

Cyber Security

Class no 04 (Theory 2)

19 Sep 2024

Lab Part:

wireshark

- tcp
- ip.addr
- ip.addr == 192.168.68.126
- ip.src == 192.168.68.126
- wireshark → statistics → http
- testphp.vulnweb.com/login.php then type user id and password of any
 - then go to wireshark and type `http.request.method == "POST"`
 - find HTTP /userinfo.php
 - then goto HTML Form URL Encoded: will be find user id and password

The image shows a Wireshark network traffic capture. The top toolbar has a filter icon highlighted with a red arrow. The filter bar contains the text `http.request.method == "POST"`. The packet list shows a series of OCSP requests, followed by a highlighted packet 7722: 714 bytes on wire (5712 bits), 714 bytes captured (5712 bits) on interface eth0, id 0. This packet is an HTTP POST request to /userinfo.php. The packet details pane shows the following structure:

- Frame 7722: 714 bytes on wire (5712 bits), 714 bytes captured (5712 bits) on interface eth0, id 0
- Ethernet II, Src: PCSSystemtec_08:25:c8 (08:00:27:08:25:c8), Dst: fa:a5:d0:0a:d3:19 (fa:a5:d0:0a:d3:19)
- Internet Protocol Version 4, Src: 192.168.43.3, Dst: 44.228.249.3
- Transmission Control Protocol, Src Port: 48082, Dst Port: 80, Seq: 1, Ack: 1, Len: 648
- Hypertext Transfer Protocol
- HTML Form URL Encoded: application/x-www-form-urlencoded
 - Form item: "uname" = "murubbi.uhu.uhu"
 - Form item: "pass" = "hellow"

The packet bytes pane shows the raw data in hexadecimal and ASCII format.