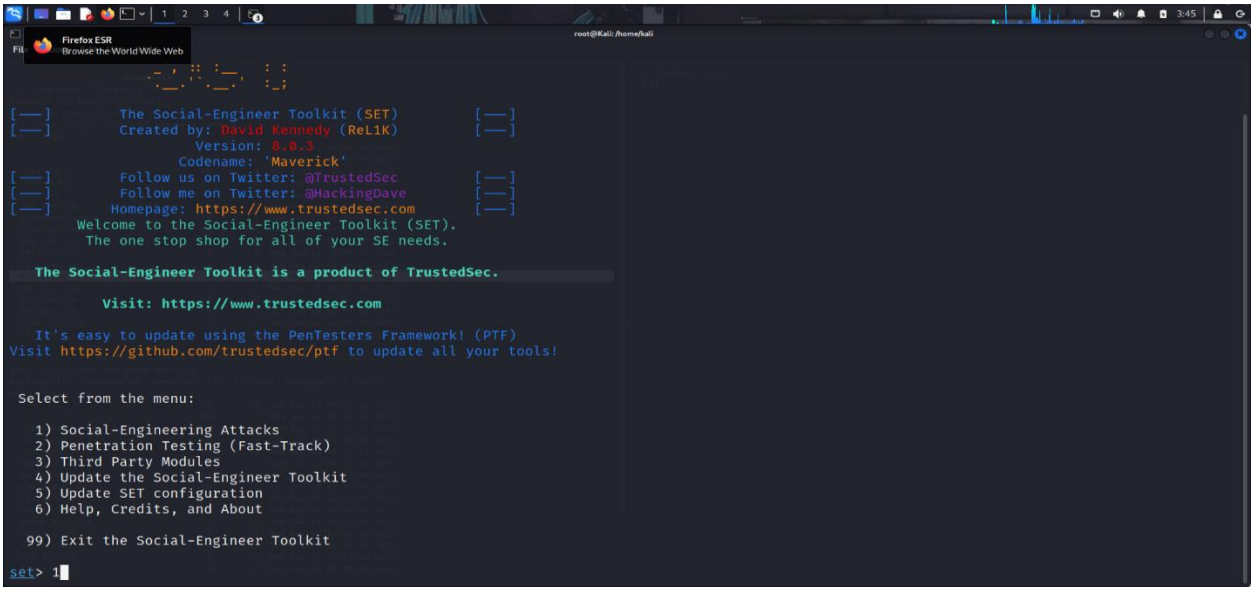
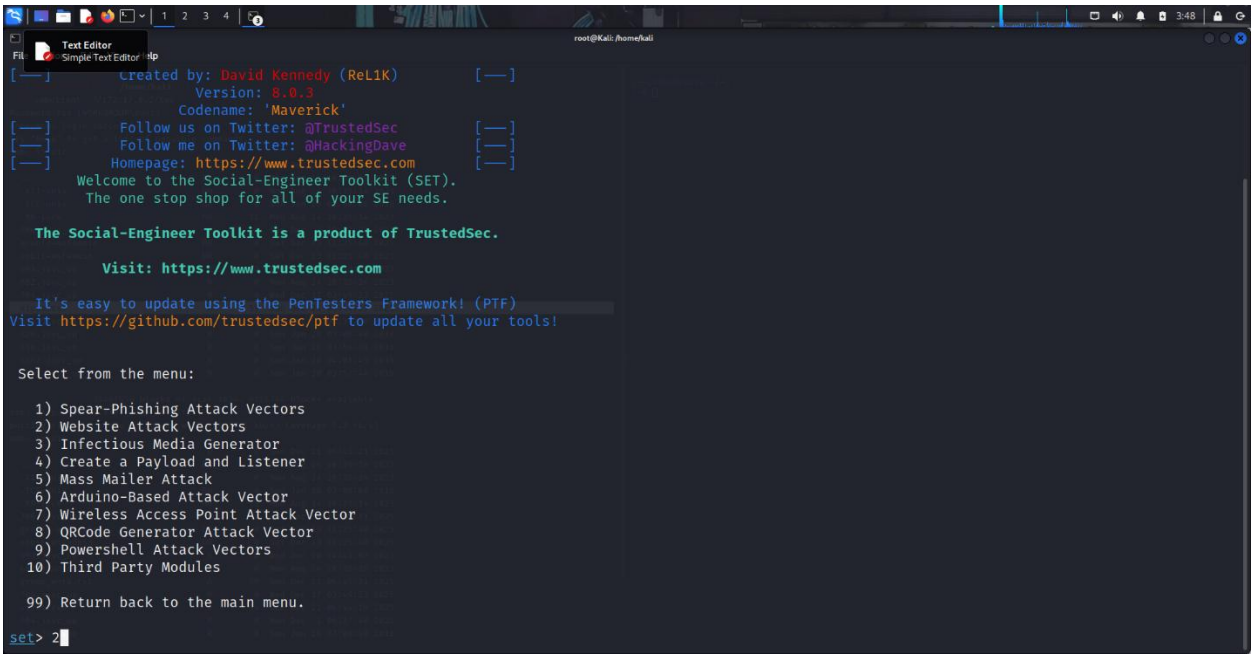
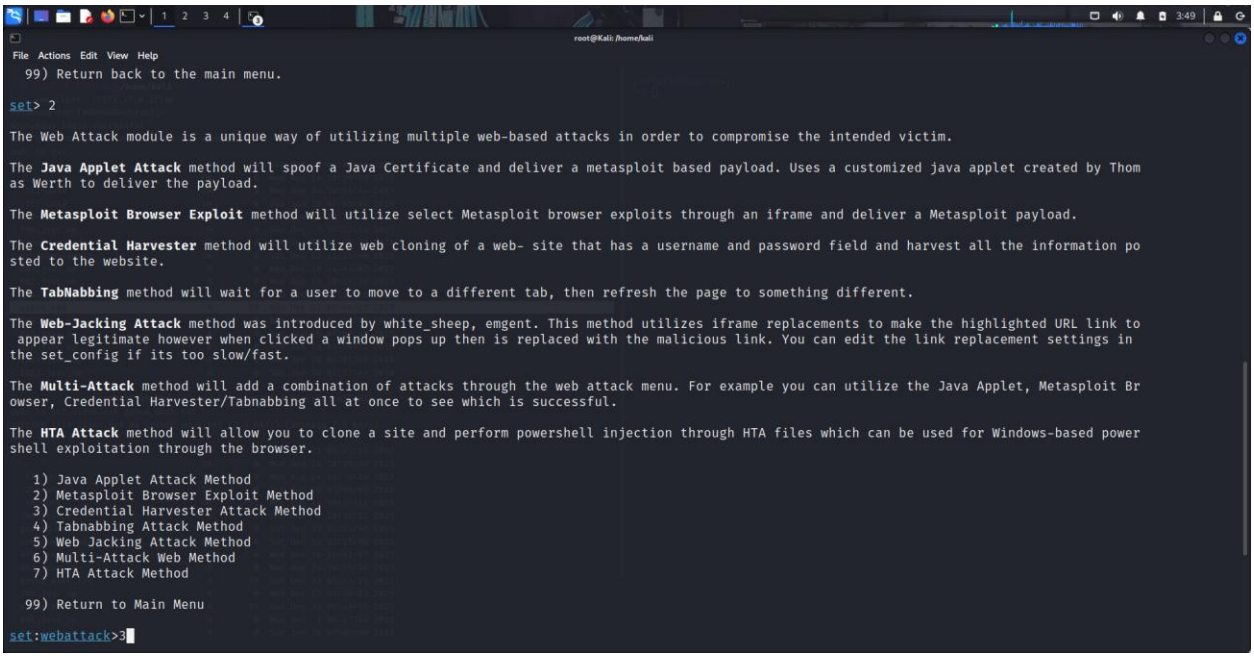
Website Cloning Lab

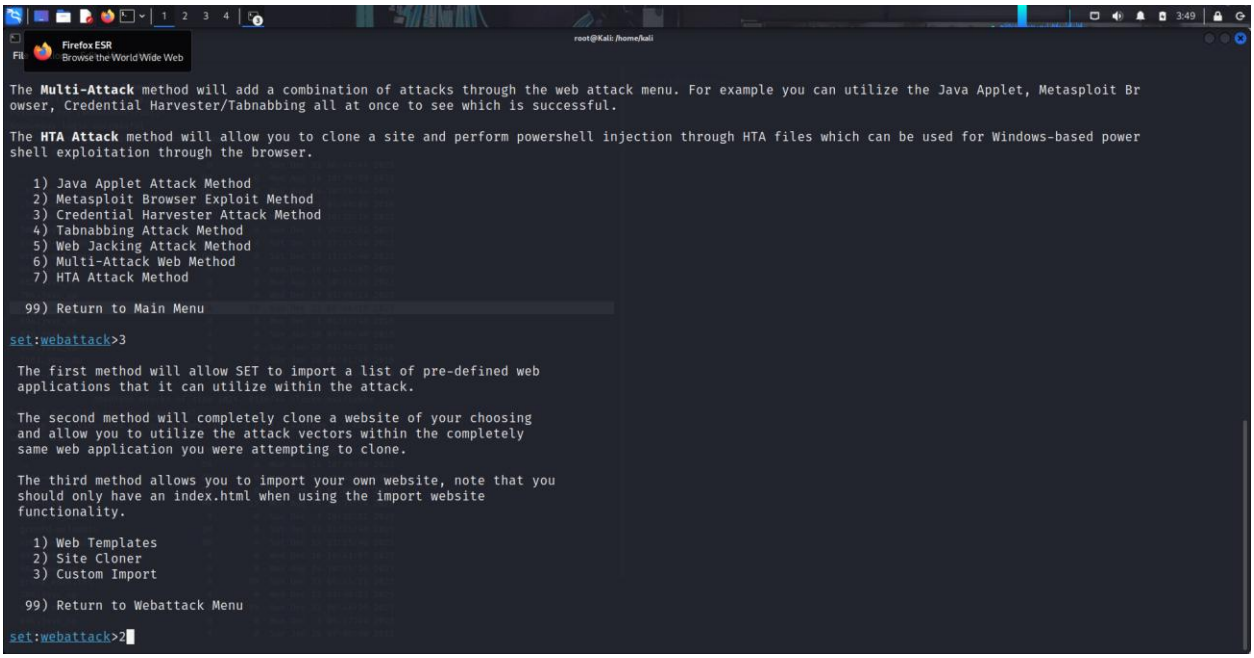
In this this lab we will create a perfect clone of a website.
Website cloning refers to creating a fake copy of a legitimate website to deceive users or harvest sensitive information. It is a common technique used in phishing, social engineering, credential theft, and fraud and for this lab's purpose we want to capture credential login details.

From the step below we use **Setookit** to access the social engineering menu.

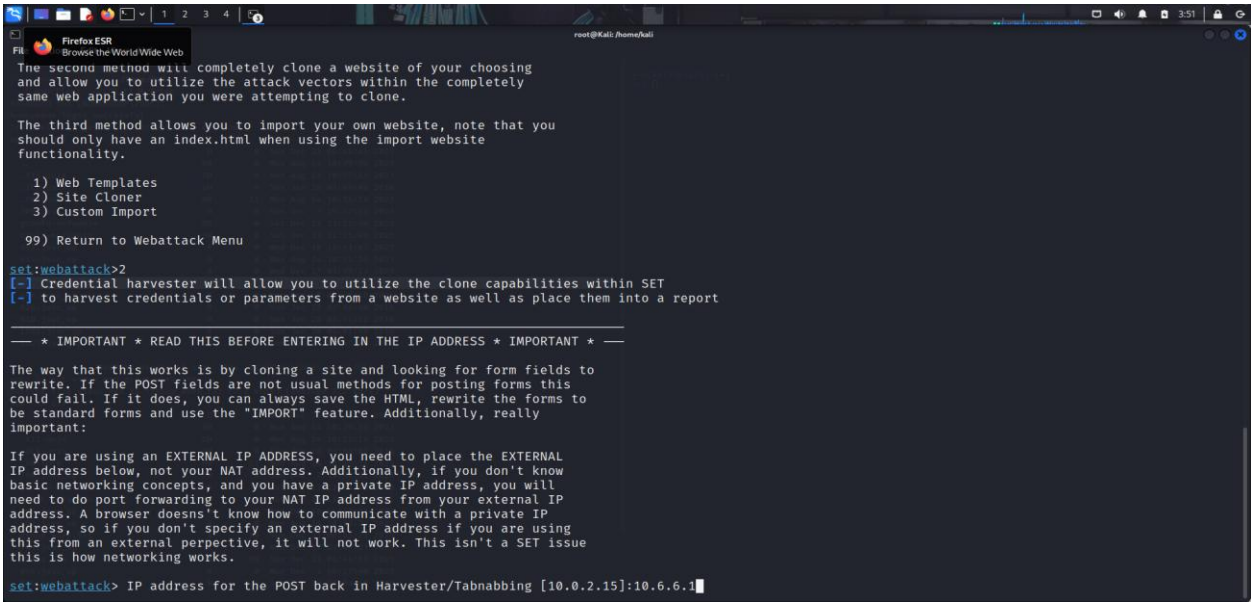




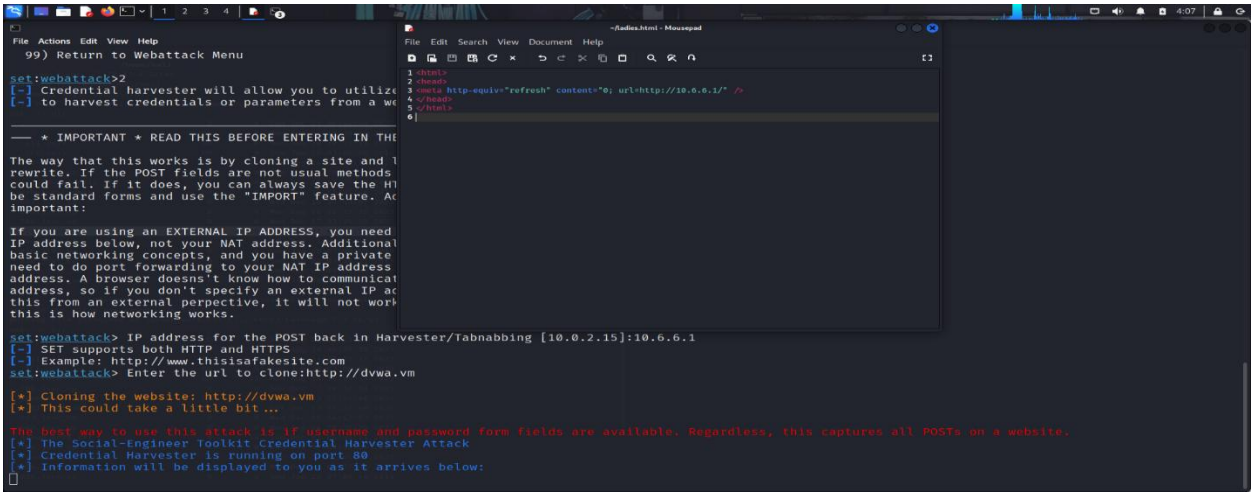

root@Kali: /home/kali
File Actions Edit View Help
99) Return back to the main menu.
set> 2
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.
The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thom as Werth to deliver the payload.
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.
The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information po sted to the website.
The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.
The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.
The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Br owser, Credential Harvester/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based power shell exploitation through the browser.
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu
set:webattack>3


root@Kali: /home/kali
Firefox ESR
Browse the World Wide Web
The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Br owser, Credential Harvester/Tabnabbing all at once to see which is successful.
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based power shell exploitation through the browser.
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method
99) Return to Main Menu
set:webattack>3
The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.
The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.
The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>2

After we are done with the steps above which help us choose the correct options for this lab. We can put the IP Address of the website we are cloning.

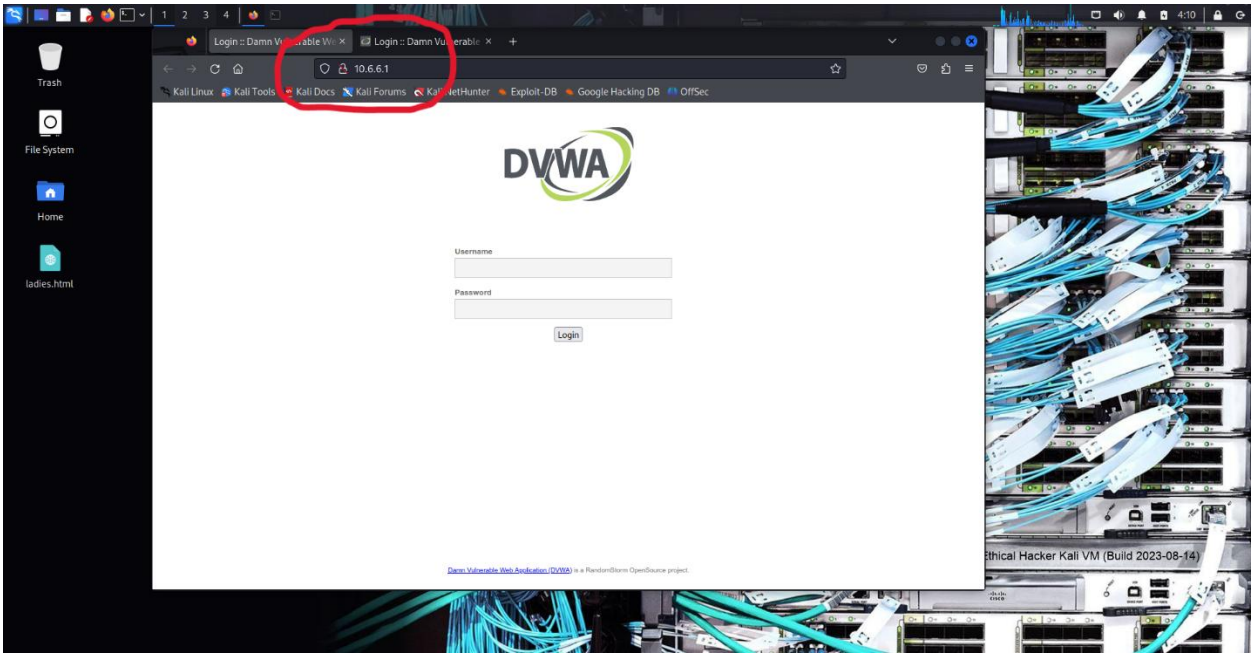


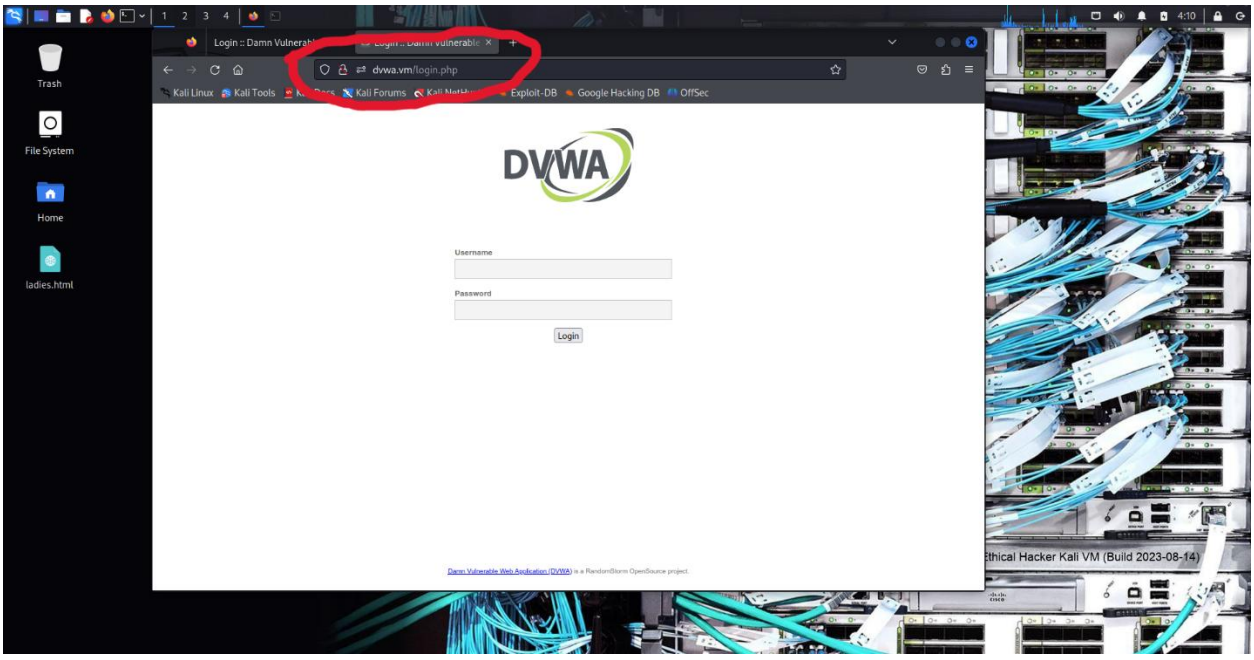
After we put the IP Address, we then enter URL of the website we want to clone which in this case is http://DVWA.vm. A listener is now active on Port 80 on the kali computer and all port 80 traffic will be redirected on this screen.



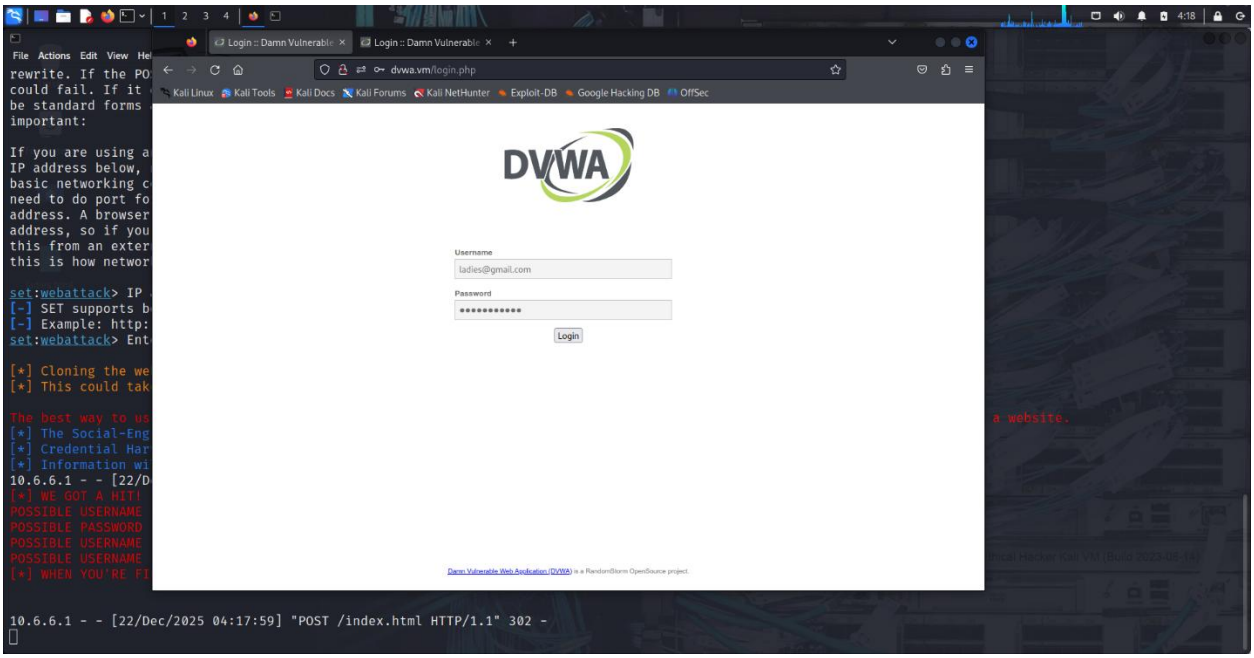
Lasty, we open a text file to write some html code which is the clone of the website we want to clone for the lab. However, in a real-life exploit in this step a phishing exploit containing a link or QR code that sends the user to the fake website is created and sent.

I the steps below we have 2 websites which are Identical but 1 is the original and other is a clone of the original. As we can see the upper website shows the IP address instead of the correct URL, this is the fake website and the 1 with the URL is the original.





Below we enter the login details and press login. The cloned webpage redirects the browser to the real web site (see the url below is now of the real website). However, the users' real credentials have been provided to the hacker's clone of the original website.



Below we see the login credentials have been captured by the listener.