

# 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**

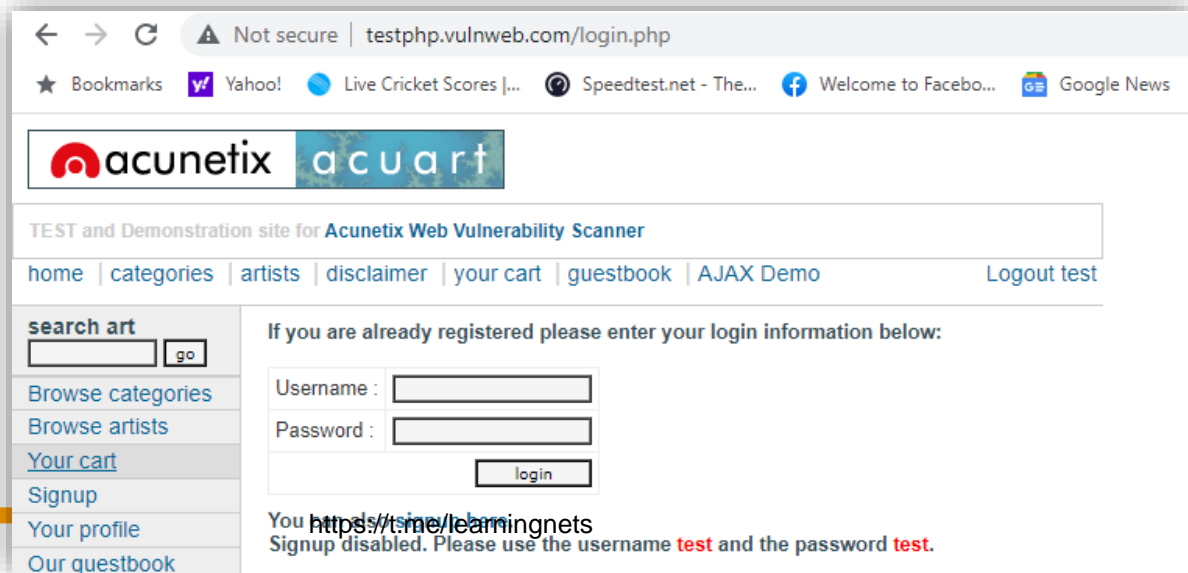


# Analysing HTTP Traffic

# 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/>



← → ↻ Not secure | testphp.vulnweb.com/login.php

★ Bookmarks | Yahoo! | Live Cricket Scores | Speedtest.net - The... | Welcome to Facebo... | Google News

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#) | [Logout test](#)

**search art**

[Browse categories](#)  
[Browse artists](#)  
[Your cart](#)  
[Signup](#)  
[Your profile](#)  
[Our guestbook](#)

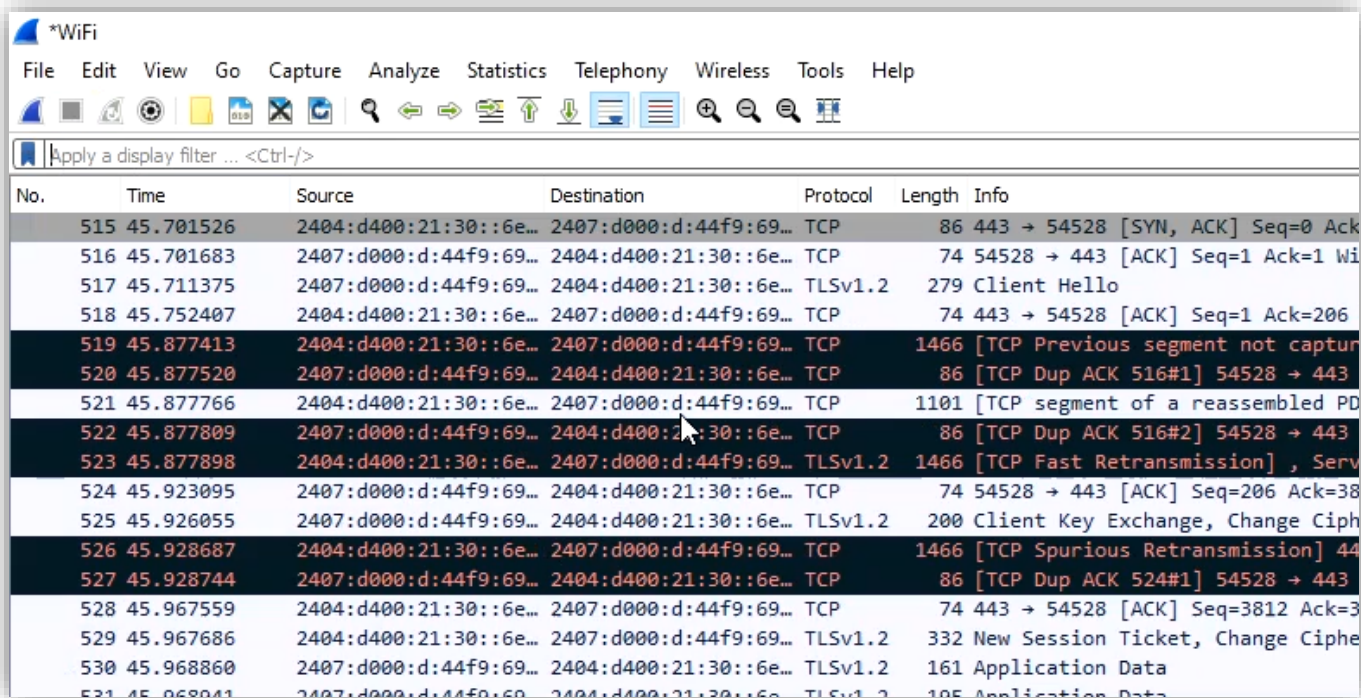
If you are already registered please enter your login information below:

Username :   
Password :

You are already registered. [https://timelearningnets](#)  
Signup disabled. Please use the username **test** and the password **test**.

# Analyse HTTP

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



\*WiFi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

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 screenshot shows the Wireshark interface with the filter `http.request.method==POST` applied. The packet list pane shows two filtered packets:

No.	Time	Source	Destination	Protocol	Length	Info
148	25.633366	192.168.18.11	44.228.249.3	HTTP	715	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
380	36.719779	192.168.18.11	44.228.249.3	HTTP	711	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

The packet details pane for packet 380 shows the following structure:

- > Frame 380: 711 bytes on wire (5688 bits), 711 bytes captured (5688 bits) on interface \Device
- > Ethernet II, Src: HonHaiPr\_46:7d:c5 (70:18:8b:46:7d:c5), Dst: HuaweiTe\_Se:8d:19 (c0:f6:c2:5e:
- > 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 raw data pane shows the hex and ASCII representation of the captured data, including the URL `https://t.me/learningnets` in the form data.



# Analysing FTP Traffic

# Analyse FTP

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

ftp

The screenshot displays the Wireshark interface with the following details:

- Packet List:** A table of captured packets. Packet 7 is selected, showing a request for the password 'echo'.
- Packet Details:** The File Transfer Protocol (FTP) section is expanded, showing:
  - Request command: PASS
  - Request arg: echo
  - Current working directory: [ ]
- Packet Bytes:** The raw data of the packet is shown in hexadecimal and ASCII.

DEMO



THANKS