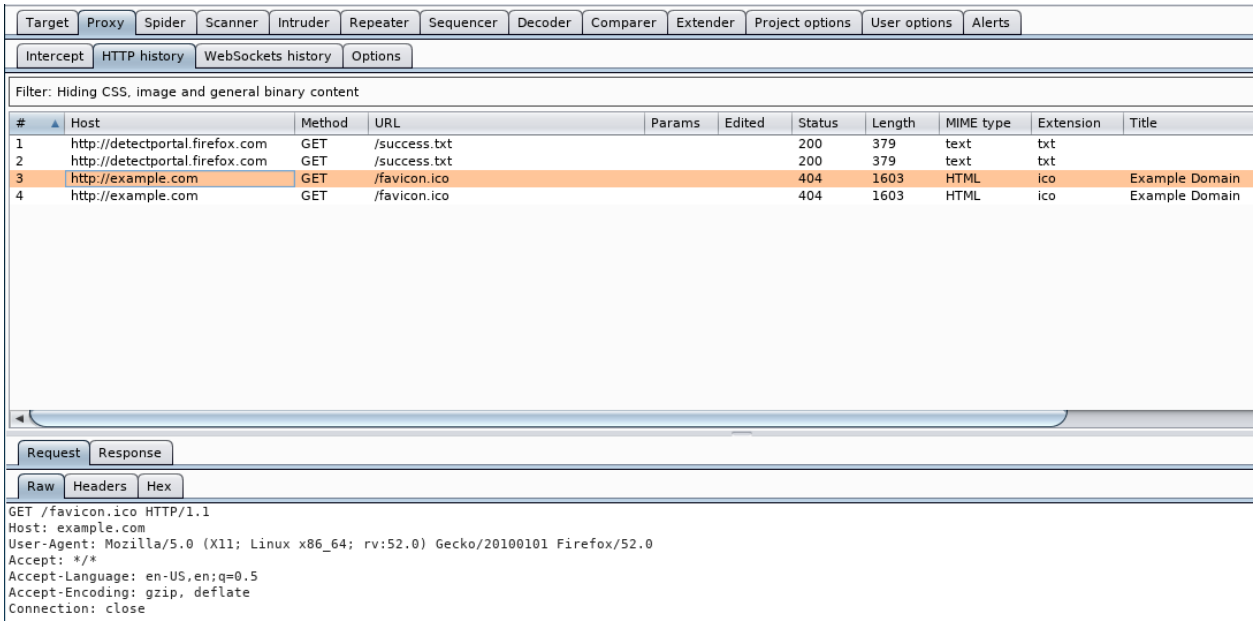


Intercepting traffic on a web page:

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

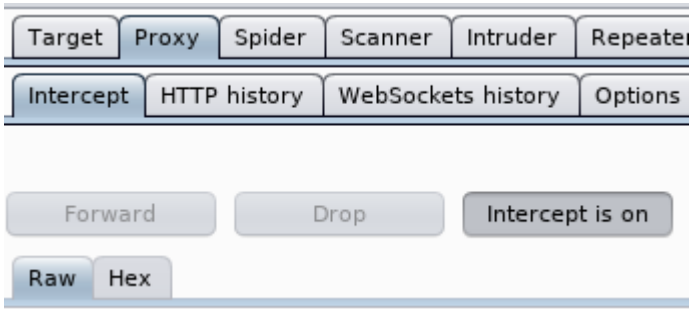


b) Return to the interface and then click on the HTTP history under Proxy and you should get information from example.com

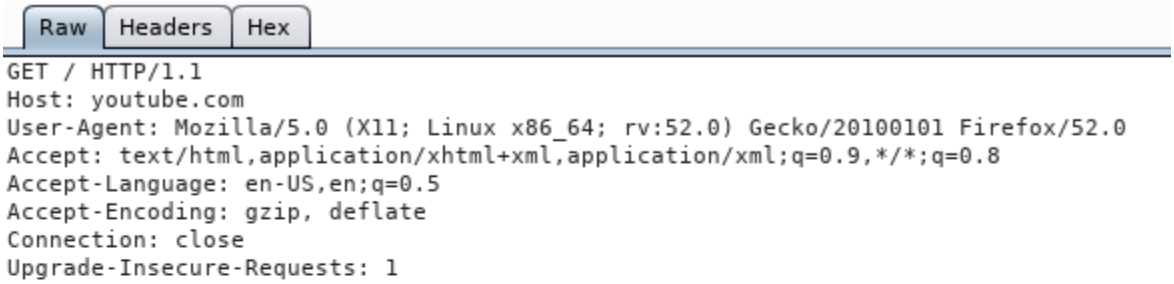


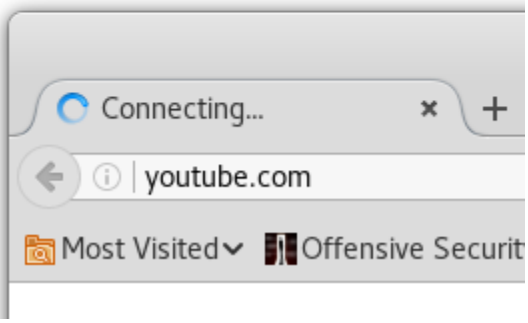
c) Here it shows a lot of information about the web page such as the URL, method and raw information that contains your Operating System. This is a basic example of how you can retrieve information about a web page which can be HTTP or HTTPS.

d) Now click the Intercept tab under Proxy and turn on the Intercept to test a web page that can be intercepted.



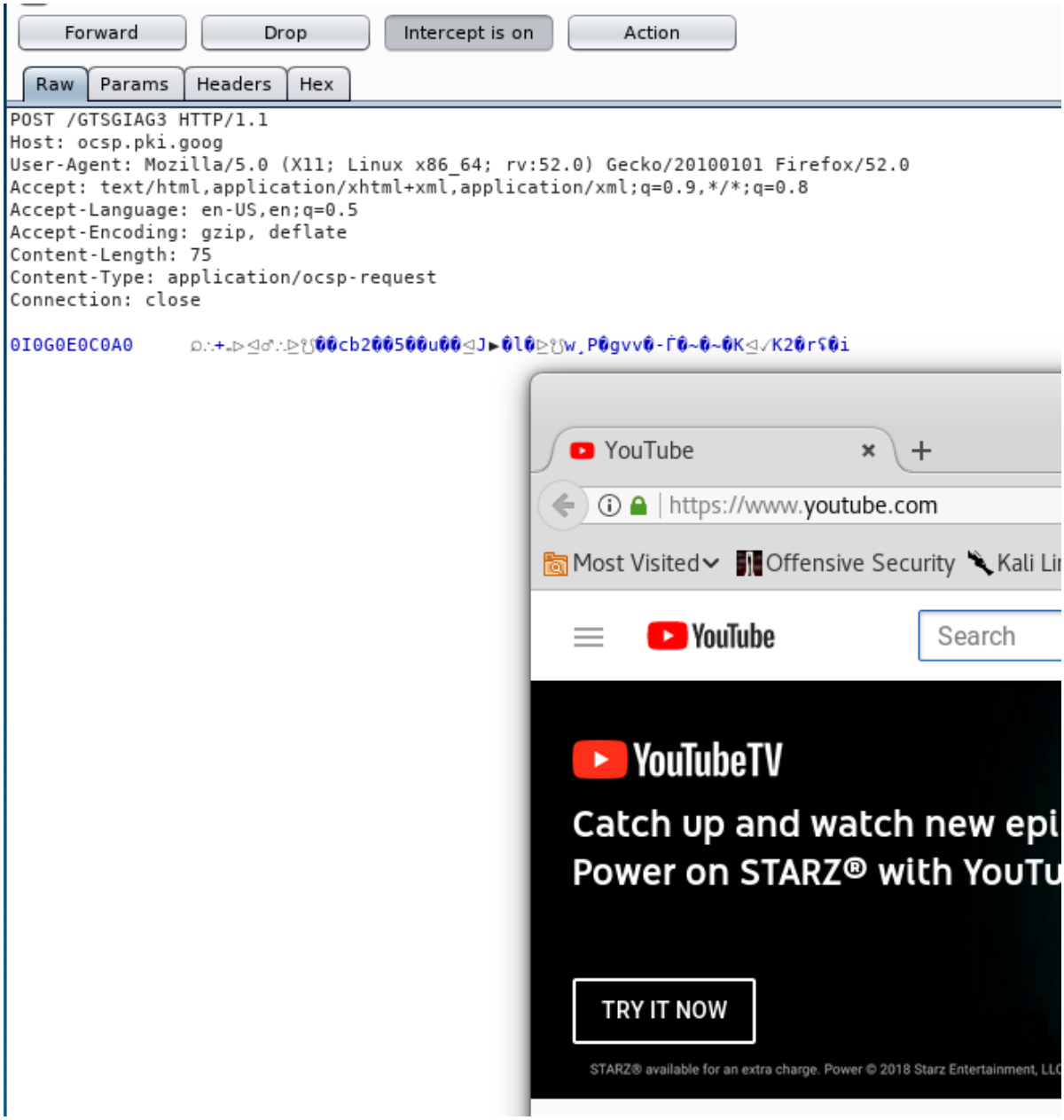
e) Go to Firefox and enter in the URL: youtube.com





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 bottom, 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.

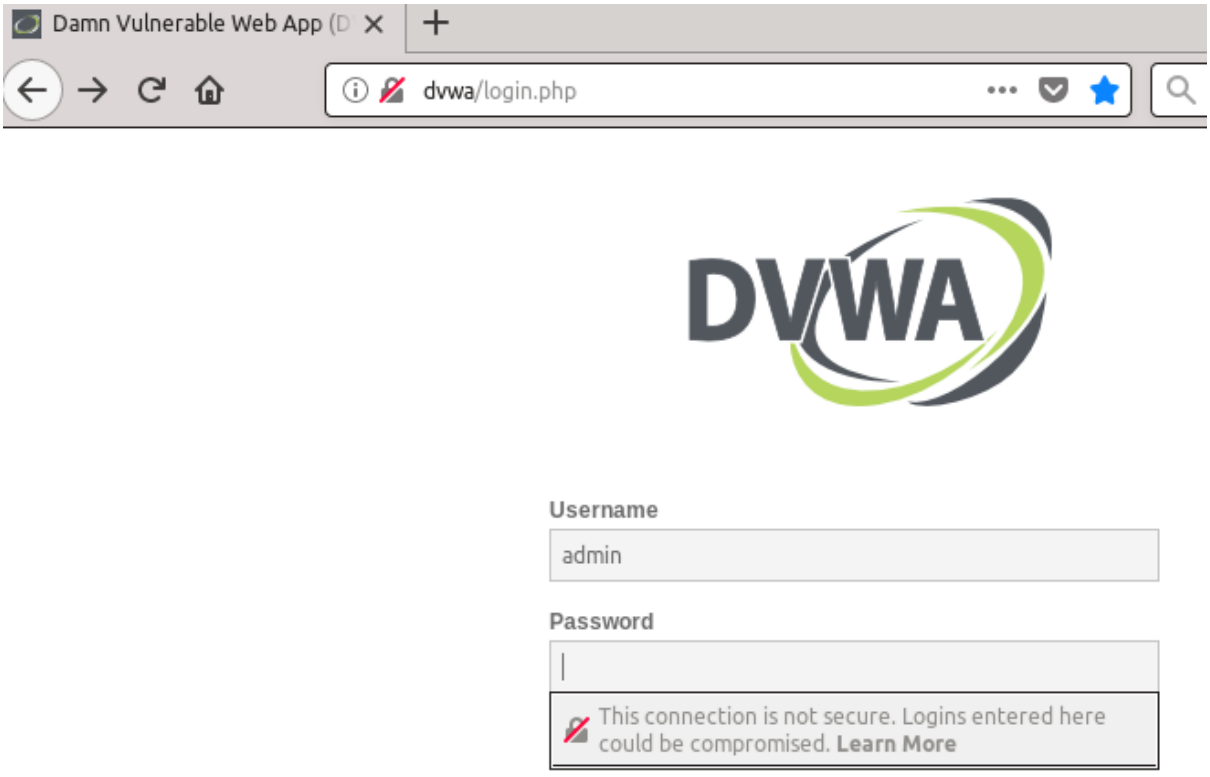
This is how you use BurpSuite as a beginner to intercept traffic on web pages. If you are a web penetration tester, this tool can be useful to test web applications on your target or the company that you are auditing to find vulnerabilities that are critical to their web server. This tool can go further 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.

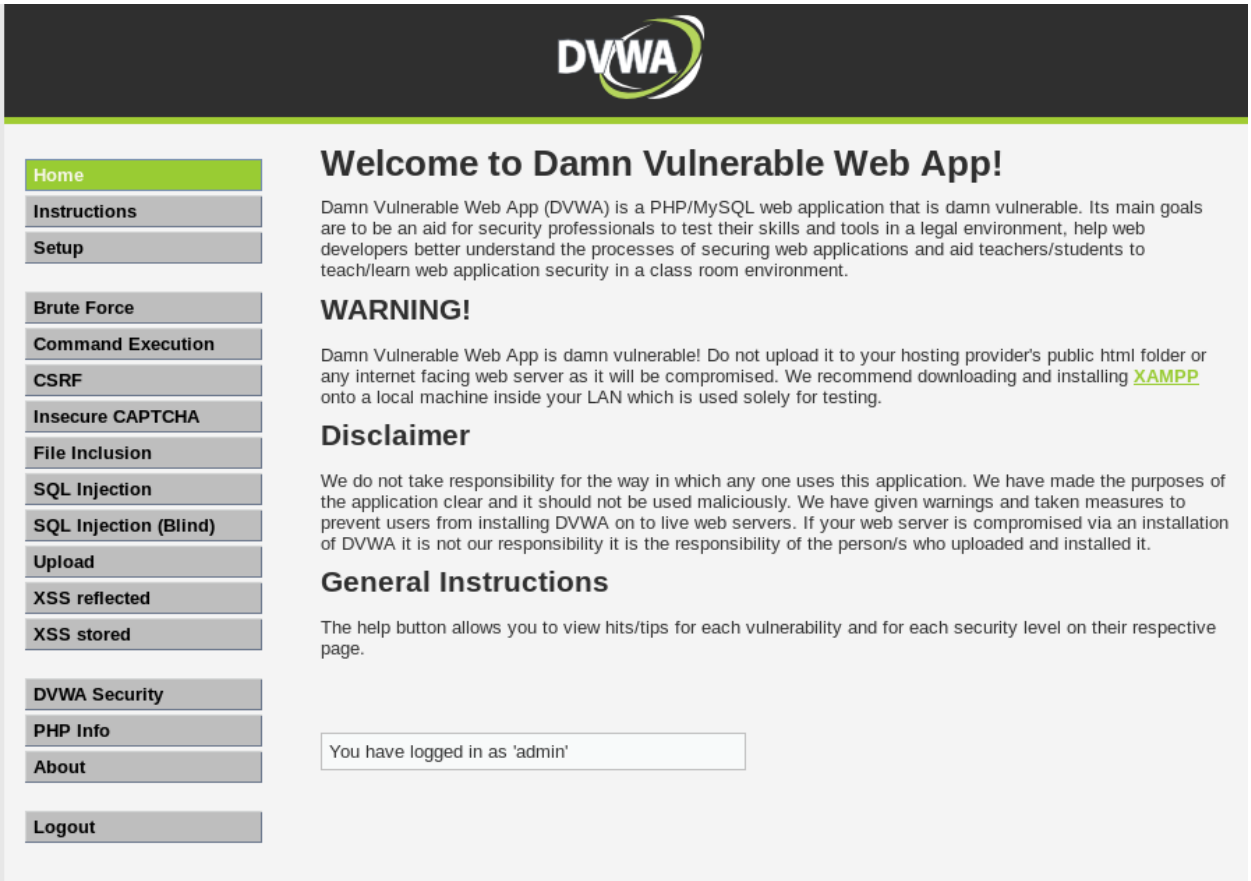
Brute Force Attack using DVWA

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.

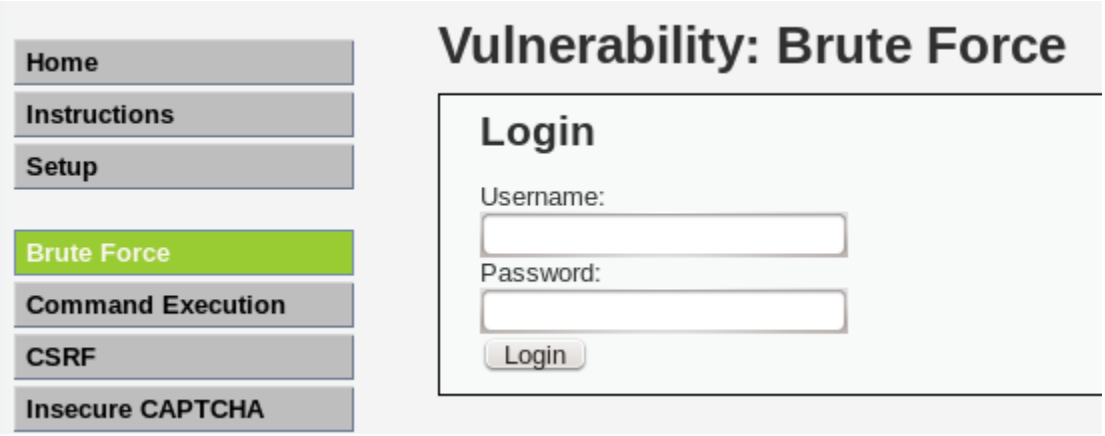
I'll be using SamuraiWTF because DVWA and BurpSuite are already installed and configured. To install SamuraiWTF, go to: https://sourceforge.net/projects/samurai/files/SamuraiWTF%203.0%20Branch/ and download the latest version of Samurai-WTF as an iso. (If you have questions of how to install it on your 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**.

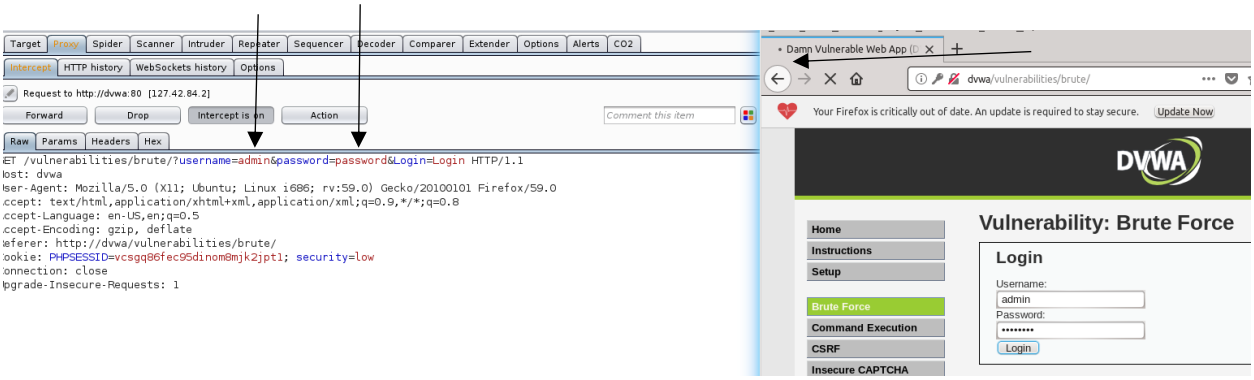




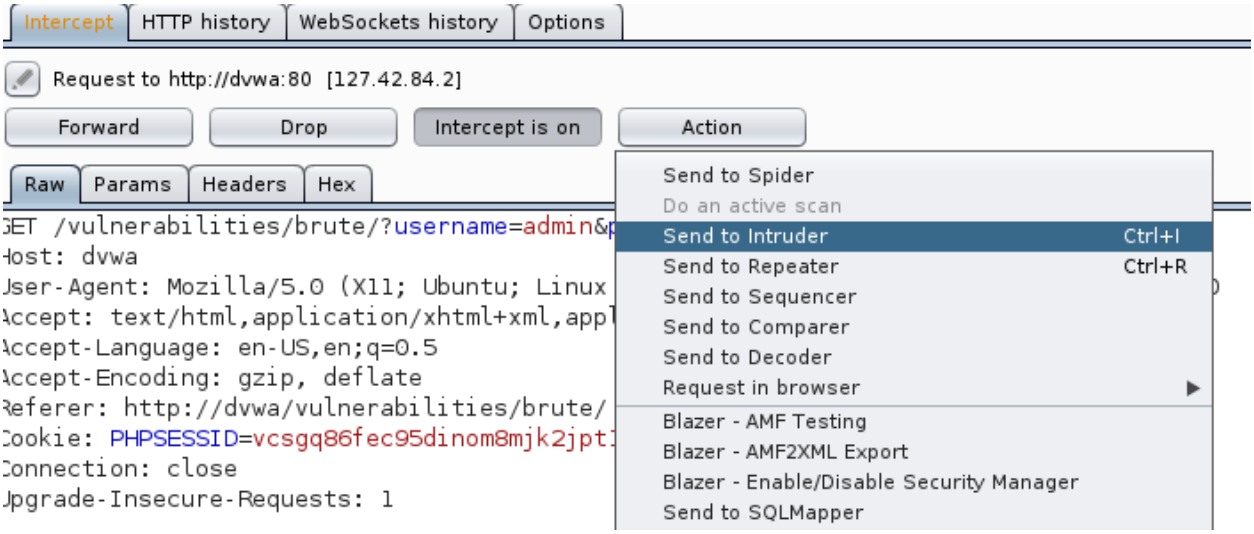
Now you are logged in as admin. Go to DVWA Security and make sure the security level is low which it should be set to low already. Now, let's go to Brute Force.



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.

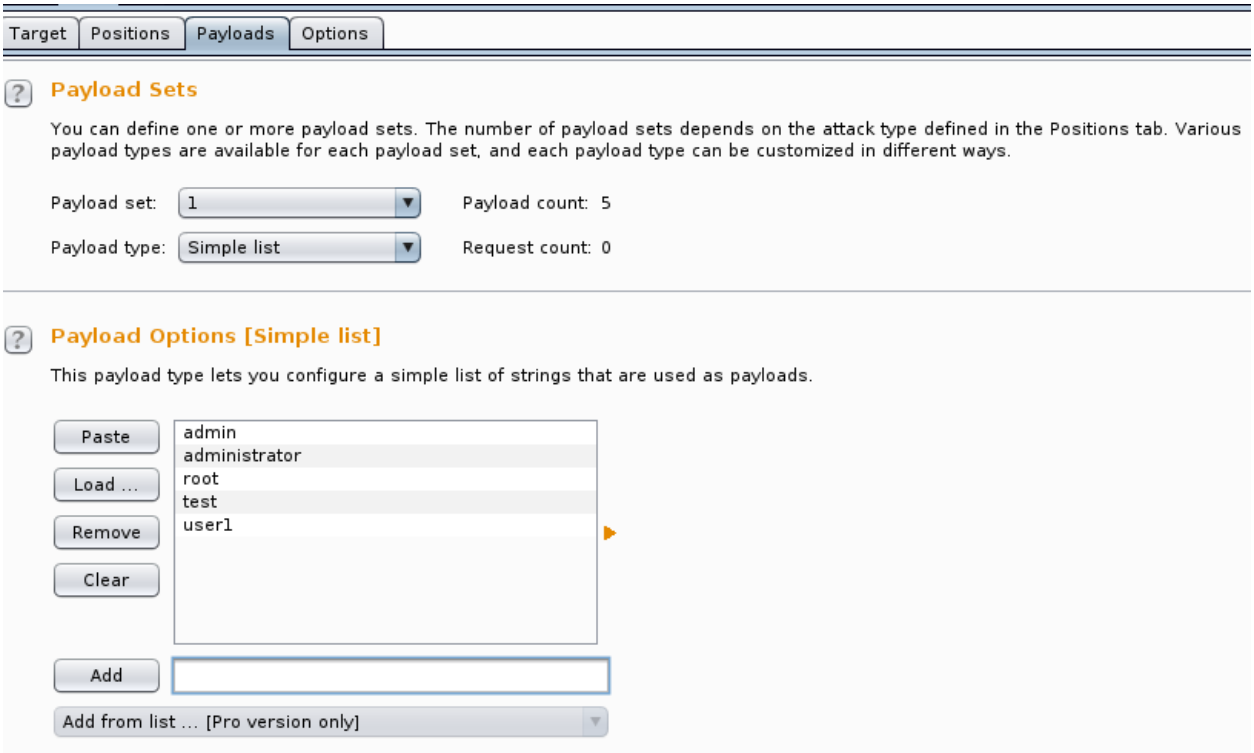


Then go to the Intruder tab and then click Positions

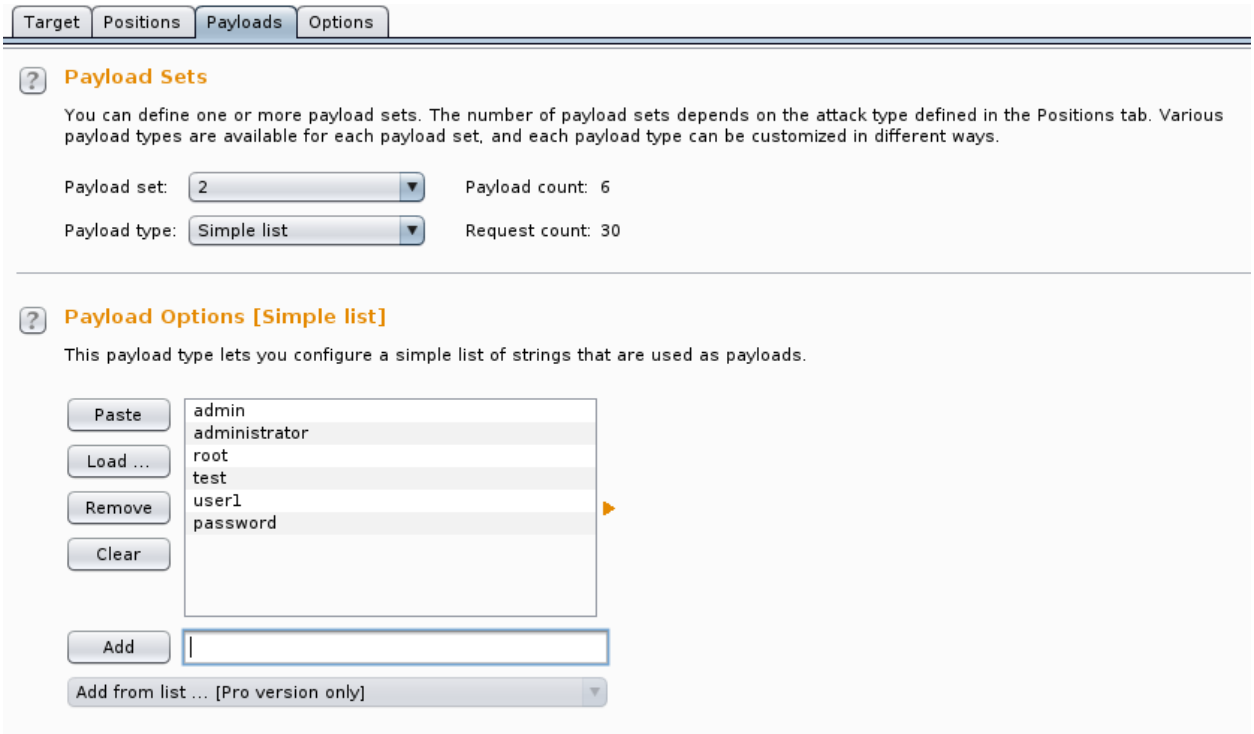
The intruder allows you to edit the parameters of the request. While you edit the parameters, you can manipulate it and then get the results you are looking for. What is highlighted are all the payloads from the request. The payloads that need to be highlighted only are the username and the password.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

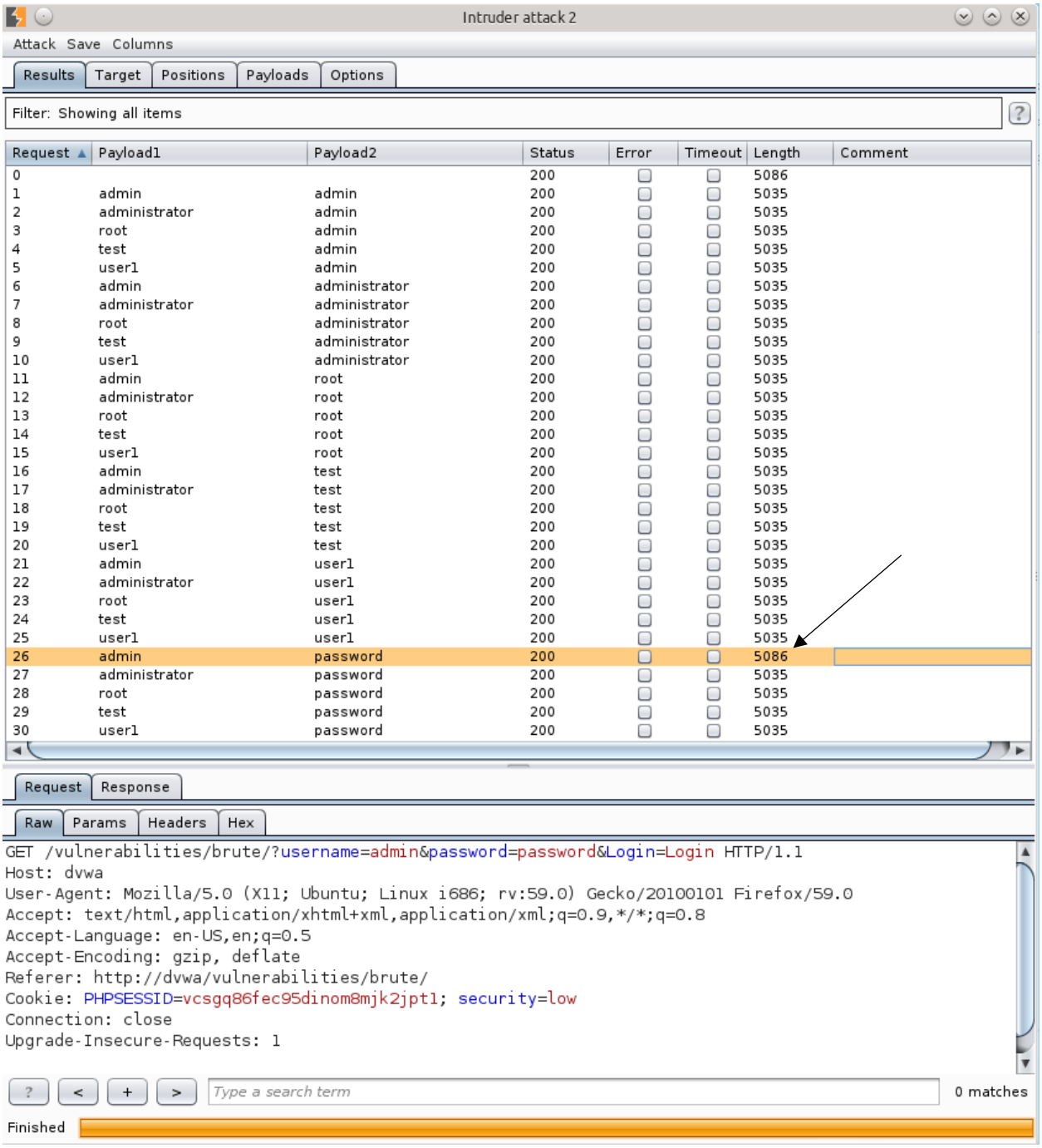
Now they are highlighted, the request is ready for the next step. Make sure you change the attack type to Cluster bomb because you are using two values for the attack which is the username and password. Once is set, go to the Payloads tab.



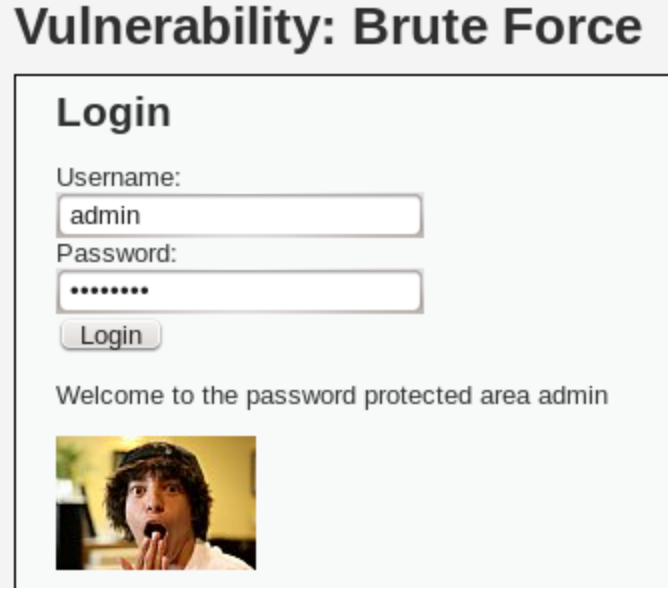
In this tab, you will set your payloads using set 1 and 2. Set 1 will be for your username. You will use the Simple list and under payload options, you can add or load a simple list of usernames. For this demonstration. I added 5 common usernames. Now switch the payload set to 2.



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.



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.



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*