**Day 16**

**Exploitation Analyst**

**Hacking HTTP protocol:**

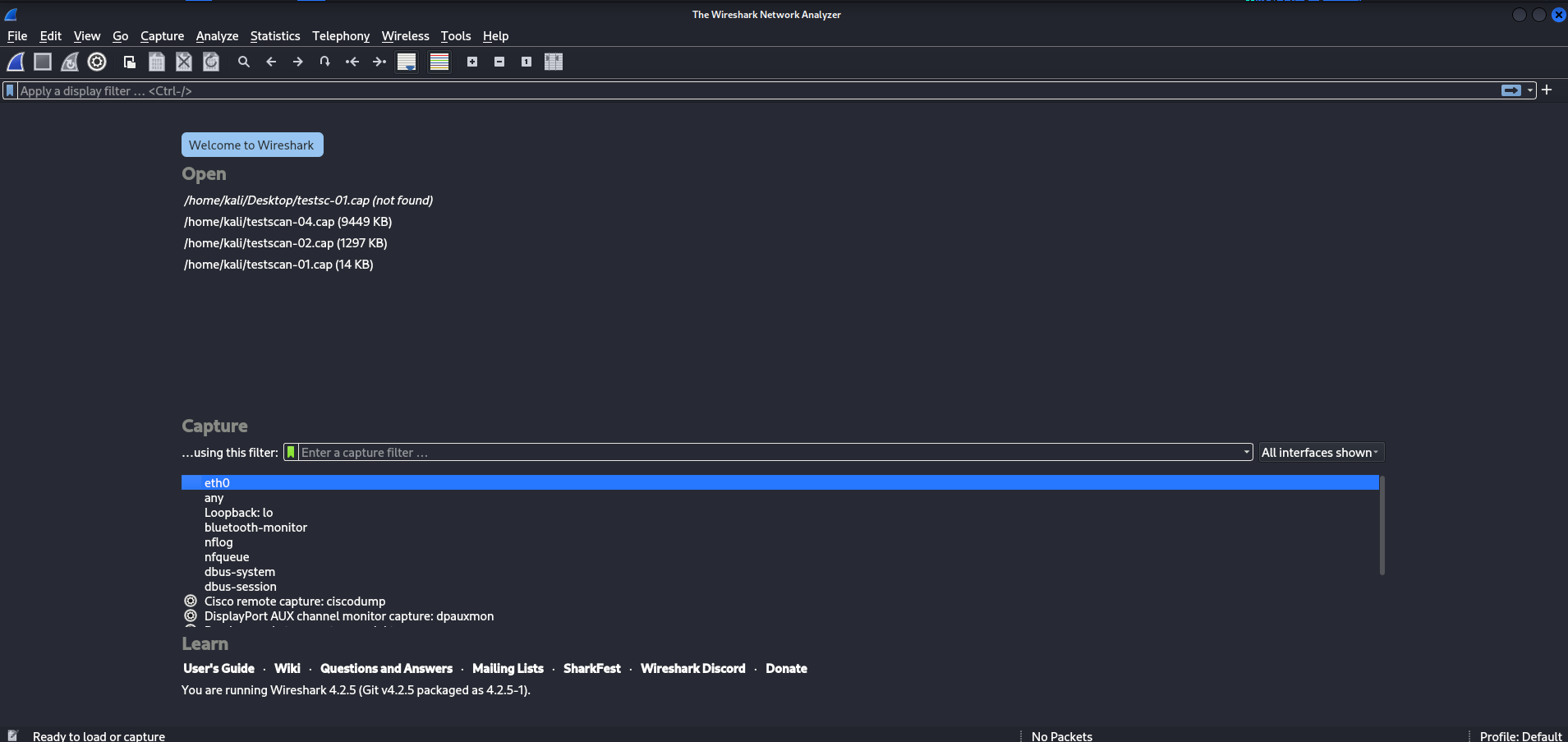
**Why hacking HTTP is so easy?**

* HTTP exposes everything in cleartext — headers, cookies, content.
* It can be intercepted or modified using tools like:
  + Wireshark
  + Burp Suite (Proxy)
  + mitmproxy

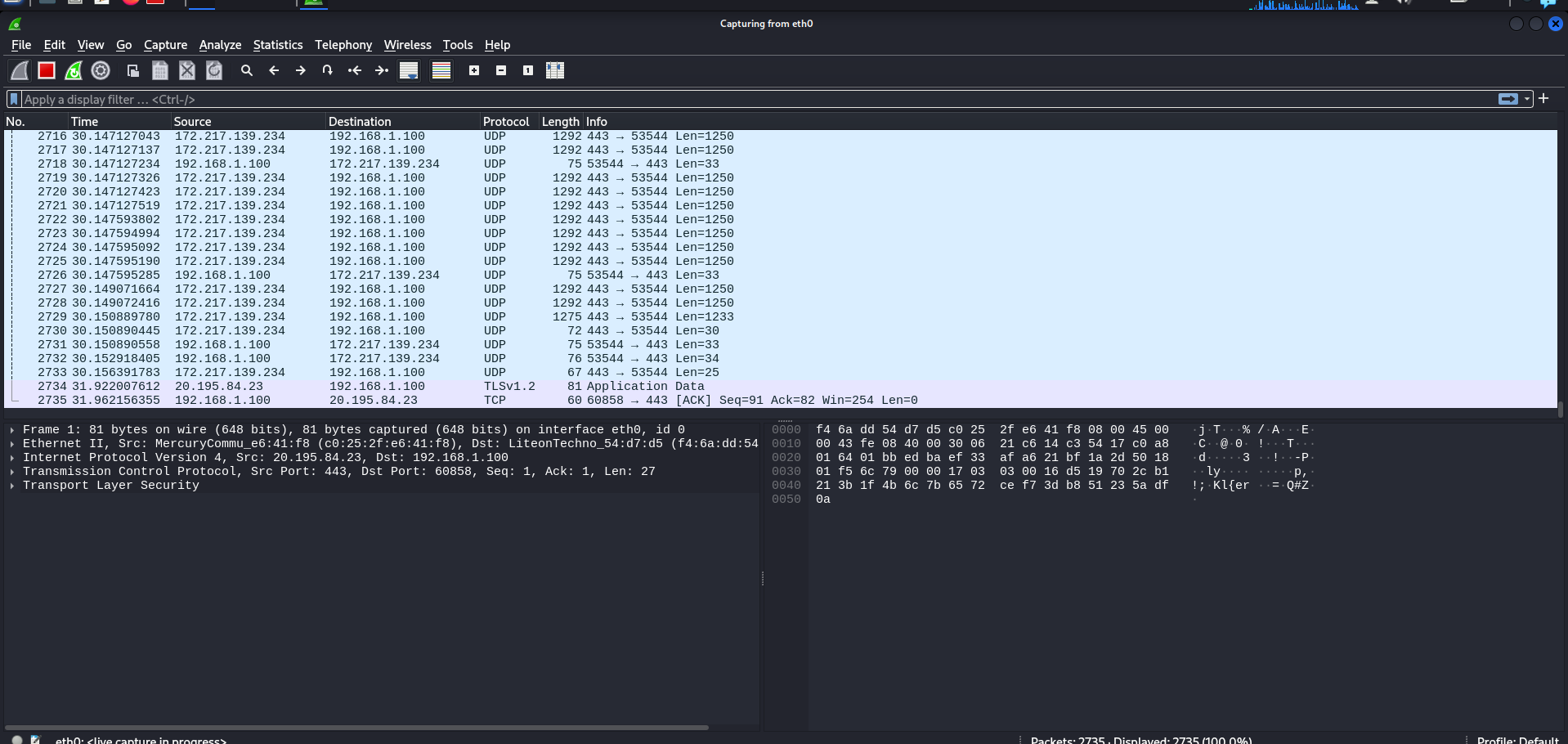
**Sniffing password using Wireshark for websites using HTTP:**

Steps:

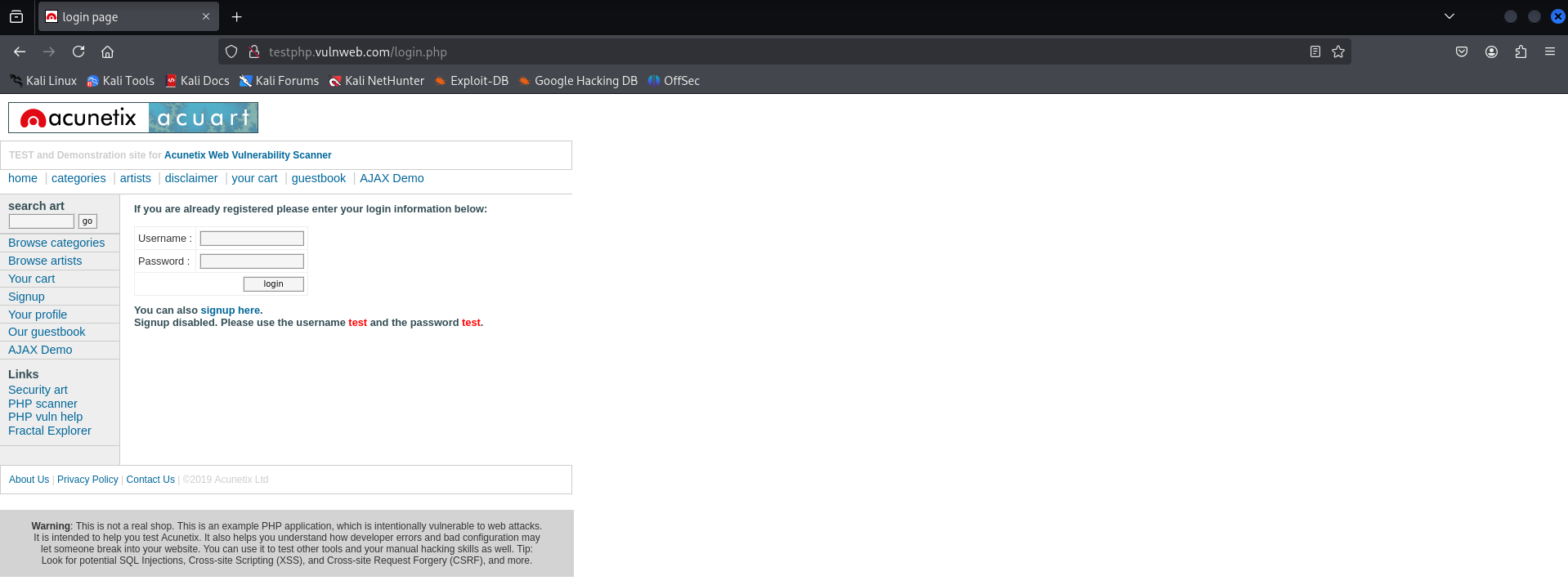
Open Wireshark:



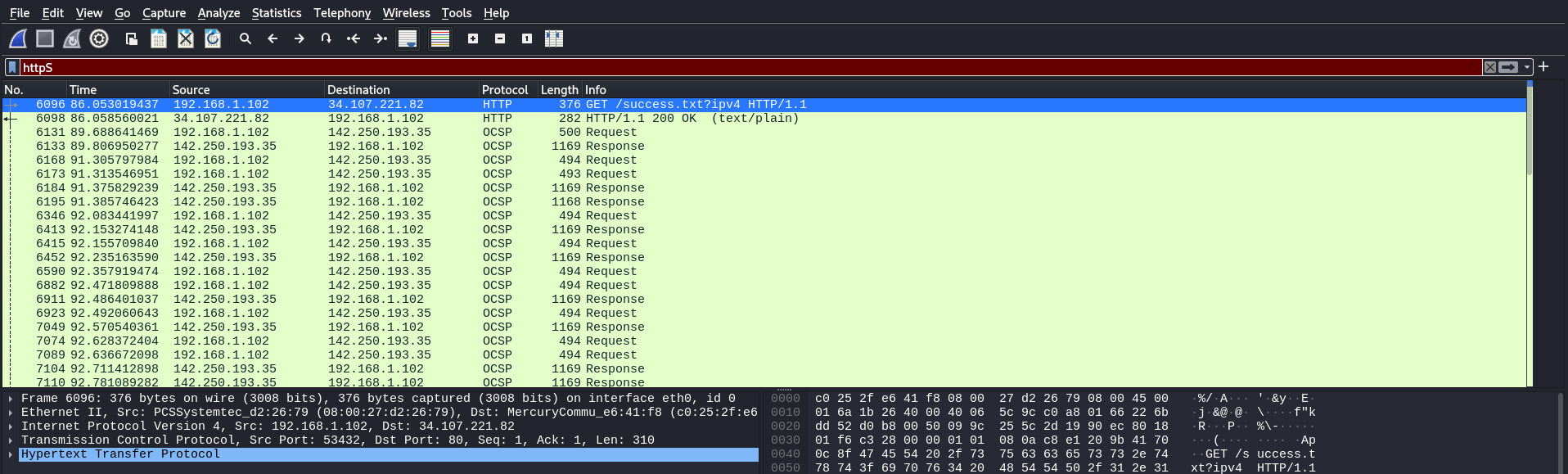
Click on ‘eth0’: following window will appear.

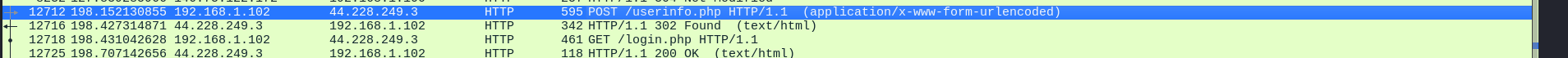


Meanwhile open the following website in the browser: enter user name and password, and click on login button. http://testphp.vulnweb.com/login.php

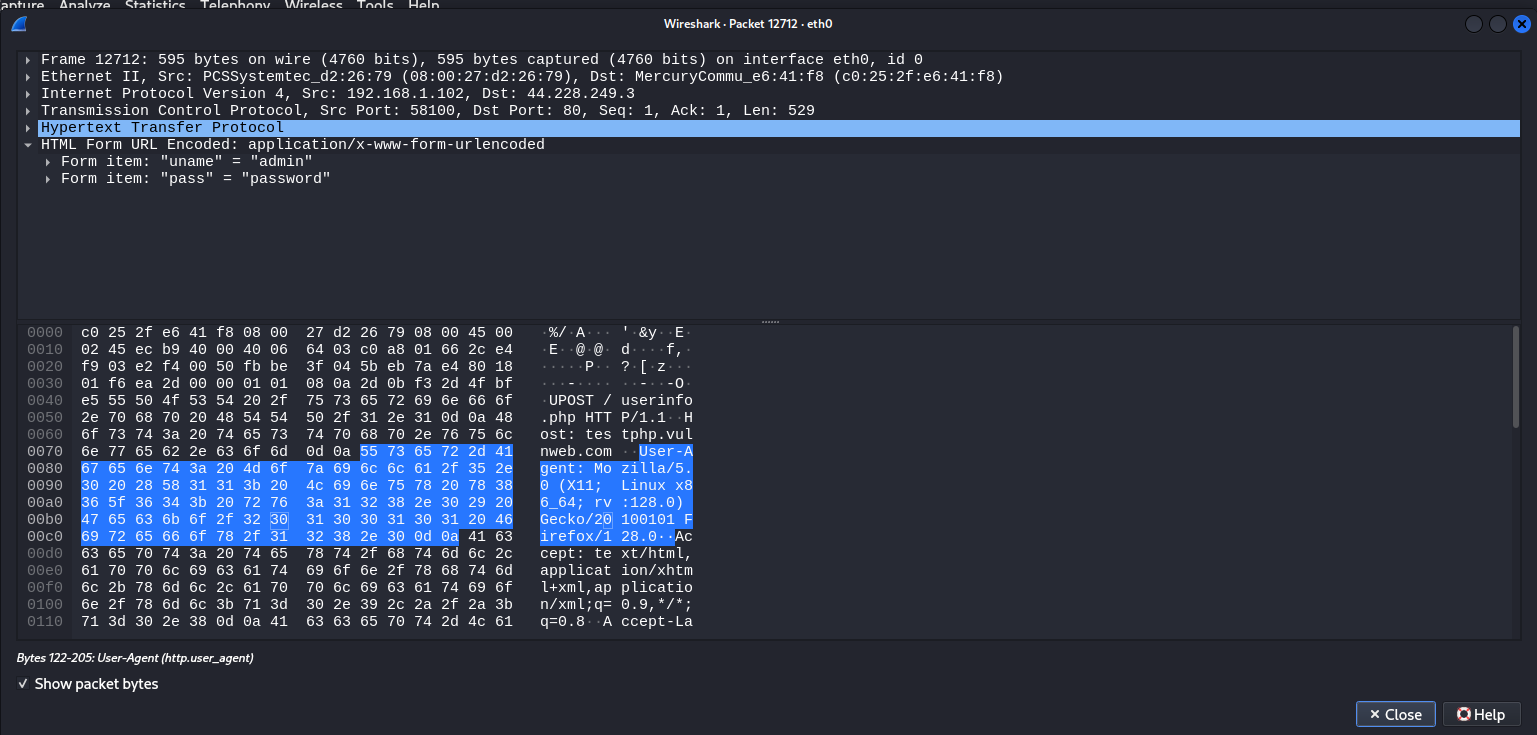


Now, go to Wireshark and click on the red button to stop capturing the packets, and then in the filter bar, type HTTP to filter out the HTTP packets:



Look for the packet whose info says ‘post’: we found it.

Click on the packet, a new popup screen will appear, here we can see the credentials we had entered on the website:

****