

Password Sniffing Using Wireshark

@mmar



Http and FTP are both unencrypted protocols and if we are able to capture their traffic, we can extract the credentials from them

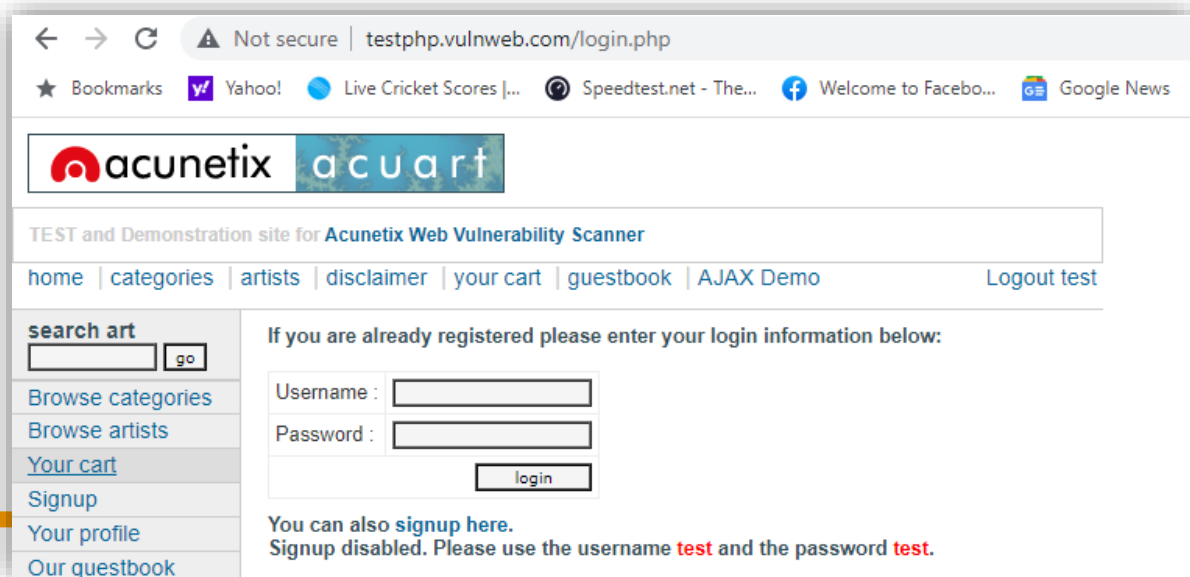


Analysing HTTP Traffic

Analyse HTTP

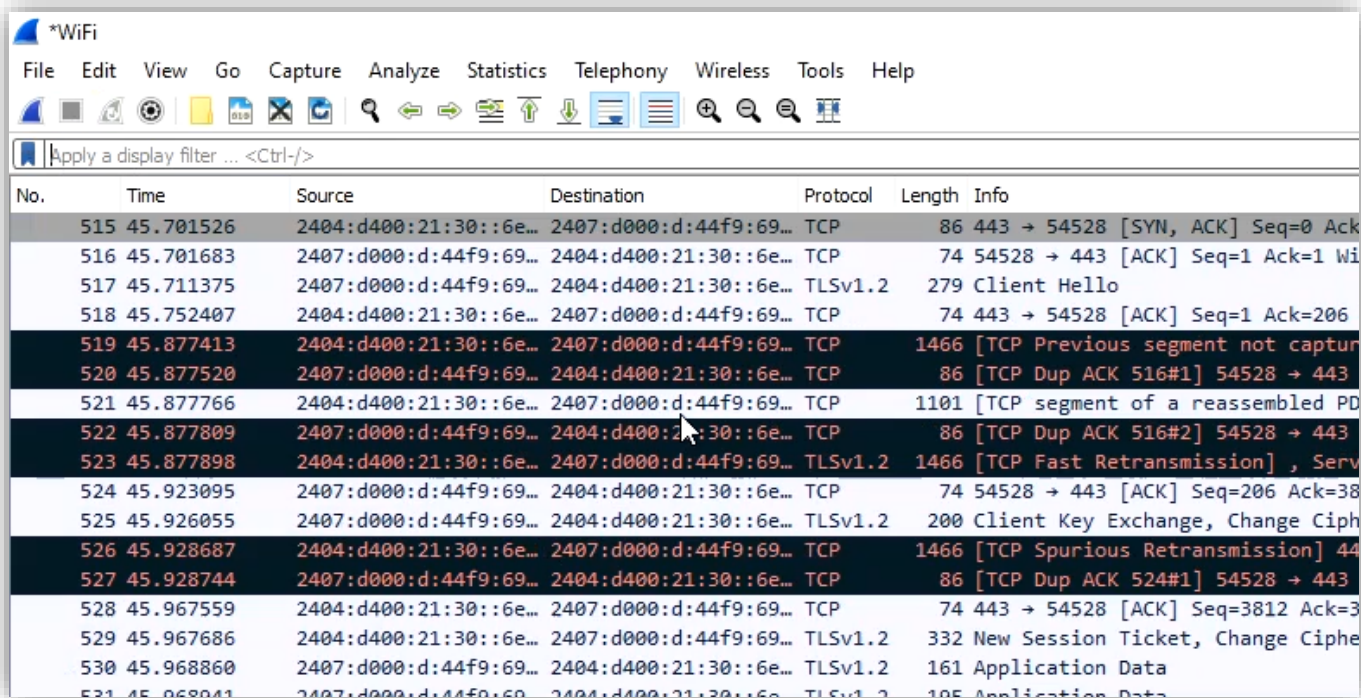
- ❖ Visit the following website. The site operates on Http only and thus allows us to capture traffic in plain text

<http://testphp.vulnweb.com/>



Analyse HTTP

- ❖ Now Open Wireshark and capture the traffic. Now login on the site. The traffic will be captured in Wireshark



No.	Time	Source	Destination	Protocol	Length	Info
515	45.701526	2404:d400:21:30::6e...	2407:d000:d:44f9:69...	TCP	86	443 → 54528 [SYN, ACK] Seq=0 Ack
516	45.701683	2407:d000:d:44f9:69...	2404:d400:21:30::6e...	TCP	74	54528 → 443 [ACK] Seq=1 Ack=1 Wi
517	45.711375	2407:d000:d:44f9:69...	2404:d400:21:30::6e...	TLSv1.2	279	Client Hello
518	45.752407	2404:d400:21:30::6e...	2407:d000:d:44f9:69...	TCP	74	443 → 54528 [ACK] Seq=1 Ack=206
519	45.877413	2404:d400:21:30::6e...	2407:d000:d:44f9:69...	TCP	1466	[TCP Previous segment not captur
520	45.877520	2407:d000:d:44f9:69...	2404:d400:21:30::6e...	TCP	86	[TCP Dup ACK 516#1] 54528 → 443
521	45.877766	2404:d400:21:30::6e...	2407:d000:d:44f9:69...	TCP	1101	[TCP segment of a reassembled PD
522	45.877809	2407:d000:d:44f9:69...	2404:d400:21:30::6e...	TCP	86	[TCP Dup ACK 516#2] 54528 → 443
523	45.877898	2404:d400:21:30::6e...	2407:d000:d:44f9:69...	TLSv1.2	1466	[TCP Fast Retransmission], Serv
524	45.923095	2407:d000:d:44f9:69...	2404:d400:21:30::6e...	TCP	74	54528 → 443 [ACK] Seq=206 Ack=38
525	45.926055	2407:d000:d:44f9:69...	2404:d400:21:30::6e...	TLSv1.2	200	Client Key Exchange, Change Ciph
526	45.928687	2404:d400:21:30::6e...	2407:d000:d:44f9:69...	TCP	1466	[TCP Spurious Retransmission] 44
527	45.928744	2407:d000:d:44f9:69...	2404:d400:21:30::6e...	TCP	86	[TCP Dup ACK 524#1] 54528 → 443
528	45.967559	2404:d400:21:30::6e...	2407:d000:d:44f9:69...	TCP	74	443 → 54528 [ACK] Seq=3812 Ack=3
529	45.967686	2404:d400:21:30::6e...	2407:d000:d:44f9:69...	TLSv1.2	332	New Session Ticket, Change Ciphe
530	45.968860	2407:d000:d:44f9:69...	2404:d400:21:30::6e...	TLSv1.2	161	Application Data
531	45.968941	2407:d000:d:44f9:69...	2404:d400:21:30::6e...	TLSv1.2	105	Application Data

Analyse HTTP

- ❖ Filter the Http Post request with following filter and you will be able to see the credentials

`http.request.method==POST`

The image shows a Wireshark network traffic capture. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The main display area shows a list of captured packets. The first packet is an HTTP POST request to /userinfo.php. The second packet is an HTTP POST request to /userinfo.php. The packet list is filtered with the expression `http.request.method==POST`. The details pane for the selected packet (No. 380) shows the following information:

- > Frame 380: 711 bytes on wire (5688 bits), 711 bytes captured (5688 bits) on interface \Device\NPF{...}
- > Ethernet II, Src: HonHaiPr_46:7d:c5 (70:18:8b:46:7d:c5), Dst: HuaweiTe_Se:8d:19 (c0:f6:c2:5e:8d:19)
- > Internet Protocol Version 4, Src: 192.168.18.11, Dst: 44.228.249.3
- > Transmission Control Protocol, Src Port: 54521, Dst Port: 80, Seq: 1683, Ack: 5773, Len: 657
- > Hypertext Transfer Protocol
- > **HTML Form URL Encoded: application/x-www-form-urlencoded**
 - > Form item: "uname" = "test"
 - > Form item: "pass" = "test"

The details pane also shows the raw data of the packet in hexadecimal and ASCII format.

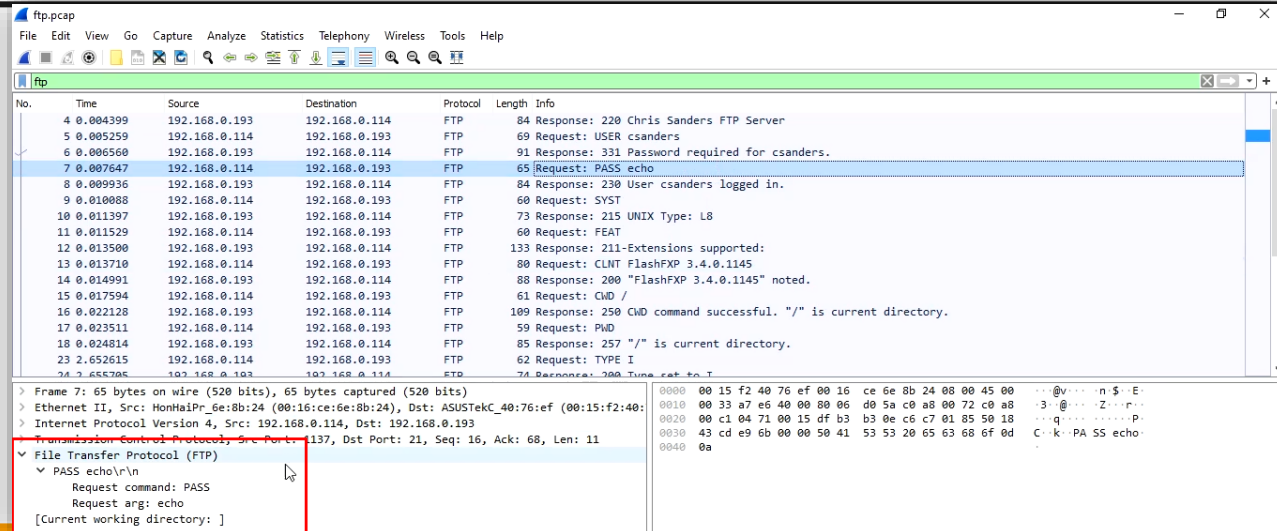


Analysing FTP Traffic

Analyse FTP

- ❖ To analyse FTP traffic, use the following filter and then look for the credentials

ftp





DEMO



THANKS