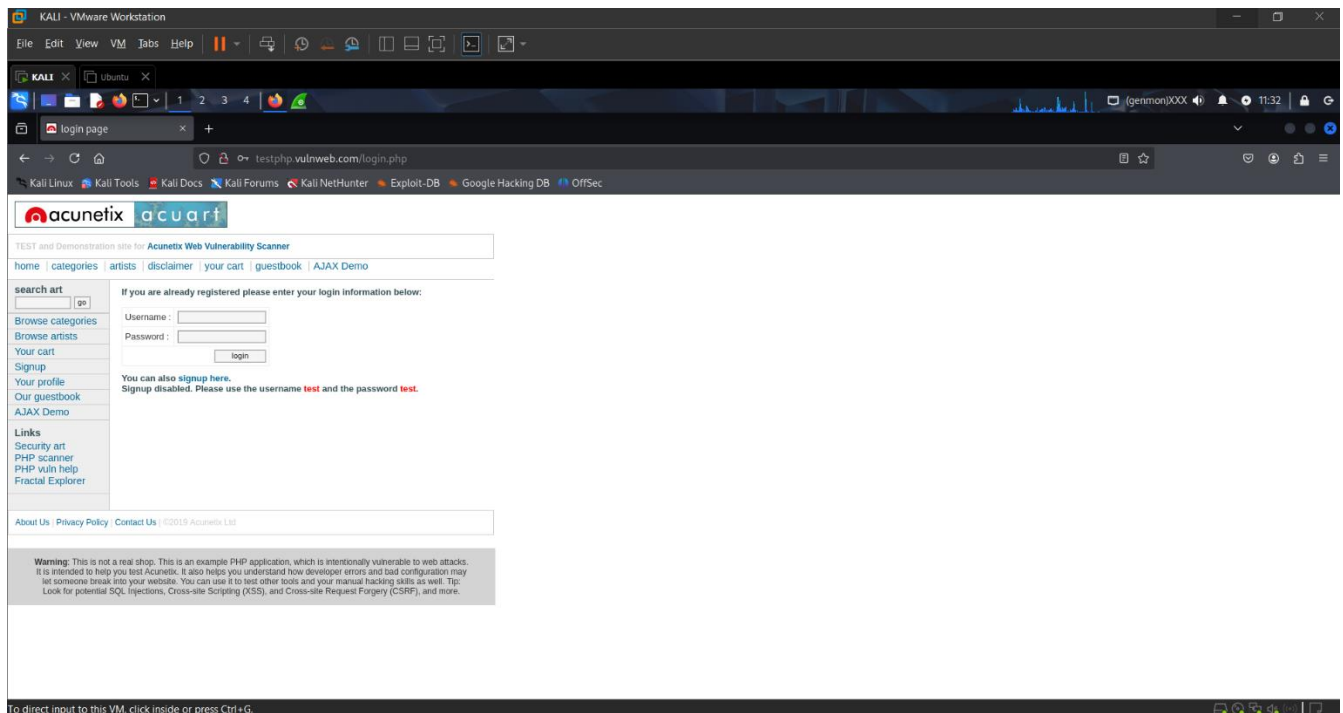


Network Packet Sniffing and Analysis

Capturing and analyse live network traffic to identify credentials or suspicious activity by Wireshark tool.

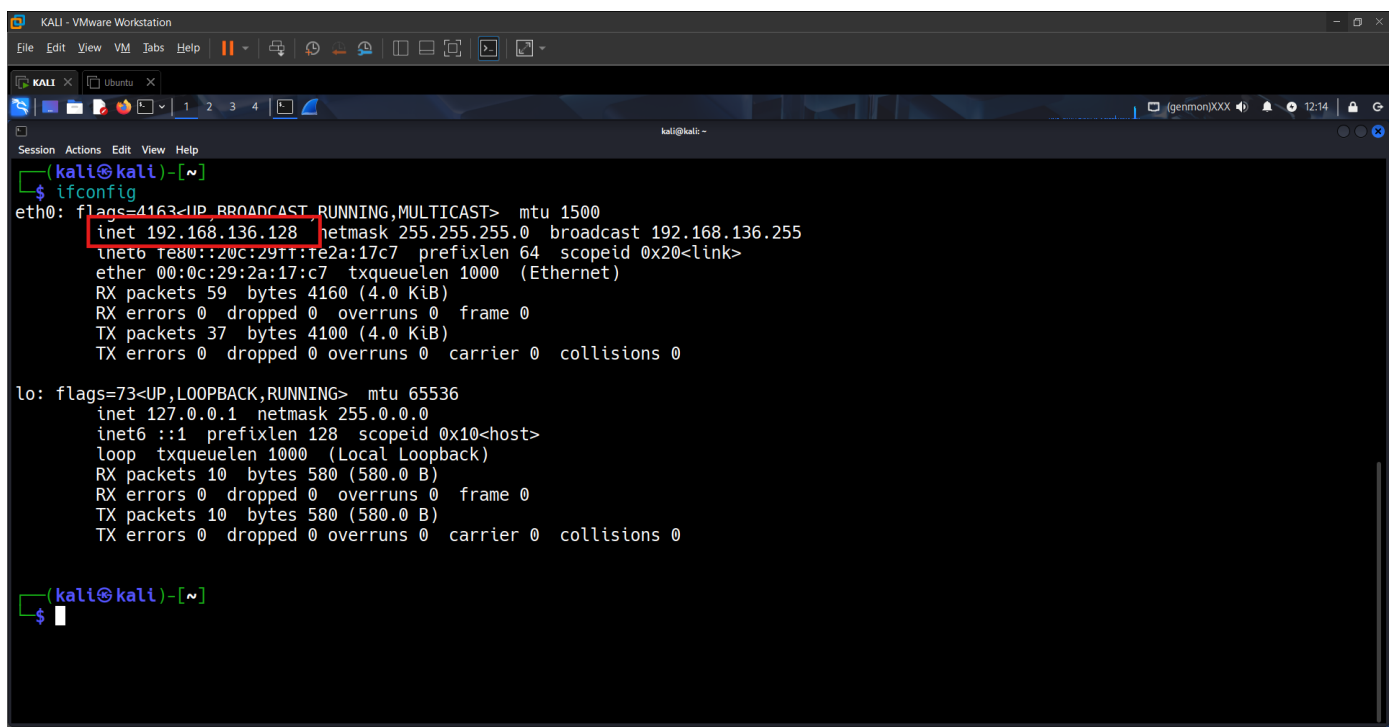
Target: vulbweb.com

Target IP: 44.228.249.3

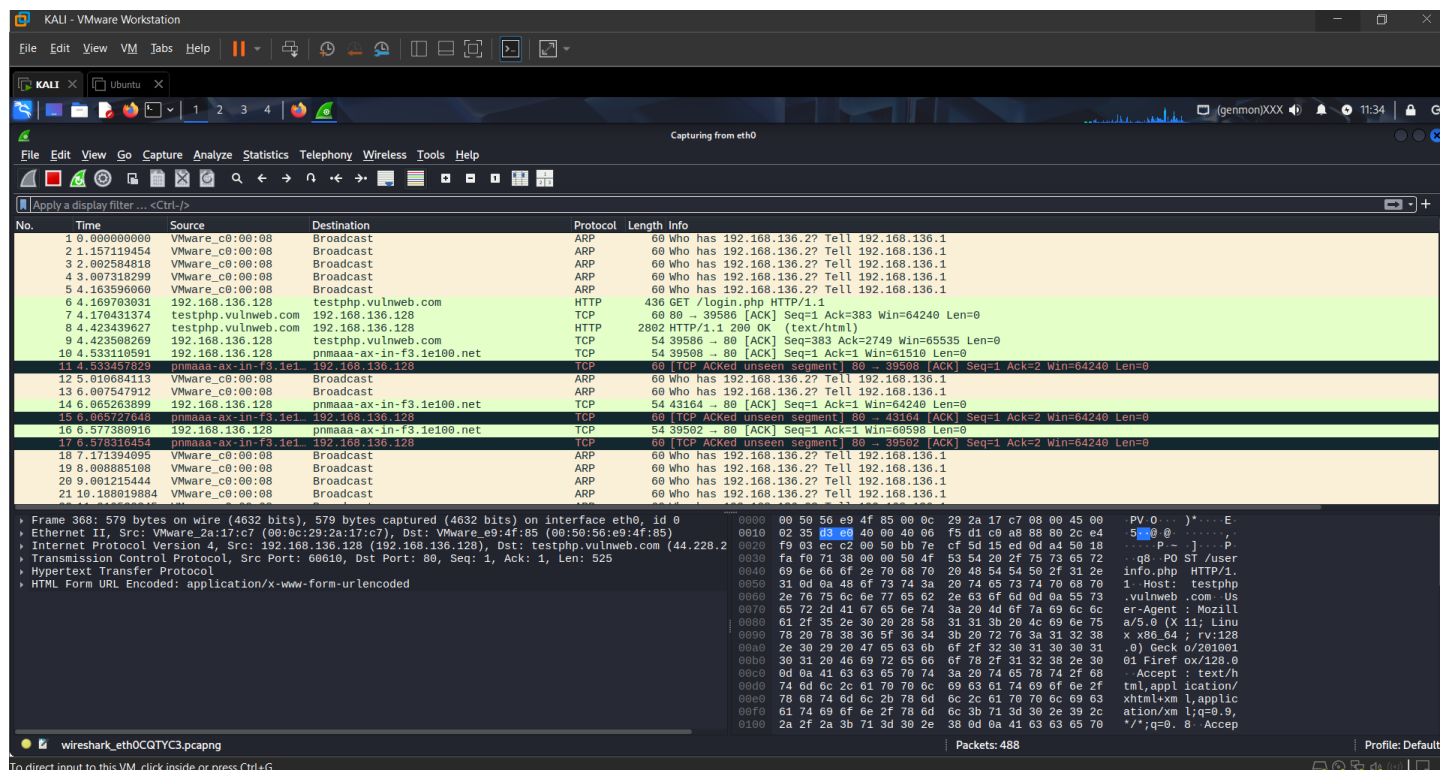


Attacker: kali Linux

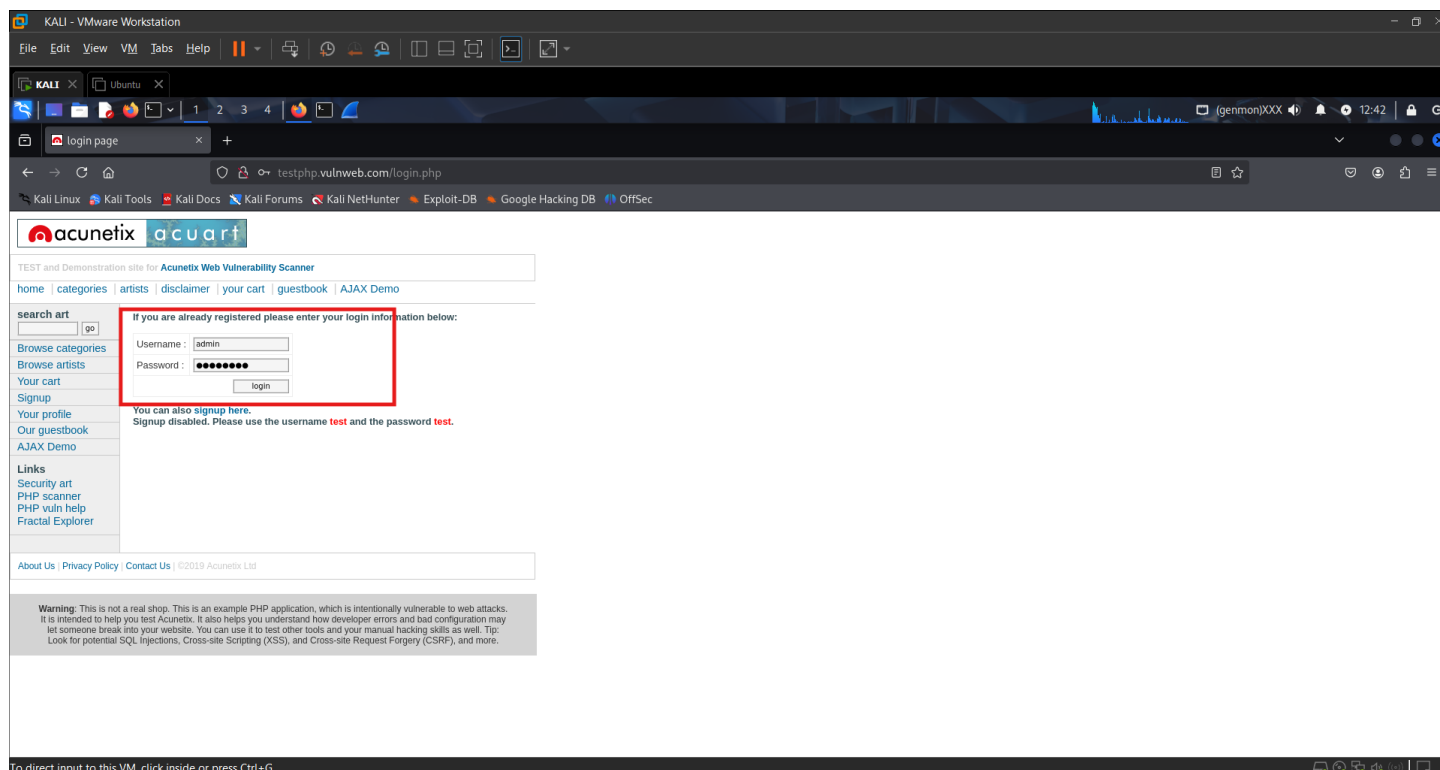
Attacker IP:192.168.136.128



The packets in below image are traffic generated by Wireshark tool



Now try to login with random credentials in target website (vulnweb).

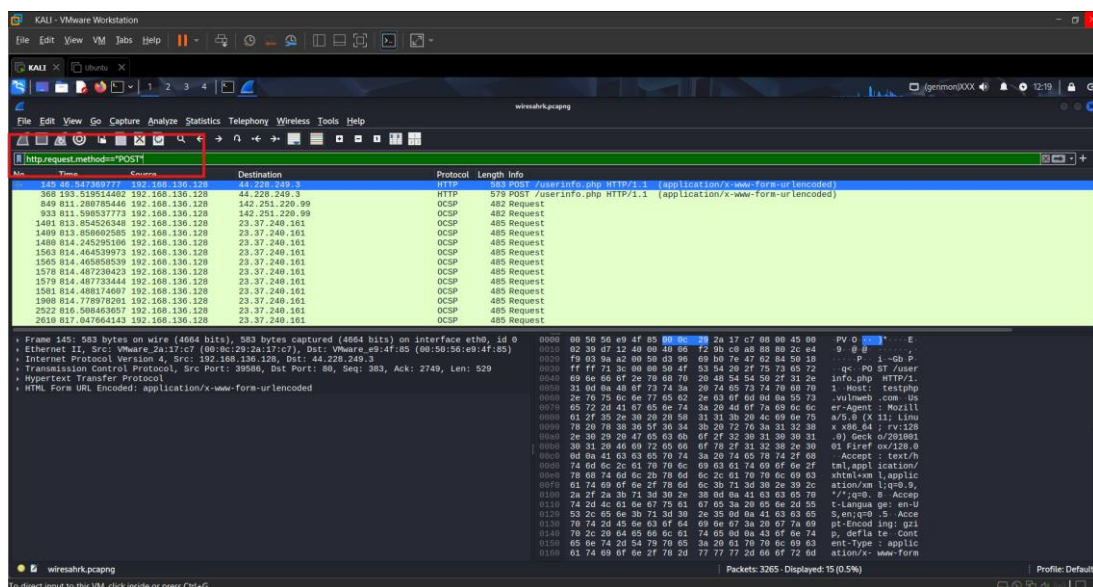


Now to inspect the packets we use filter to limit the packets to make the task easy.

Filter: http.request.method=="POST"

This filter will show packets which are http request and POST method.

POST method is where we send data to server, when we enter the credentials or user input then it is said to be POST method.



The 1st packet we had packet name “/userinfo.php” with HTTP (Hyper Text Transfer protocol) protocol.

In Transmission Control Protocol, we have

Source Port: 39586 (kali Linux),

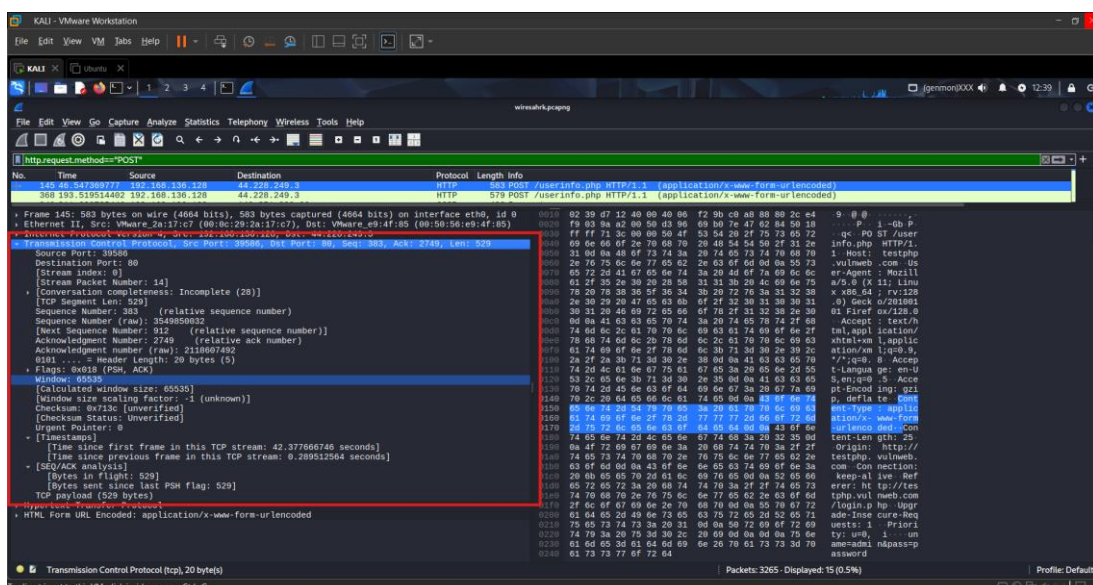
Destination Port: 80(target),

Seq: 383, Ack: 2749, Len: 529

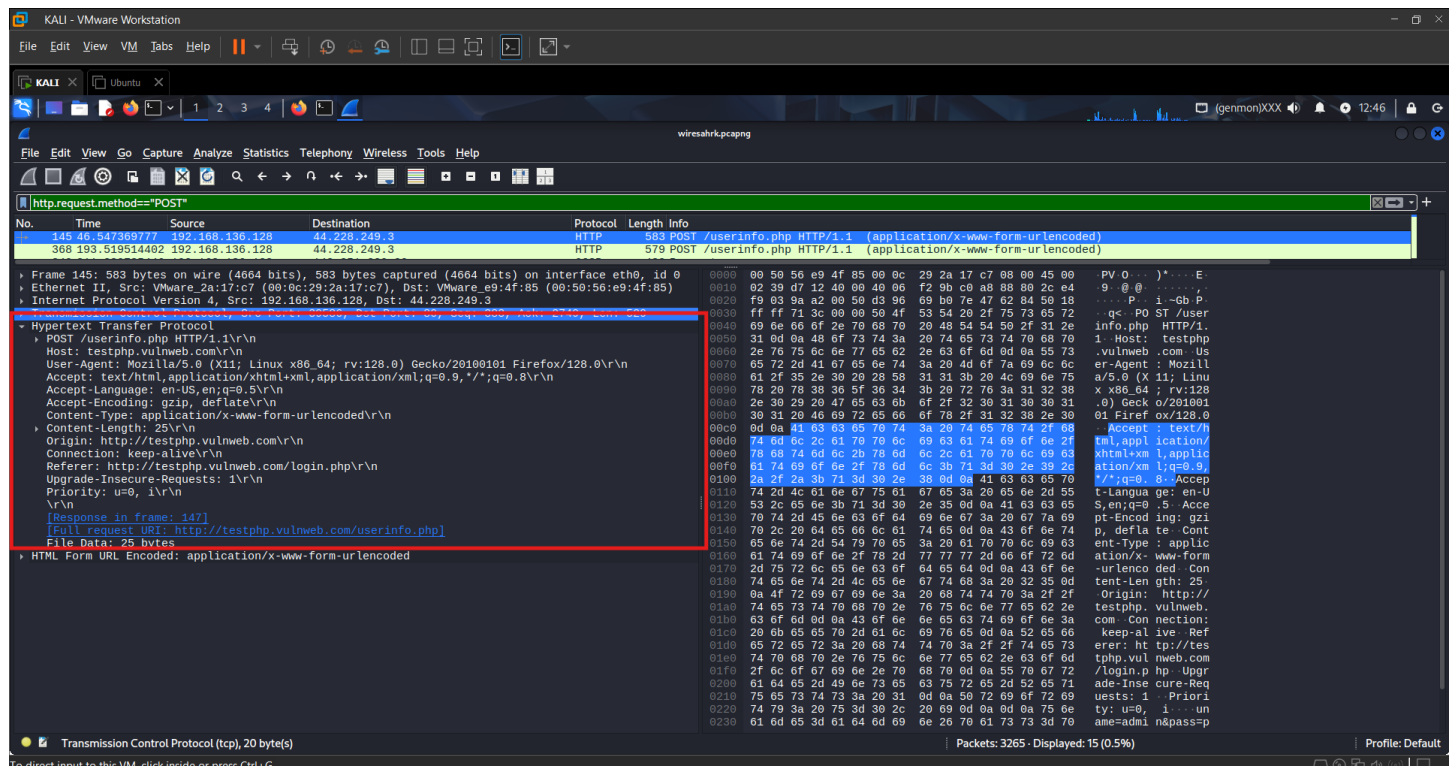
IP version: IPV4

[SEQ/ACK analysis]

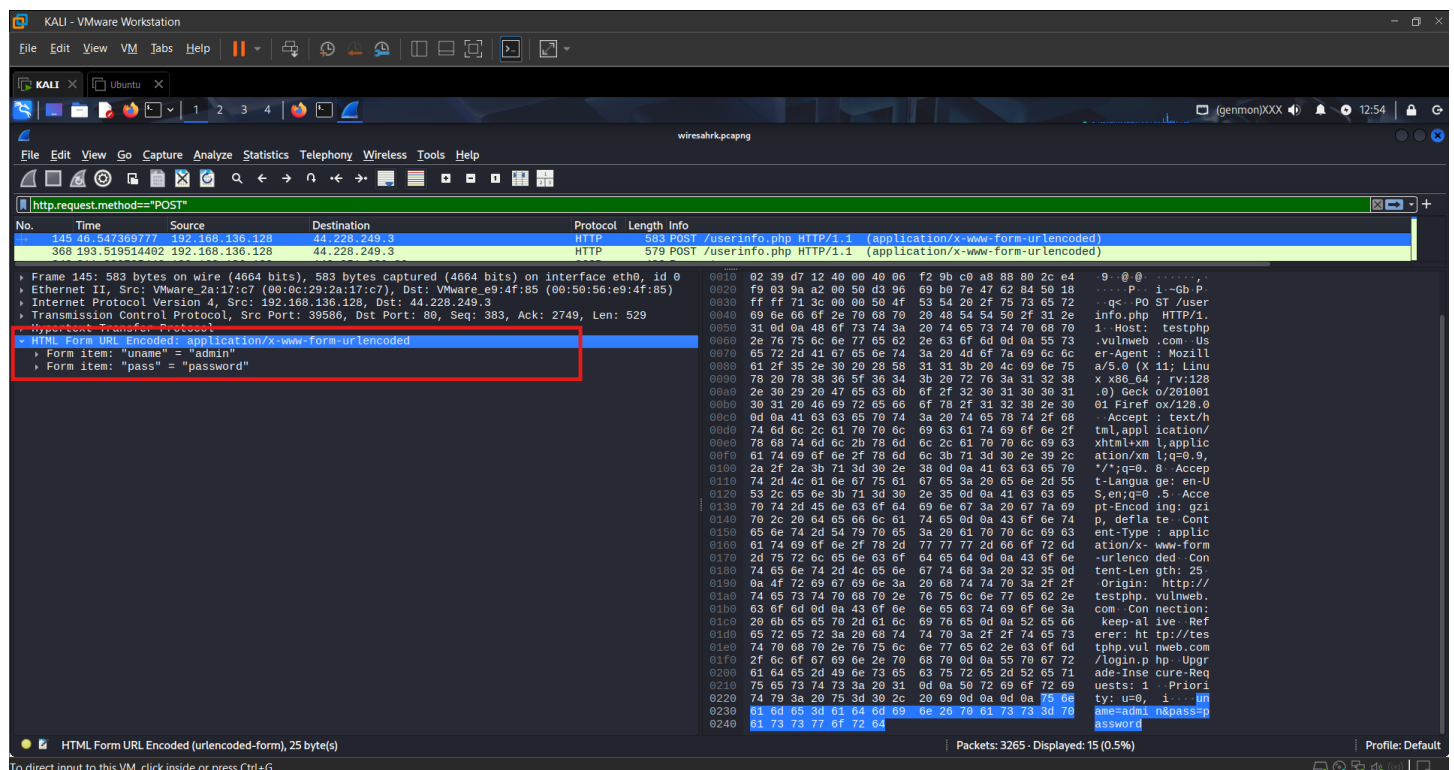
TCP payload and other details of packet as shown in below image.



If we inspect Hypertext Transfer Protocol we have version, URL and other details of target website as shown in below image.



If you see HTML form URL Encoded, inspect it there you will see the plain text of credentials you gave in target website as shown in below image.



This says the website is vulnerable as the website discloses the credentials in a plain text.

Let's check on other website