**EXPERIMENT-6**

**PASSWORD SNIFFING**

**Password Sniffing**

Password Sniffing is a hacking technique that uses a special software application that **allows a hacker to steal usernames and passwords simply by observing and passively recording network traffic**. This often happens on public Wi-Fi networks where it is relatively easy to spy on weak or unencrypted traffic.

**Tools**:

* Kali Linux
* Wire shark

: Wireshark is a widely used tool for network traffic analysis and can also be used to find credentials which are transported in plain text.

**Step1**:

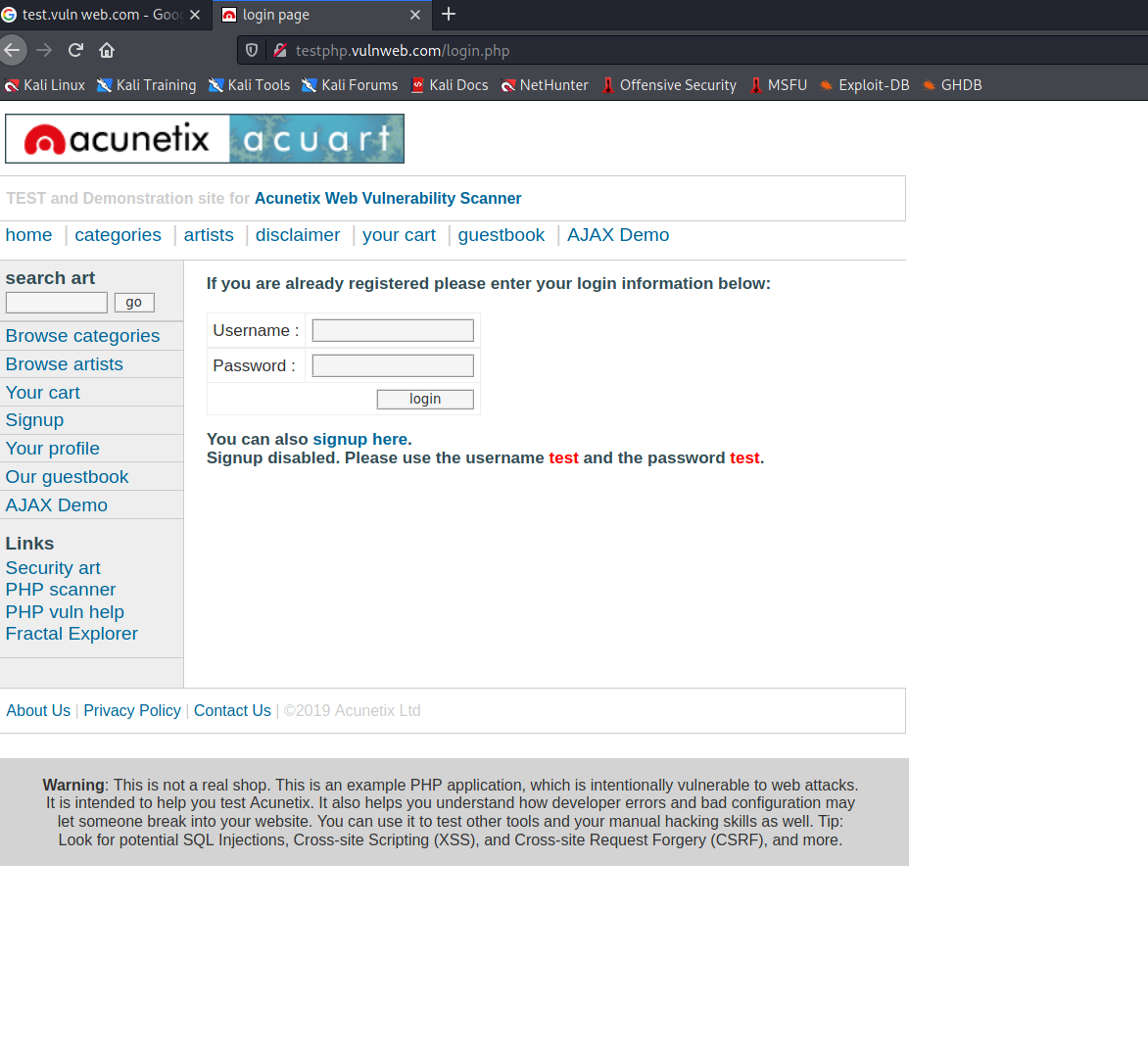


Figure 6.1

* First, Open a web browser and type a **HTTP** website “<http://testphp.vulnweb.com/login.php>”

**Step2:**

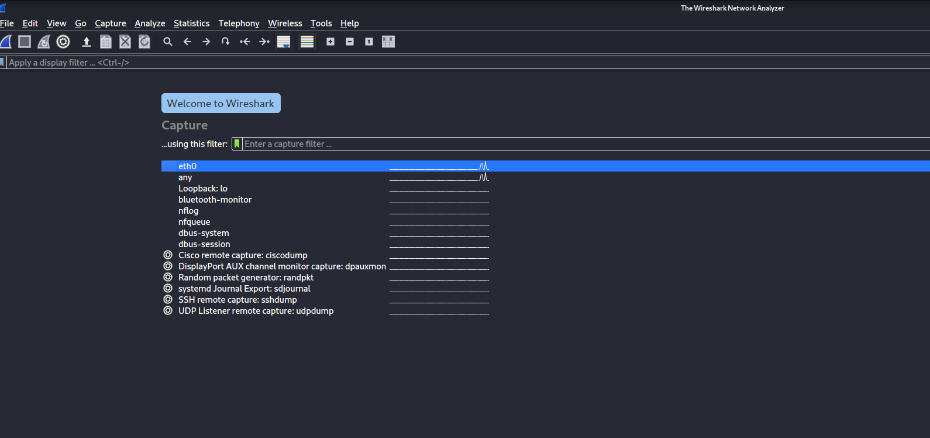


Figure 6.2

* In step2 we open Wireshark network sniffing tool on kali Linux.
* Then we click on **blue** button on **Top left** corner.

**Step3:**

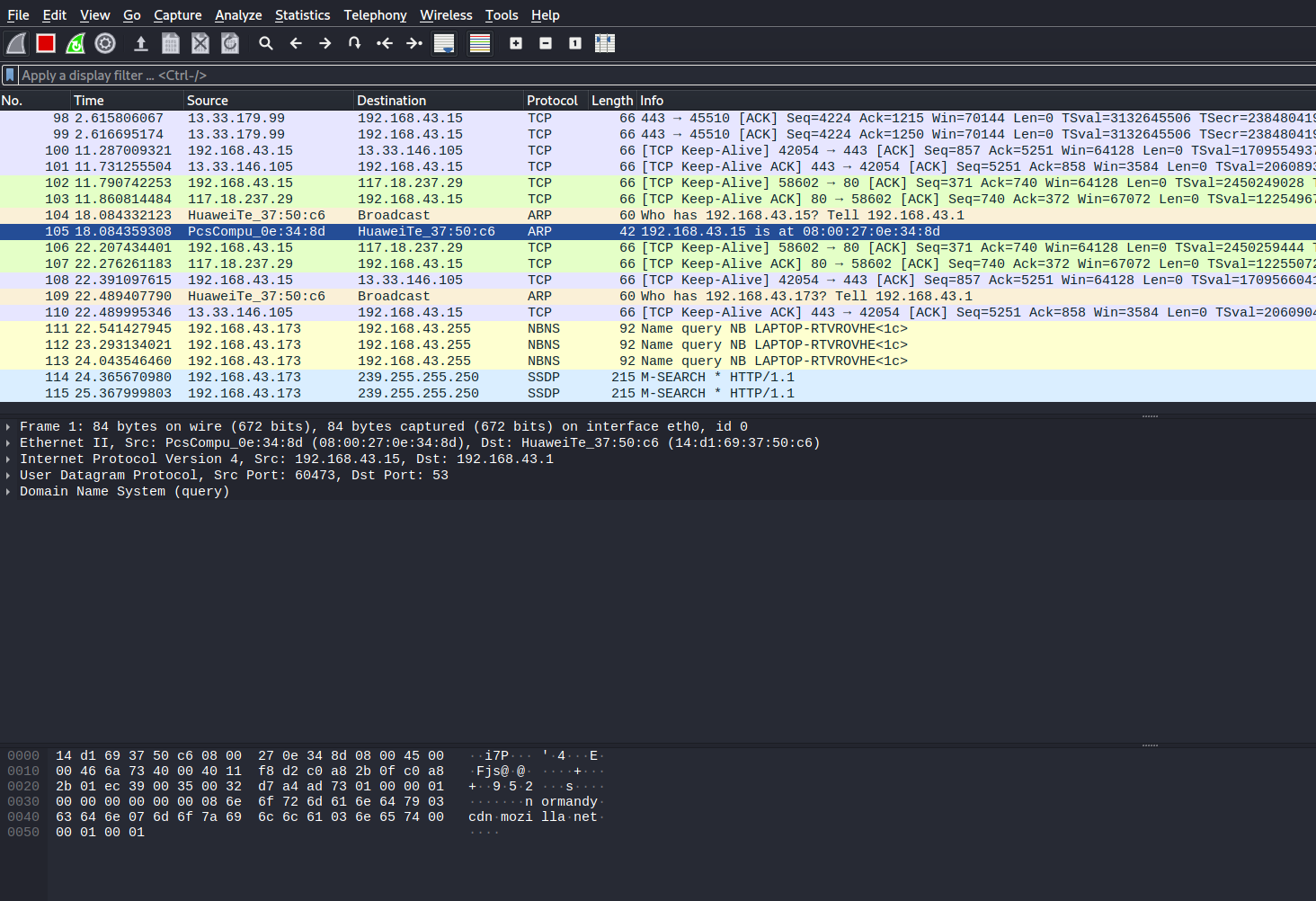


Figure 6.3

* After clicking the blue button, the wire shark tool captures the network packet on this particular LAN network.

**Step4:**

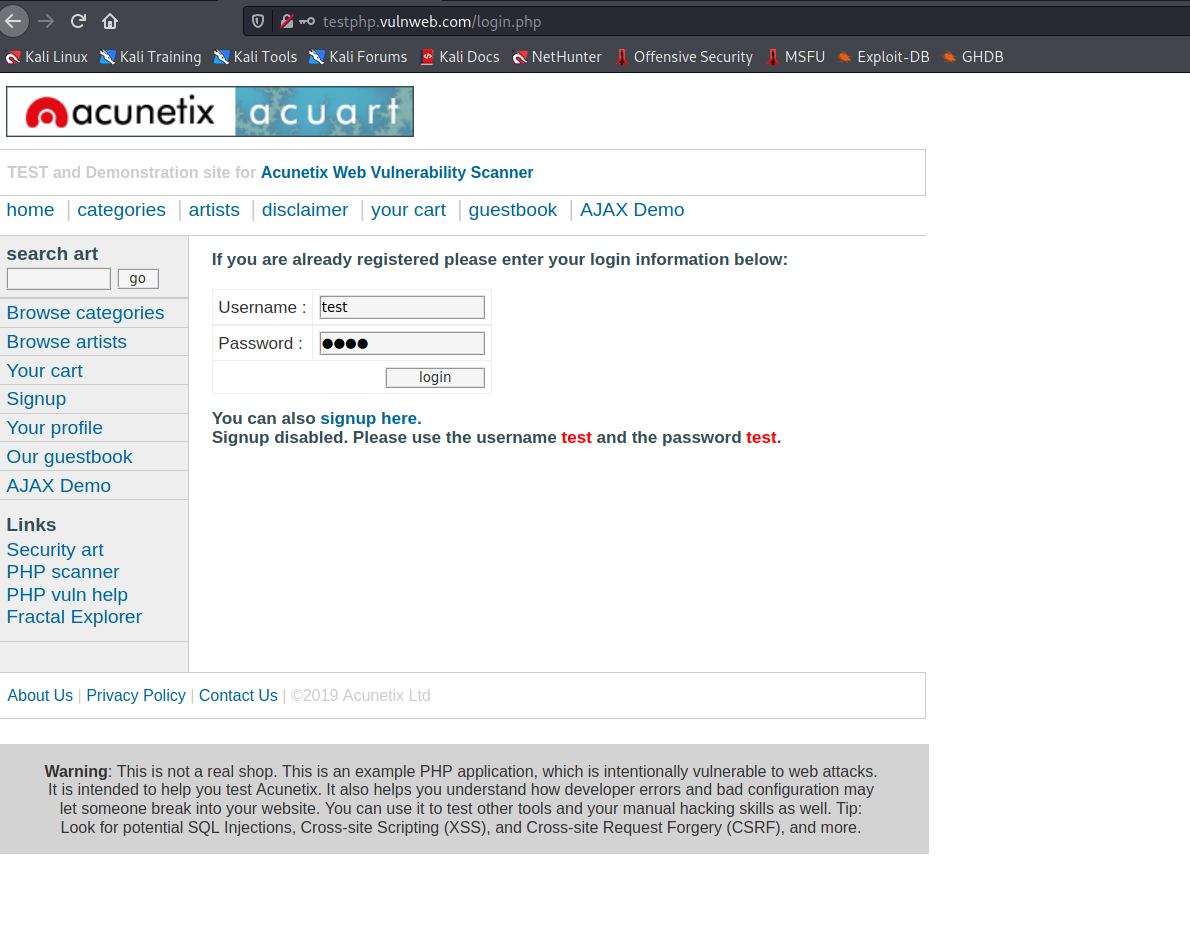


Figure 6.4

* Now we type username and password on this website and login.
* Username is **test** and the password is **test**.

**Step 5:**

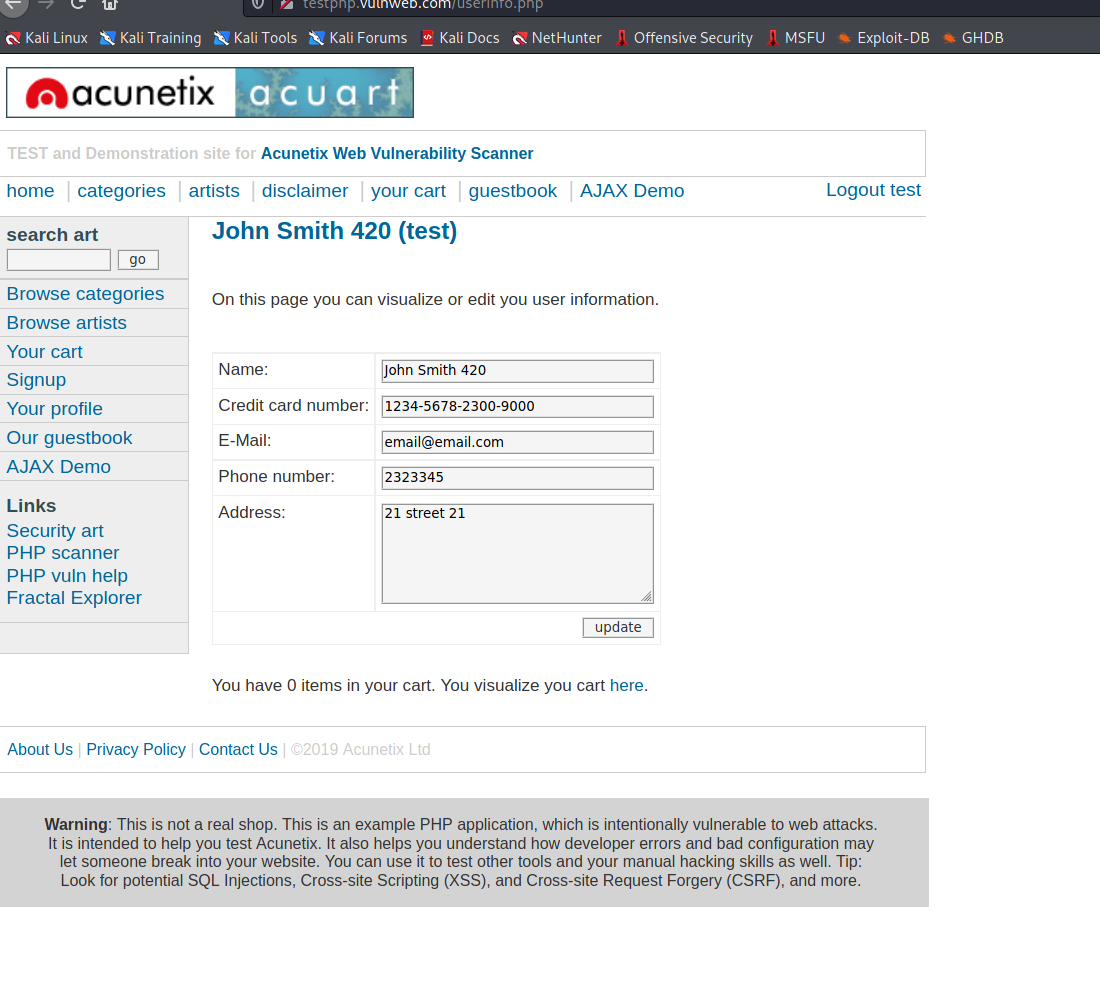


Figure 6.5

* Now we Logged in the website.

**Step 6:**

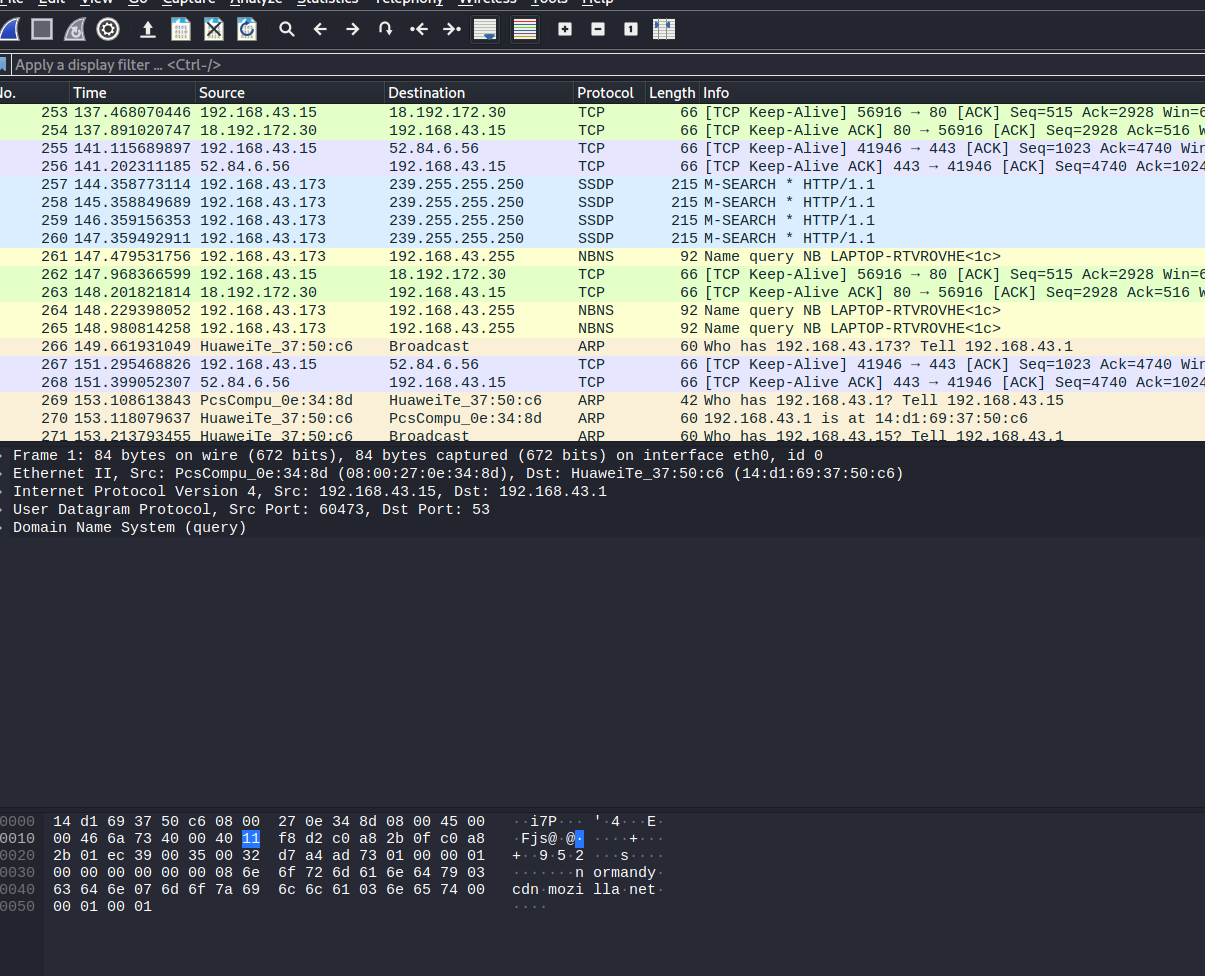


Figure 6.6

* After login we came back to the Wireshark tool and click on red button near by the blue button.
* After clicking the red button Wireshark stop capturing the packet in the particular network.
* Now we ready to analyses the network packet.

**Step 7:**

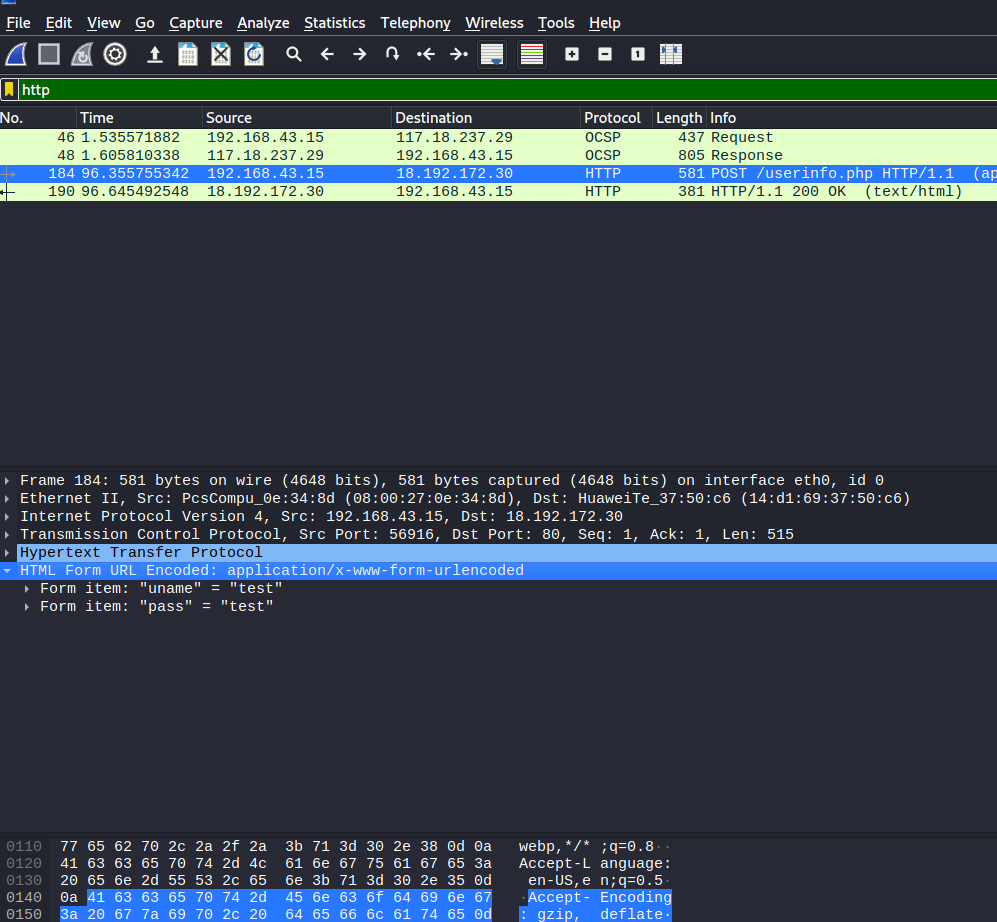


Figure 6.7

* After stop the network sniffing, we click on **Apply a display filter** and type **http**.
* After type http it show all http request on the network which are requested by the client to server.
* Then we check all the **http request packets** and we find the **username** & **password** which we are used to logged in a http website.

**Result:**

The username and password was obtained.