

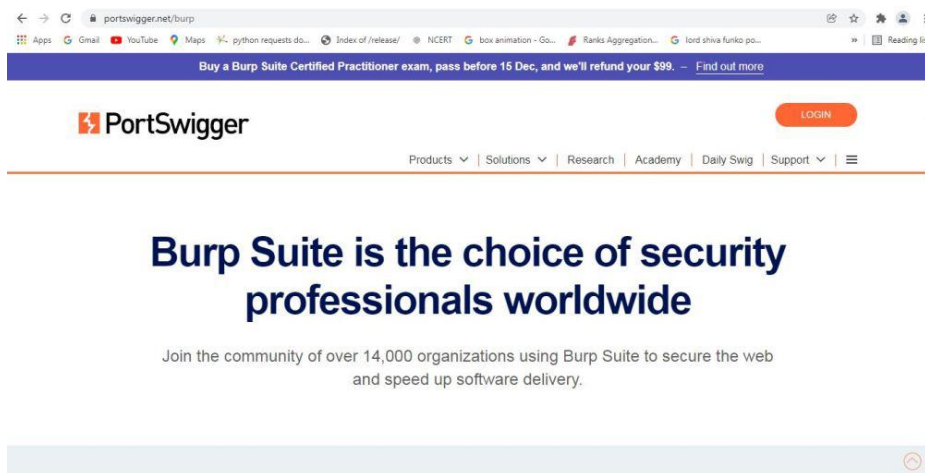
Burp Suite:-

Burp Suite can be understood as a web vulnerability scanner. It is a collection of different tools which are brought together in a single application for performing security testing of Web applications. Burp Suite is widely used by penetration testers to test and identify different vulnerabilities which are present in web applications and exploit them to fix those security issues. Burp Suite has a large number of features which include proxy, intruder, repeater, sequencer, decoder, compare, and many more. Burp Suite has a large number of users.

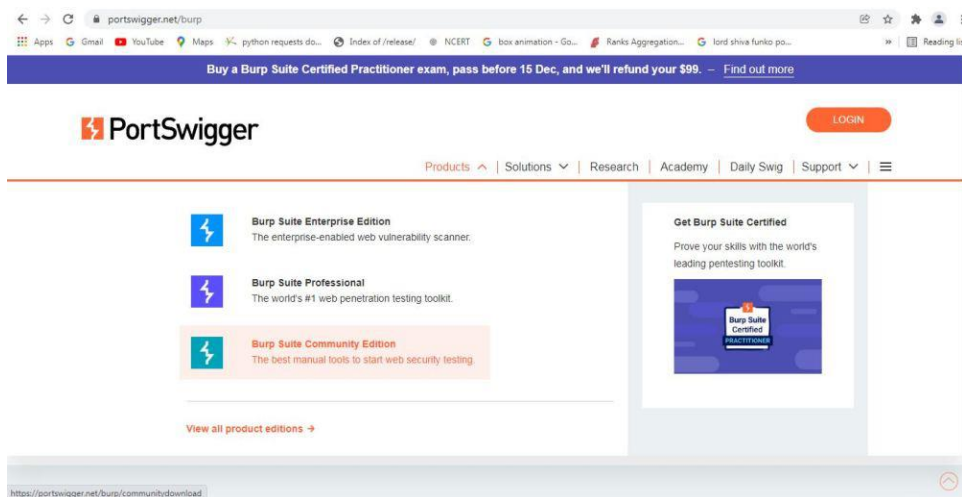
Installing and configuring Burp Suite on Windows:

Below are few steps for installation of Burp Suite on Windows:

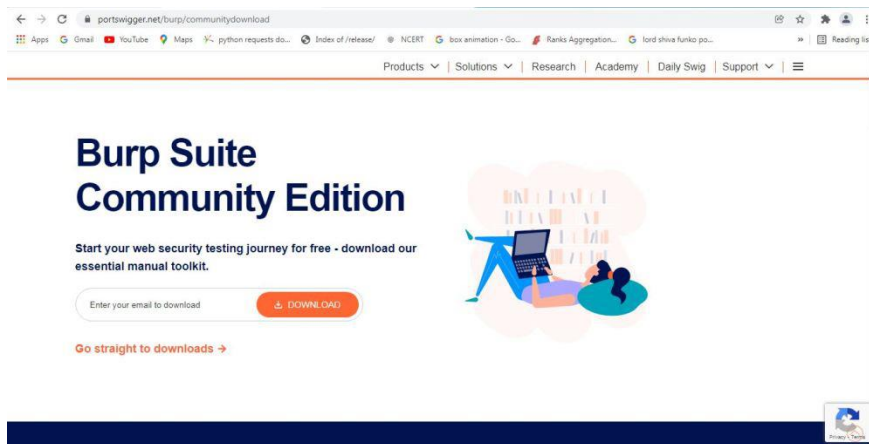
Step 1: Visit the [official Burp Suite website](https://portswigger.net/burp) using any web browser.



Step 2: Click on Products, a list of different Burp Suites will open, choose Burp suite Community Edition as it is free, click on it.

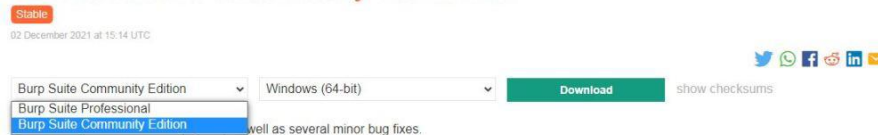


Step 3: New webpage will open, which will ask for email id, and other option is Go Straight to downloads. Click on Go straight to downloads.

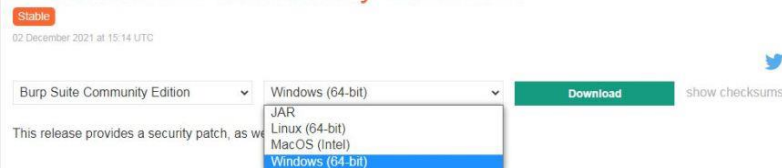


Step 4: After clicking on Go straight to downloads new webpage will open which will contain two versions of burp suite one is Burp suite community edition and the other is burp suite professional along with compatibility for different operating systems.

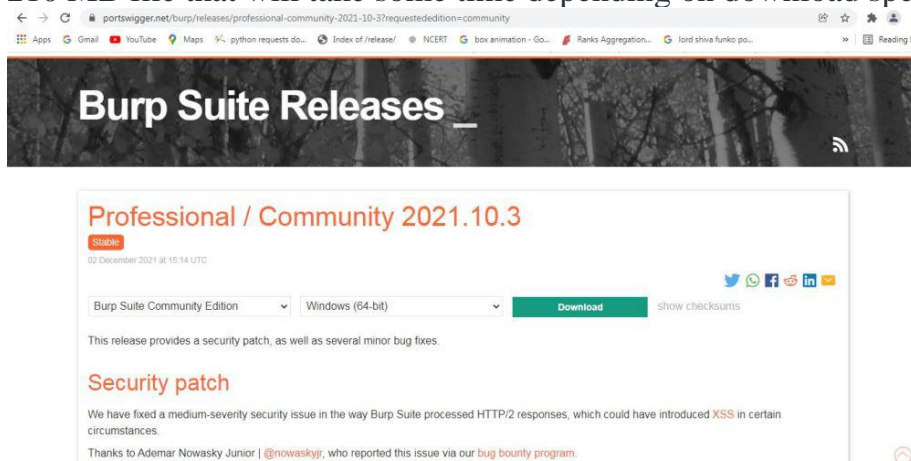
Professional / Community 2021.10.3



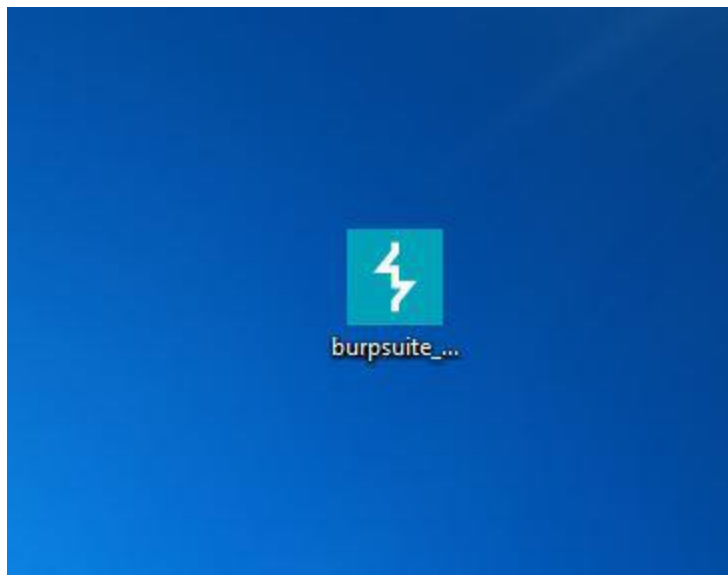
Professional / Community 2021.10.3



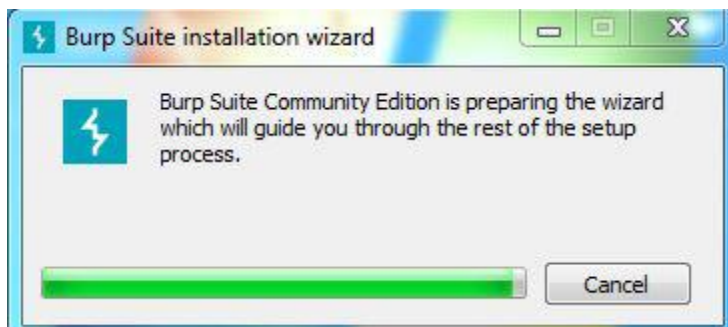
Step 5: Choose Burp suite Community Edition along with Windows (64-bit). Click on the download button, downloading of the executable file will start shortly. It is a big 210 MB file that will take some time depending on download speed.



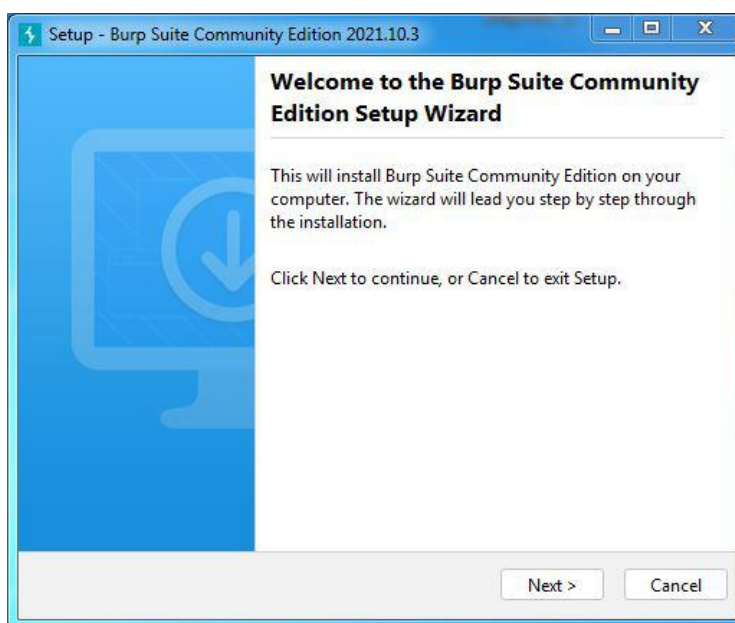
Step 6: Now check for the executable file in downloads in your system and run it.



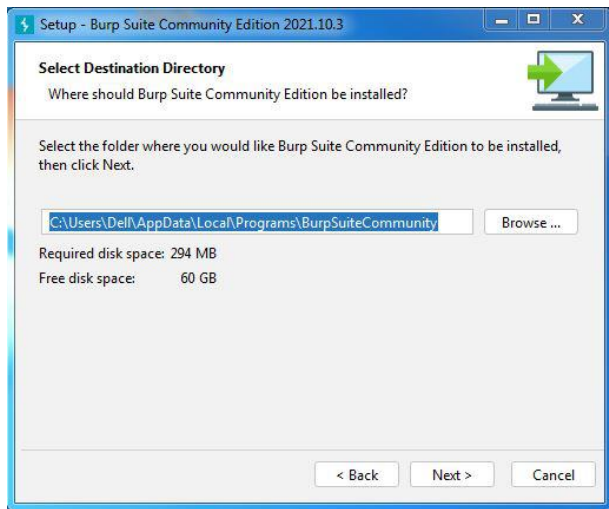
Step 7: Loading of Installation Wizard will appear which will take a few seconds.



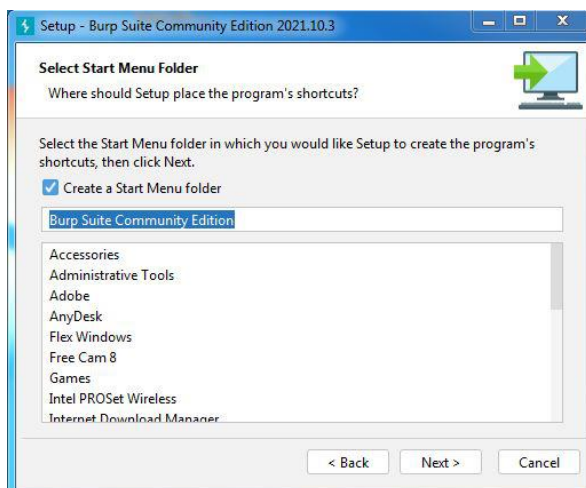
Step 8: After this Setup screen will appear, click on Next.



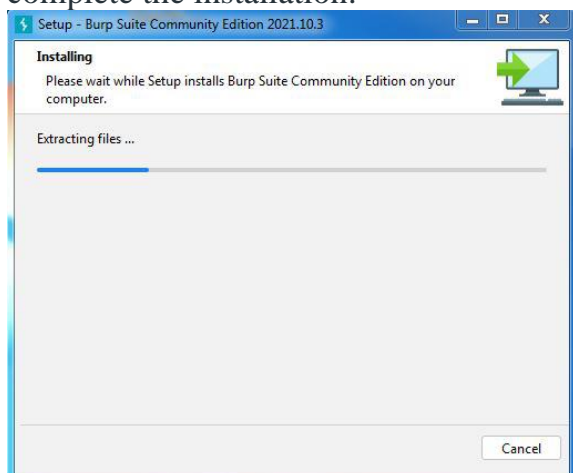
Step 9: The next screen will be of installing location so choose the drive which will have sufficient memory space for installation. It needed a memory space of 294 MB.



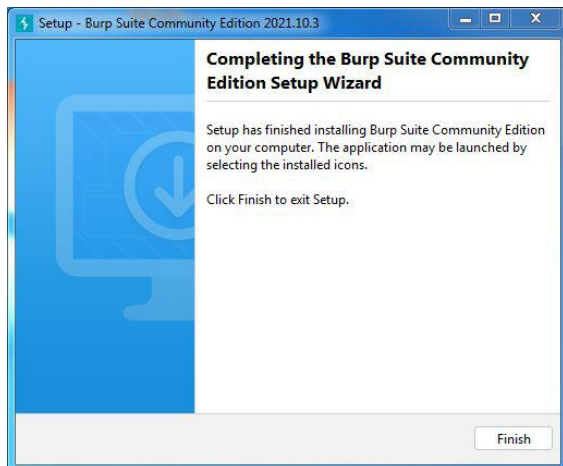
Step 10: Next screen will be of choosing Start menu folder so don't do anything just click on Next Button.



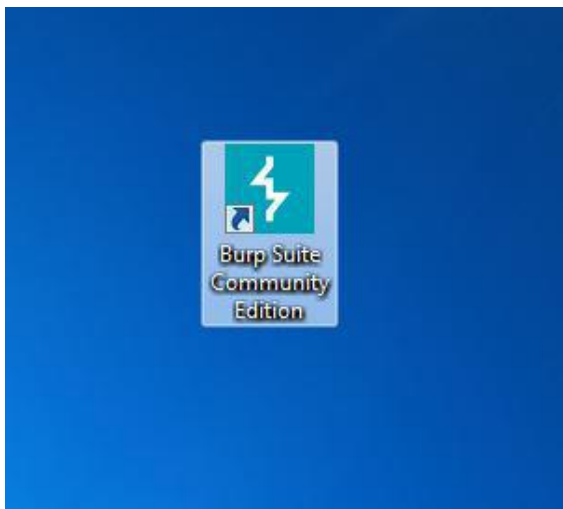
Step 11: After this installation process will start and will hardly take a minute to complete the installation.



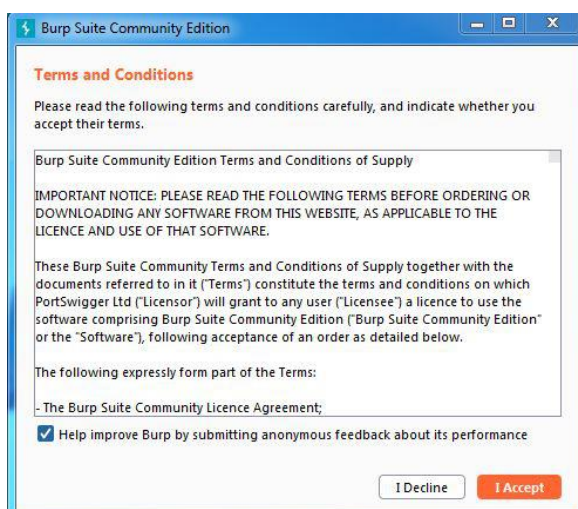
Step 12: Click on Finish after the installation process is complete.



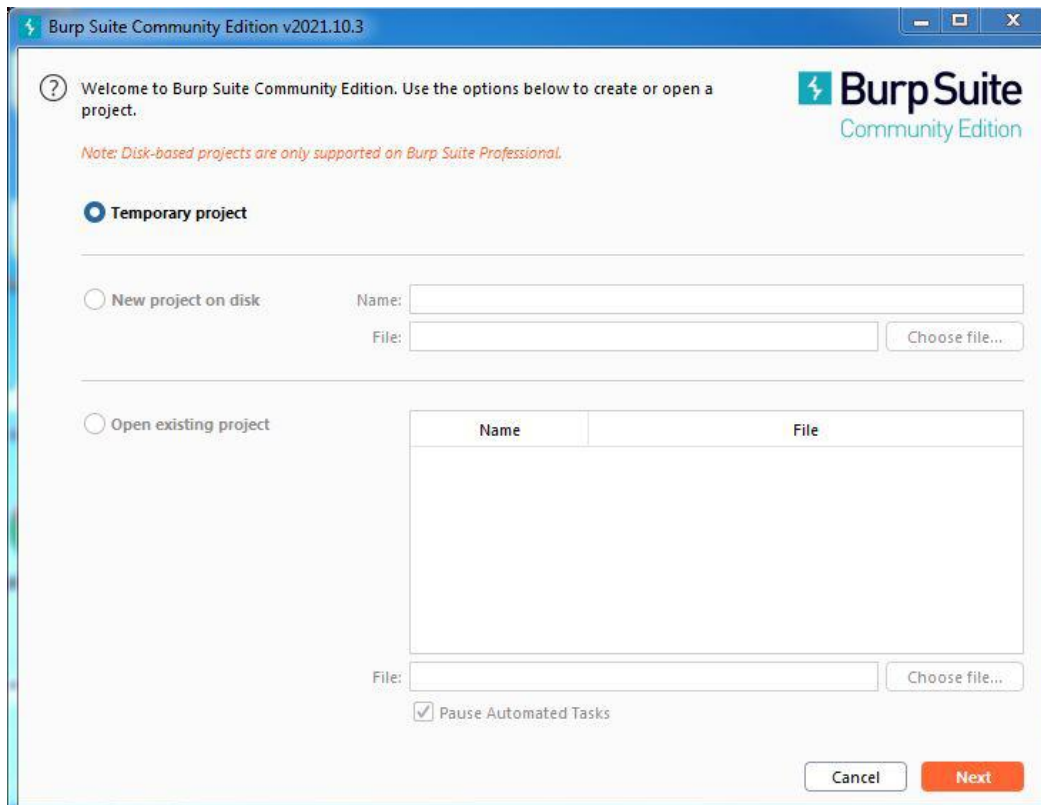
Step 13: Burp suite is successfully installed on the system and an icon is created on the desktop.



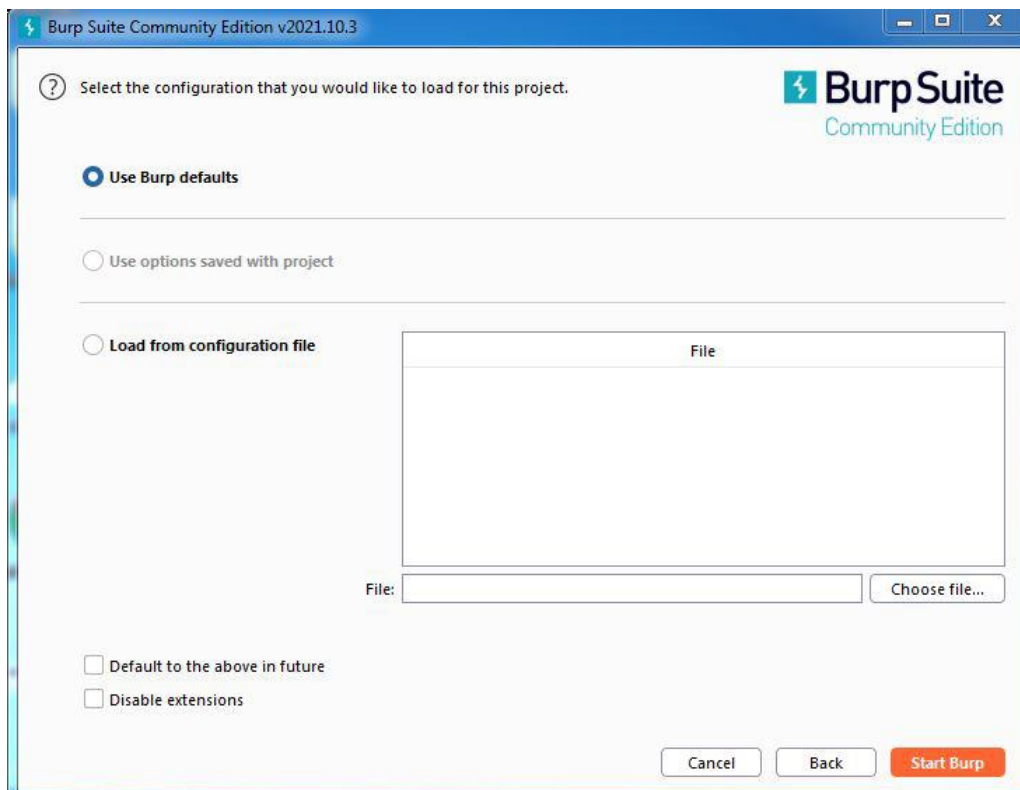
Step 14: Run the software, screen containing terms and conditions will appear Click on I Accept.



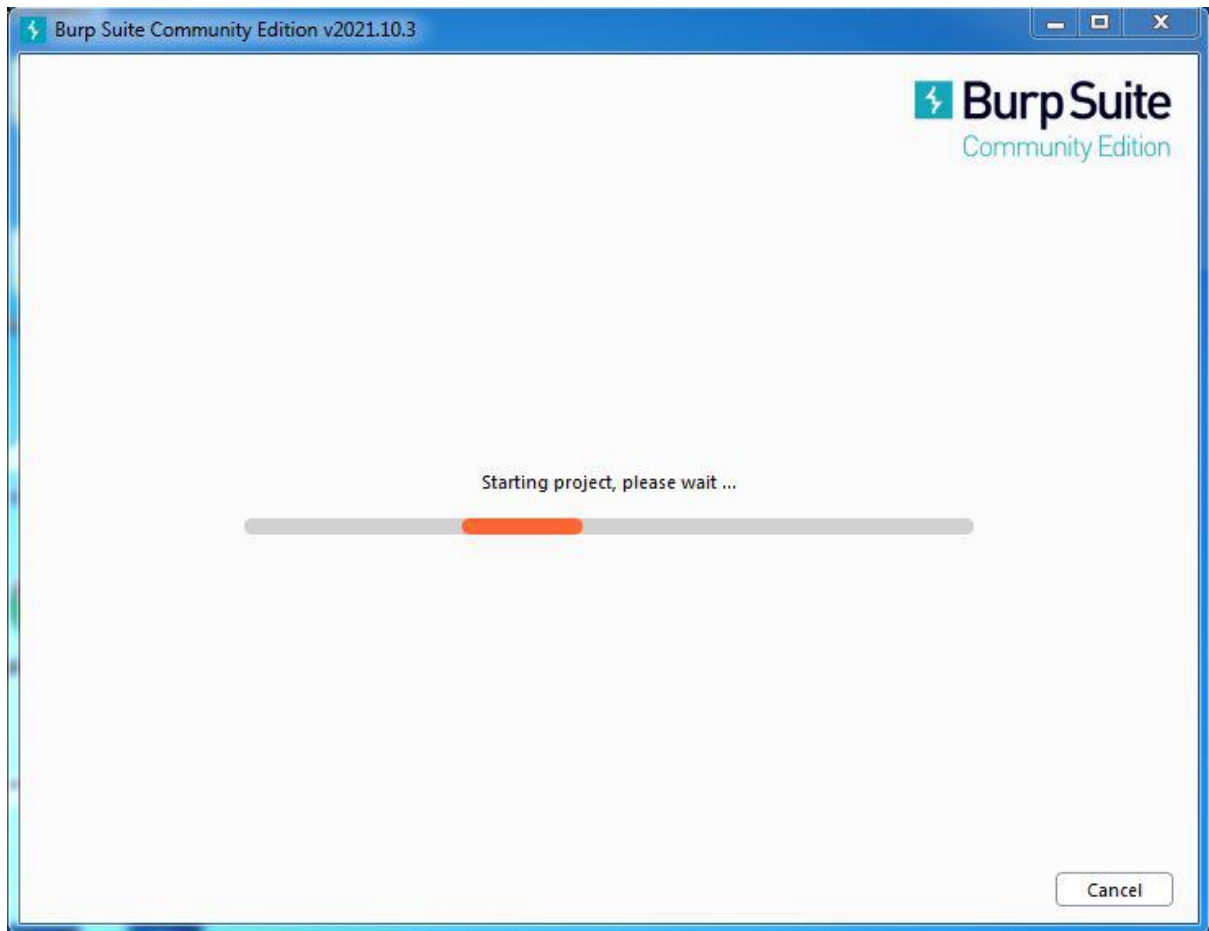
Step 15: New screen containing information regarding the project will appear, Choose temporary project and click Next.



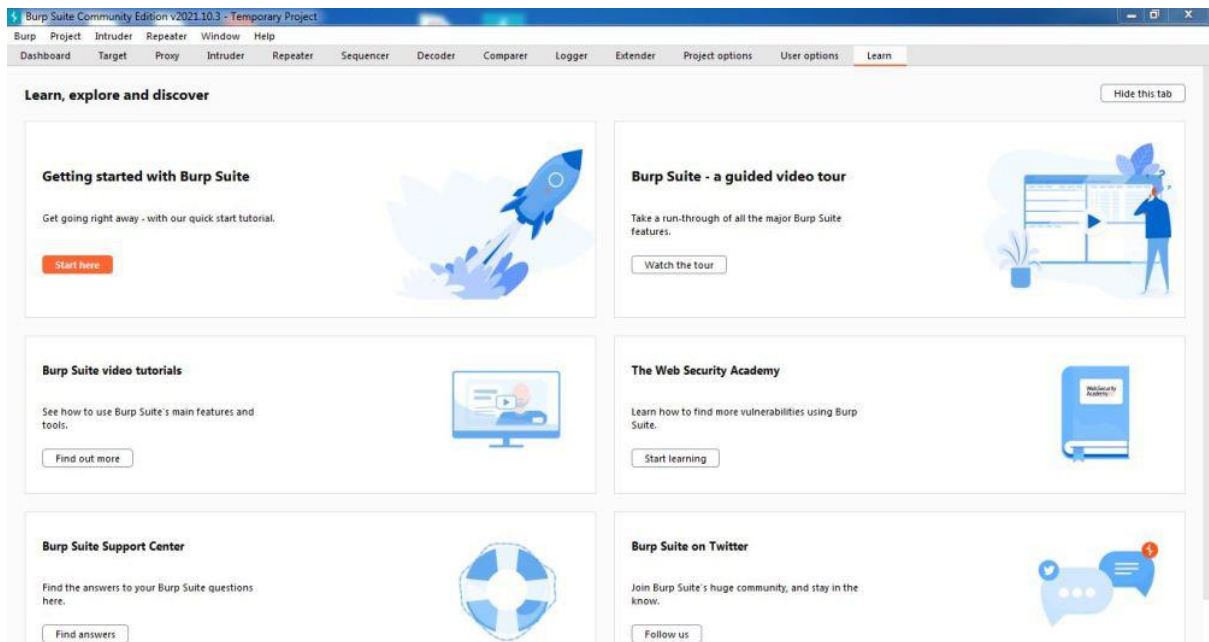
Step 16: Next screen is about using default settings or loading from configuration file, click on Use Burp Defaults.



Step 17: Project will start loading.



Step 18: Finally new project window will appear.



Usage of Burp suite:-

Burp or Burp Suite is a set of tools used for penetration testing of web applications. It is developed by the company named Portswigger, which is also the alias of its founder

Dafydd Stuttard. BurpSuite aims to be an all in one set of tools and its capabilities can be enhanced by installing add-ons that are called BApps. The tools offered by BurpSuite are:

1. Spider:

It is a web spider/crawler that is used to map the target web application. The objective of the mapping is to get a list of endpoints so that their functionality can be observed and potential vulnerabilities can be found. Spidering is done for a simple reason that the more endpoints you gather during your recon process, the more attack surfaces you possess during your actual testing.

2. Proxy:

BurpSuite contains an intercepting proxy that lets the user see and modify the contents of requests and responses while they are in transit. It also lets the user send the request/response under monitoring to another relevant tool in BurpSuite, removing the burden of copy-paste. The proxy server can be adjusted to run on a specific loop-back ip and a port. The proxy can also be configured to filter out specific types of request-response pairs.

3. Intruder:

It is a fuzzer. This is used to run a set of values through an input point. The values are run and the output is observed for success/failure and content length. Usually, an anomaly results in a change in response code or content length of the response. BurpSuite allows brute-force, dictionary file and single values for its payload position. The intruder is used for:

- Brute-force attacks on password forms, pin forms, and other such forms.
- The dictionary attack on password forms, fields that are suspected of being vulnerable to XSS or SQL injection.
- Testing and attacking rate limiting on the web-app.

4. Repeater:

Repeater lets a user send requests repeatedly with manual modifications. It is used for:

- Verifying whether the user-supplied values are being verified.
- If user-supplied values are being verified, how well is it being done?
- What values is the server expecting in an input parameter/request header?
- How does the server handle unexpected values?
- Is input sanitation being applied by the server?
- How well the server sanitizes the user-supplied inputs?
- What is the sanitation style being used by the server?
- Among all the cookies present, which one is the actual session cookie.
- How is CSRF protection being implemented and if there is a way to bypass it?

5. Sequencer:

The sequencer is an entropy checker that checks for the randomness of tokens generated by the webserver. These tokens are generally used for authentication in sensitive operations: cookies and anti-CSRF tokens are examples of such tokens. Ideally, these tokens must be generated in a fully random manner so that the probability of appearance of each possible character at a position is distributed uniformly. This should be achieved both bit-wise and character-wise. An entropy analyzer tests this hypothesis for being true. It works like this: initially, it is assumed that the tokens are random. Then the tokens are tested on certain parameters for certain characteristics. A term significance level is defined as a minimum value of probability that the token will exhibit for a characteristic, such that if the token has a characteristics probability below significance level, the hypothesis that the token is random will be rejected. This tool can be used to find out the weak tokens and enumerate their construction.

6. Decoder:

Decoder lists the common encoding methods like URL, HTML, Base64, Hex, etc. This tool comes handy when looking for chunks of data in values of parameters or headers. It is also used for payload construction for various vulnerability classes. It is used to uncover primary cases of IDOR and session hijacking.

7. Extender:

BurpSuite supports external components to be integrated into the tools suite to enhance its capabilities. These external components are called BApps. These work just like browser extensions. These can be viewed, modified, installed, uninstalled in the Extender window. Some of them are supported on the community version, but some require the paid professional version.

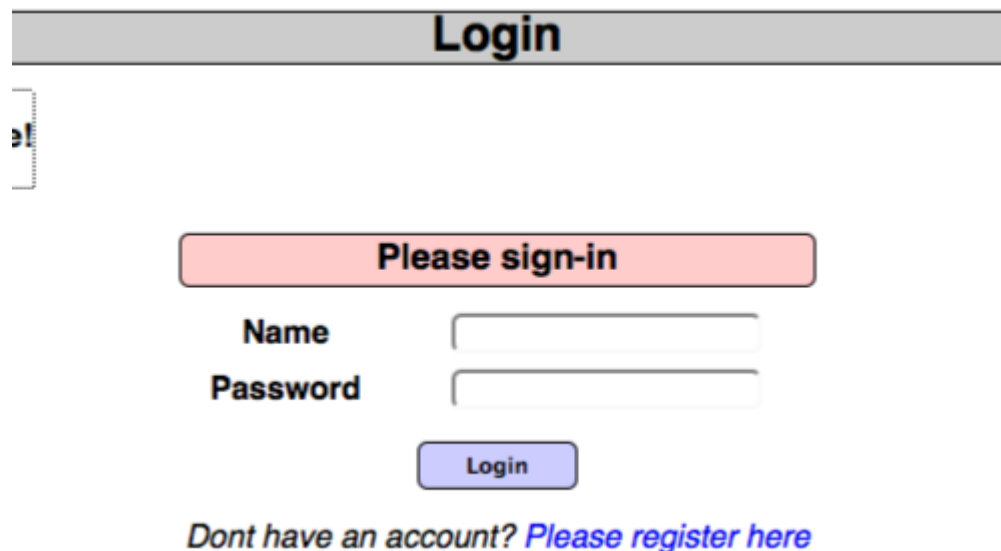
8. Scanner:

The scanner is not available in the community edition. It scans the website automatically for many common vulnerabilities and lists them with information on confidence over each finding and their complexity of exploitation. It is updated regularly to include new and less known vulnerabilities.

Using Burp to Brute Force a Login Page

Authentication lies at the heart of an application's protection against unauthorized access. If an attacker is able to break an application's authentication function then they may be able to own the entire application.

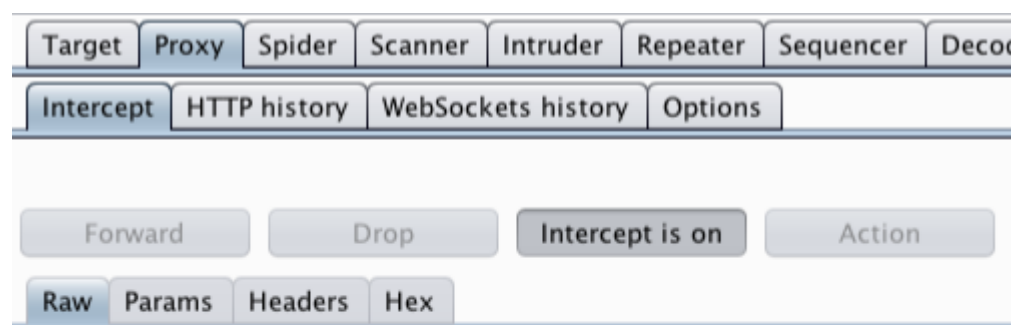
The following tutorial demonstrates a technique to bypass authentication using a simulated login page from the "Mutillidae" training tool. The version of "Mutillidae" we are using is taken from OWASP's Broken Web Application Project. Find out how to download, install and use this project.



The screenshot shows a web page with a grey header bar containing the word "Login" in bold black text. Below the header, on the left, is a small icon of a person. The main content area has a pink rounded rectangle with the text "Please sign-in" in bold black. Underneath this are two input fields: the first is labeled "Name" and the second is labeled "Password". To the right of each label is a white rectangular input box. Below the input fields is a blue rounded rectangle with the word "Login" in white. At the bottom of the form area, there is a line of text: "Dont have an account? [Please register here](#)".

First, ensure that Burp is correctly configured with your browser.

In the Burp Proxy tab, ensure "Intercept is off" and visit the login page of the application you are testing in your browser.



Return to Burp.

In the Proxy "Intercept" tab, ensure "Intercept is on".

Login

3!

Please sign-in

Name

test

Password

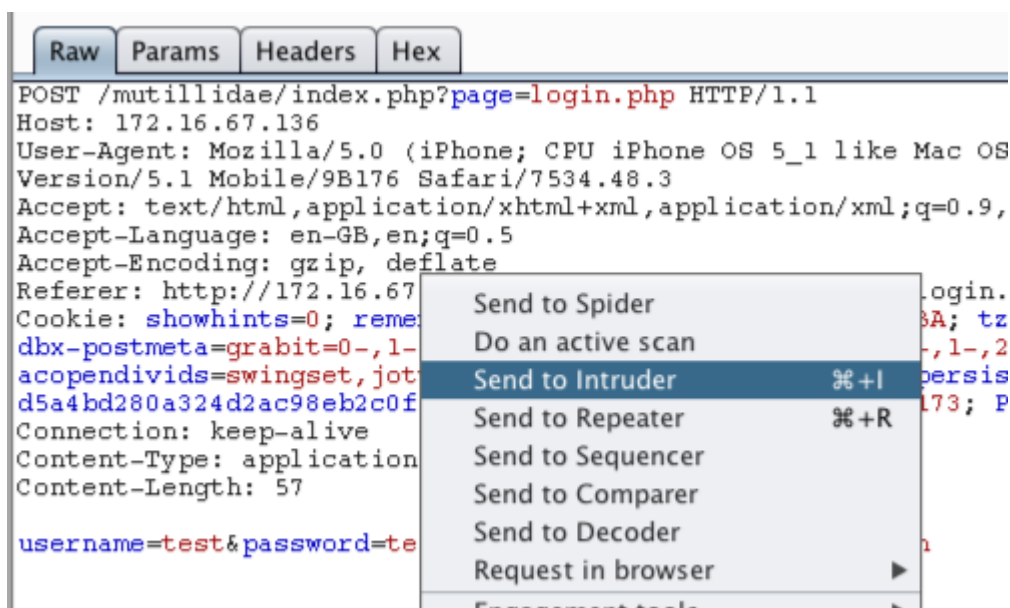
....

Login



Dont have an account? [Please register here](#)

In your browser enter some arbitrary details in to the login page and submit the request.



The captured request can be viewed in the Proxy "Intercept" tab.

Right click on the request to bring up the context menu.

Then click "Send to Intruder".

Note: You can also send requests to the Intruder via the context menu in any location where HTTP requests are shown, such as the site map or Proxy history.

? **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.

Attack type: Cluster bomb

```
POST /mutillidae/index.php?page=login.php HTTP/1.1
Host: 172.16.67.136
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 5_1 like Mac OS X)
AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176
Safari/7534.48.3
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.16.67.136/mutillidae/index.php?page=login.php
Cookie: showhints=0; remember_token=PRkIXJ3DG8iXL0P4vRAMBA;
tz_offset=3600;
dbx-postmeta=grabit=0-,1-,2-,3-,4-,5-,6-advancedstuff=0-,1-,2-;
ecopendivide=swingset,jotto,phpbk2,redmine;
ecgroupswithpersist=nada;
d5a4bd280a324d2ac98eb2c0fe58b9e0-aplamed3d0hordo7nrl3fuv173;
PHPSESSID=29jrpjak954g8k8jlgk9fid23
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 57

username=$test$password=$testlogin.php-submit-button=Login
```

Add \$
Clear \$
Auto \$
Refresh

Go to the Intruder "Positions" tab.

Clear the pre-set payload positions by using the "Clear" button on the right of the request editor.

Add the "username" and "password" parameter values as positions by highlighting them and using the "Add" button.

Change the attack to "Cluster bomb" using the "Attack type" drop down menu.

? **Payload Sets** Start attack

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: 1 Payload count: 9
Payload type: Simple list Request count: 18

? **Payload Options [Simple list]**

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

Paste Load ... Remove Clear Add Add from list ...

Admin
Admin1
Dave
User
Pete
Paul
Oscar
Harrison

Go to the "Payloads" tab.

In the "Payload sets" settings, ensure "Payload set" is "1" and "Payload type" is set to "Simple list".

In the "Payload options" settings enter some possible usernames. You can do this manually or use a custom or pre-set payload list.

Payload Sets

[Start attack](#)

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: 3,424
Payload type: Request count: 30,816

Payload Options [Simple list]

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

Paste

Load ...

Remove

Clear

Add

!@#\$%

!@#\$%^

!@#\$%^&

!@#\$%^&*

!root

\$\$SRV

\$secure\$

*3noguru

Enter a new item

Next, in the "Payload Sets" options, change "Payload" set to "2".

In the "Payload options" settings enter some possible passwords. You can do this manually or using a custom or pre-set list.

Click the "Start attack" button.

Results

Target

Positions

Payloads

Options

Filter: Showing all items

Request	Payload1	Payload2	Status ▾	Error	Timeout	Length
118	Admin	ADMIN	302	<input type="checkbox"/>	<input type="checkbox"/>	39590
442	Admin	Admin	302	<input type="checkbox"/>	<input type="checkbox"/>	39590
9595	Admin	admin	302	<input type="checkbox"/>	<input type="checkbox"/>	39590
8527	User	USER	302	<input type="checkbox"/>	<input type="checkbox"/>	39593
8653	User	User	302	<input type="checkbox"/>	<input type="checkbox"/>	39593
29362	User	user	302	<input type="checkbox"/>	<input type="checkbox"/>	39593
0			200	<input type="checkbox"/>	<input type="checkbox"/>	39432
1	Admin	!@#\$\$	200	<input type="checkbox"/>	<input type="checkbox"/>	39432
2	Admin1	!@#\$\$	200	<input type="checkbox"/>	<input type="checkbox"/>	39432
3	Dave	!@#\$\$	200	<input type="checkbox"/>	<input type="checkbox"/>	39432
4	User	!@#\$\$	200	<input type="checkbox"/>	<input type="checkbox"/>	39432
5	Pete	!@#\$\$	200	<input type="checkbox"/>	<input type="checkbox"/>	39432
6	Paul	!@#\$\$	200	<input type="checkbox"/>	<input type="checkbox"/>	39432

Request

Response

Raw

Params

Headers

Hex

?

<

+

>

Type a search term

0 m

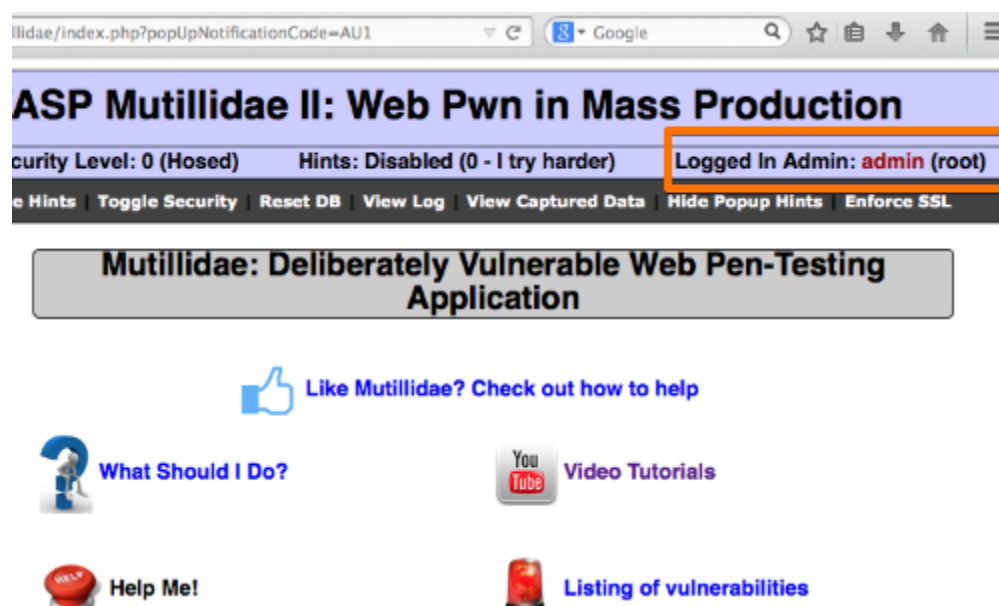
In the "Intruder attack" window you can sort the results using the column headers.

In this example sort by "Length" and by "Status".

Request	Response
	<div>Raw Headers Hex HTML Render</div> <pre>HTTP/1.1 302 Found Date: Fri, 06 Mar 2015 13:36:36 GMT Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-lubunt proxy_html/3.0.1 mod_python/3.3.1 Python/2.6.5 mod_ssl/2.2.14 Phusion_Passenger/3.0.17 mod_perl/2.0.4 Perl/v5.10.1 X-Powered-By: PHP/5.3.2-lubuntu4.5 Set-Cookie: username=admin Set-Cookie: uid=1 Location: index.php?popupNotificationCode=AU1 Logged-In-User: admin Vary: Accept-Encoding Content-Length: 39071 Connection: close Content-Type: text/html <!-- I think the database password is</pre>

The table now provides us with some interesting results for further investigation.

By viewing the response in the attack window we can see that request 118 is logged in as "admin".



To confirm that the brute force attack has been successful, use the gathered information (username and password) on the web application's login page.

Burpsuite : Bypass OTP!

Let's Start :

Firstly, target any site or we can say select any site for the attack .

I selected the website.



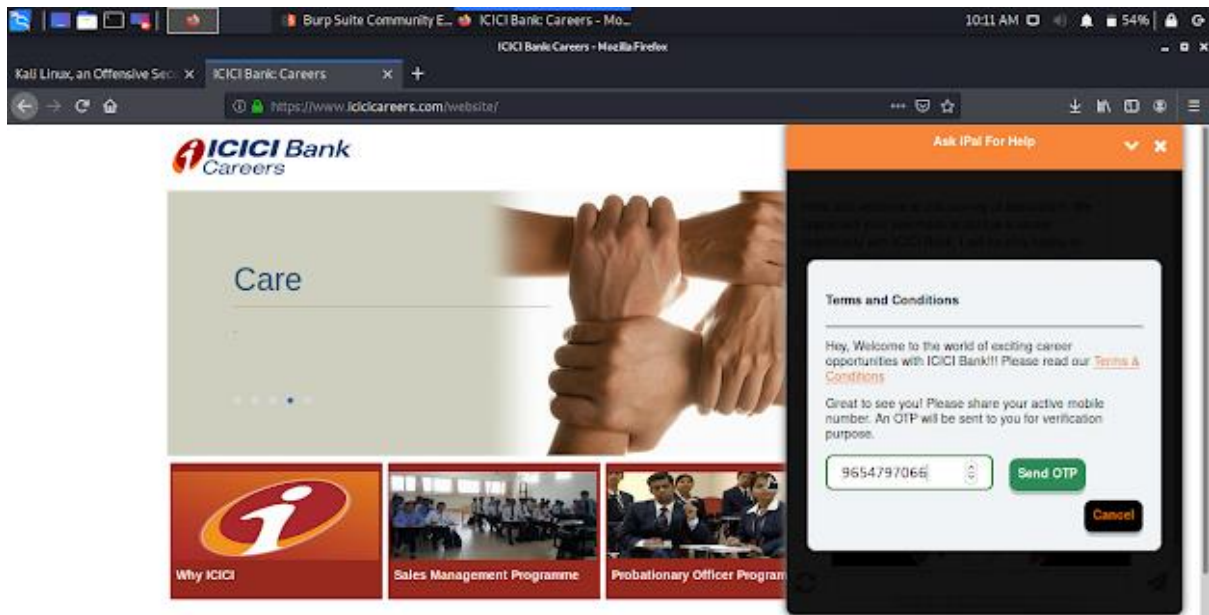
Burp Suite on!

So First step :

First you need to configure your browser with the burpsuite and secondly, you need to configure your browser to use the Burp Proxy listener as its HTTP proxy server. To do this, you need to change your browser's proxy settings to use the proxy host address (by default, 127.0.0.1) and port (by default, 8080) for both HTTP and HTTPS protocols, with no exceptions.

NOTE : If the listener is still not running, then Burp was not able to open the default proxy listener port (8080).

So, here i entered my phone number for the OTP.



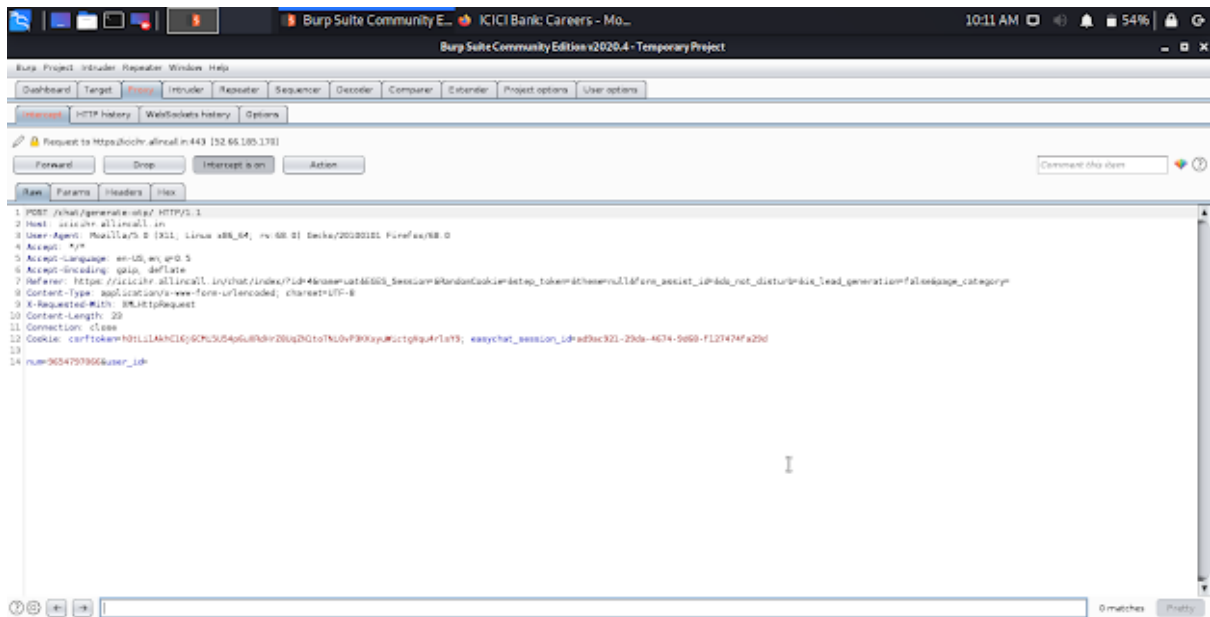
Download Youtube short videos YTShorts Downloader

Now open burp suite:

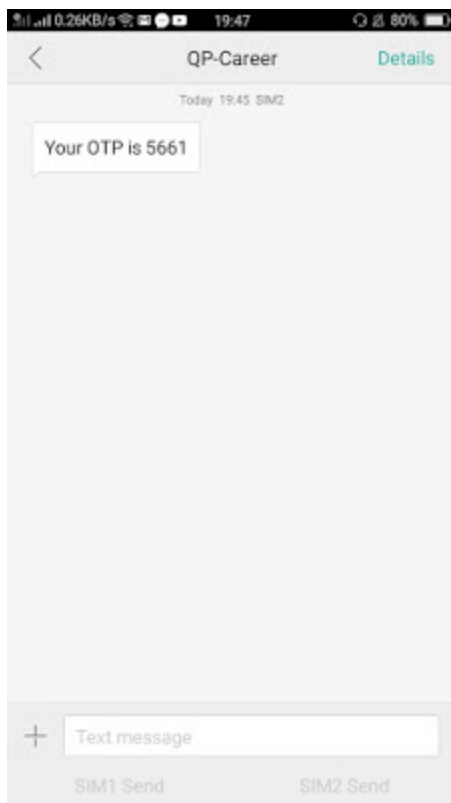
Intercept the request coming from the server.

Intercept: It capture the packet coming from the website or Server.

Now,we will captured the packet which was being sent over as a request packet to the server.



Here i received the OTP in my phone. Let me show you.....



NEED TO KNOW : #In the response,the server gives error as (0) and

if the statement is successful it gives(1).

#Sometimes it gives error in code, so change it to Success.

So now, i send the server request to the repeater and forward the post request to the intruder.

