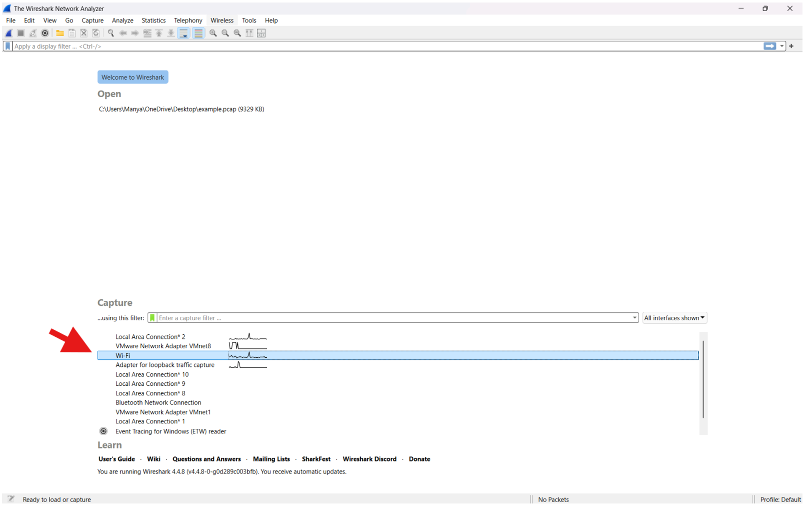
Ex.No.3 Wireshark – Network Packet Capture and Analysis Tool

Aim

To capture plaintext **login credentials** transmitted over HTTP using **Wireshark**, and analyze how insecure protocols expose sensitive information.

Step 1: Start Capturing Packets

- Open **Wireshark** in your Windows/Linux machine.
- Select the active network interface (e.g., **Wi-Fi**).
- Click the **blue shark fin** 🦈 icon to begin capturing packets.

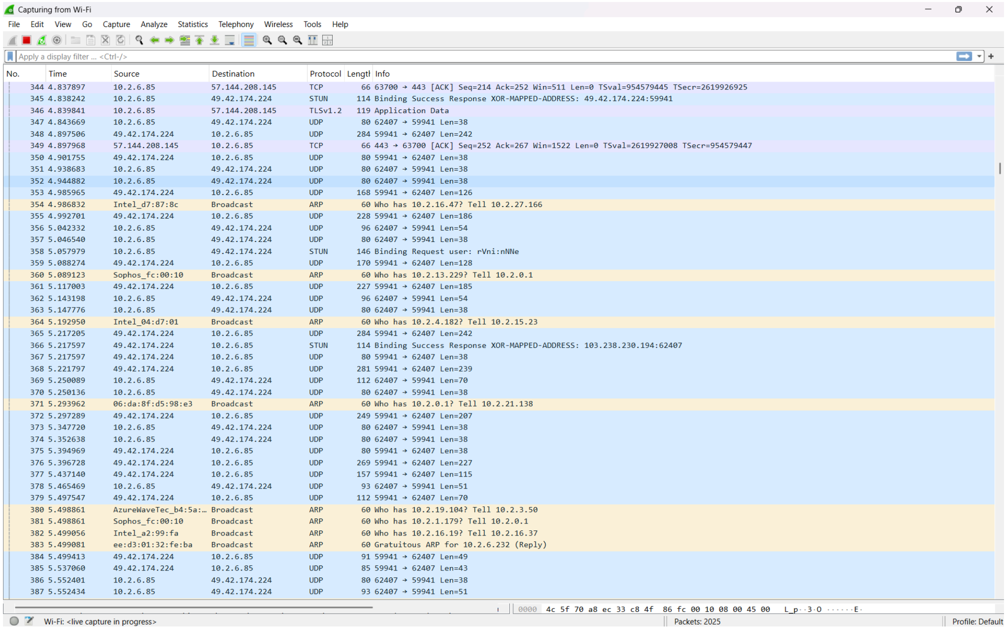

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

C:\Users\Manya\OneDrive\Desktop\example.pcap (9329 KB)

Local Area Connection* 2
VMware Network Adapter VMnet8
Wi-Fi
Adapter for loopback traffic capture
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
VMware Network Adapter VMnet1
Local Area Connection* 1
Event Tracing for Windows (ETW) reader

You are running Wireshark 4.4.8 (v4.4.8-0-g0d289c003bfb). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default



```
No.   Time      Source               Destination      Protocol Lengtl Info
  344 4.837897  10.2.6.85            57.144.208.145   TCP        66 63700 → 443 [ACK] Seq=214 Ack=252 Win=511 Len=0 TSval=954579445 TSecr=2619926925
  345 4.838242  10.2.6.85            49.42.174.224    STUN      114 Binding Success Response XOR-MAPPED-ADDRESS: 49.42.174.224:59941
  346 4.839841  10.2.6.85            57.144.208.145   TLSv1.2   119 Application Data
  347 4.843669  10.2.6.85            49.42.174.224    UDP        80 62407 → 59941 Len=38
  348 4.897506  49.42.174.224        10.2.6.85        UDP       284 59941 → 62407 Len=242
  349 4.897968  57.144.208.145       10.2.6.85        TCP        66 443 → 63700 [ACK] Seq=252 Ack=267 Win=1522 Len=0 TSval=2619927008 TSecr=954579447
  350 4.901755  49.42.174.224        10.2.6.85        UDP        80 59941 → 62407 Len=38
  351 4.938683  10.2.6.85            49.42.174.224    UDP        80 62407 → 59941 Len=38
  352 4.944882  10.2.6.85            49.42.174.224    UDP        80 62407 → 59941 Len=38
  353 4.985965  49.42.174.224        10.2.6.85        UDP       168 59941 → 62407 Len=126
  354 4.986832  Intel_d7:87:8c       Broadcast        ARP        60 Who has 10.2.16.47? Tell 10.2.27.166
  355 4.992701  49.42.174.224        10.2.6.85        UDP       228 59941 → 62407 Len=186
  356 5.042332  10.2.6.85            49.42.174.224    UDP        96 62407 → 59941 Len=54
  357 5.046540  10.2.6.85            49.42.174.224    UDP        80 62407 → 59941 Len=38
  358 5.057979  10.2.6.85            49.42.174.224    STUN      146 Binding Request user: rVni:nNNe
  359 5.088274  49.42.174.224        10.2.6.85        UDP       170 59941 → 62407 Len=128
  360 5.089123  Sophos_fc:00:10      Broadcast        ARP        60 Who has 10.2.13.229? Tell 10.2.0.1
  361 5.117003  49.42.174.224        10.2.6.85        UDP       227 59941 → 62407 Len=185
  362 5.143198  10.2.6.85            49.42.174.224    UDP        96 62407 → 59941 Len=54
  363 5.147776  10.2.6.85            49.42.174.224    UDP        80 62407 → 59941 Len=38
  364 5.192950  Intel_04:d7:01       Broadcast        ARP        60 Who has 10.2.4.182? Tell 10.2.15.23
  365 5.217205  49.42.174.224        10.2.6.85        UDP       284 59941 → 62407 Len=242
  366 5.217597  49.42.174.224        10.2.6.85        STUN      114 Binding Success Response XOR-MAPPED-ADDRESS: 103.238.230.194:62407
  367 5.217597  49.42.174.224        10.2.6.85        UDP        80 59941 → 62407 Len=38
  368 5.221797  49.42.174.224        10.2.6.85        UDP       281 59941 → 62407 Len=239
  369 5.250089  10.2.6.85            49.42.174.224    UDP       112 62407 → 59941 Len=70
  370 5.250136  10.2.6.85            49.42.174.224    UDP        80 62407 → 59941 Len=38
  371 5.293962  06:da:8f:d5:98:e3    Broadcast        ARP        60 Who has 10.2.0.1? Tell 10.2.21.138
  372 5.297289  49.42.174.224        10.2.6.85        UDP       249 59941 → 62407 Len=207
  373 5.347720  10.2.6.85            49.42.174.224    UDP        80 62407 → 59941 Len=38
  374 5.352638  10.2.6.85            49.42.174.224    UDP        80 62407 → 59941 Len=38
  375 5.394969  49.42.174.224        10.2.6.85        UDP        80 59941 → 62407 Len=38
  376 5.396728  49.42.174.224        10.2.6.85        UDP       269 59941 → 62407 Len=227
  377 5.437140  49.42.174.224        10.2.6.85        UDP       157 59941 → 62407 Len=115
  378 5.465469  10.2.6.85            49.42.174.224    UDP        93 62407 → 59941 Len=51
  379 5.497547  49.42.174.224        10.2.6.85        UDP       112 59941 → 62407 Len=70
  380 5.498861  AzureWaveTec_b4:5a:… Broadcast        ARP        60 Who has 10.2.19.104? Tell 10.2.3.50
  381 5.498861  Sophos_fc:00:10      Broadcast        ARP        60 Who has 10.2.1.179? Tell 10.2.0.1
  382 5.499056  Intel_a2:99:fa       Broadcast        ARP        60 Who has 10.2.16.19? Tell 10.2.16.37
  383 5.499081  ee:d3:01:32:fe:ba    Broadcast        ARP        60 Gratuitous ARP for 10.2.6.232 (Reply)
  384 5.499413  49.42.174.224        10.2.6.85        UDP        91 59941 → 62407 Len=49
  385 5.537060  49.42.174.224        10.2.6.85        UDP        85 59941 → 62407 Len=43
  386 5.552401  10.2.6.85            49.42.174.224    UDP        80 62407 → 59941 Len=38
  387 5.552434  10.2.6.85            49.42.174.224    UDP        93 62407 → 59941 Len=51

0000  4c 5f 70 a8 ec 33 c8 4f  86 fc 00 10 08 00 45 00   L_p··3·O ······E·

Wi-Fi: <live capture in progress>          Packets: 2025          Profile: Default
```

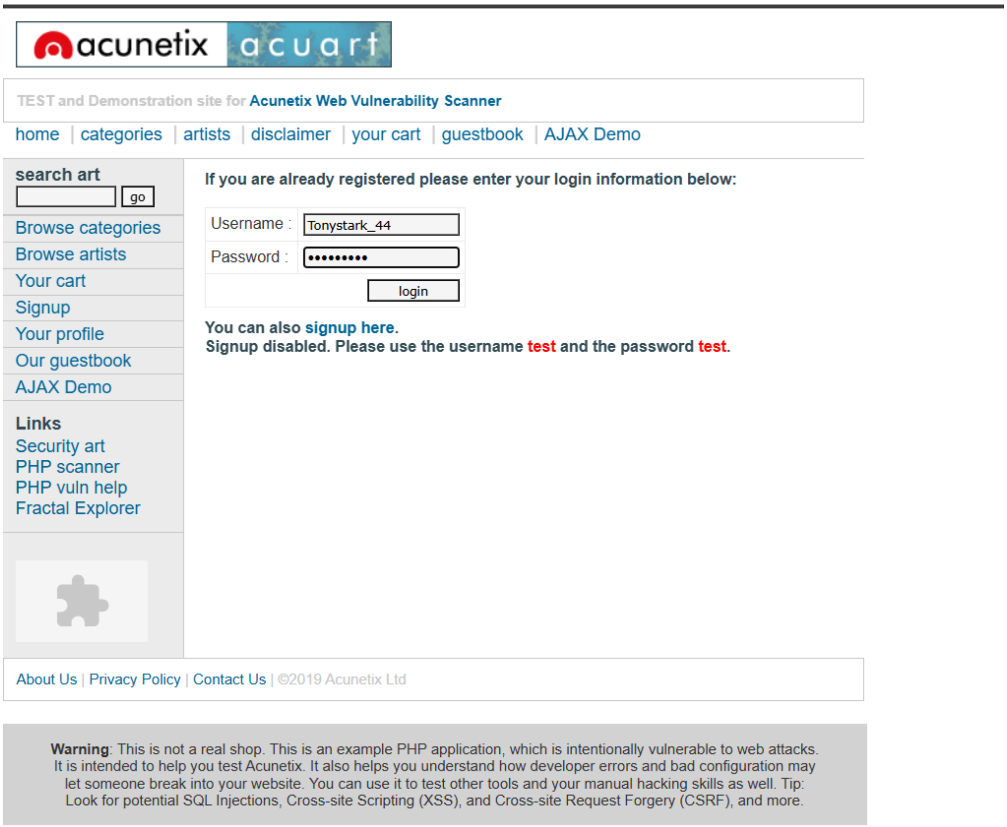
Step 2: Generate Login Traffic

- Open a browser and navigate to a test login page (e.g., `http://testphp.vulnweb.com/login.php`).
- Enter dummy credentials. For this example:

  Username: Tonystark_44

  Password: tony@1234

- Submit the form.
- Even if the login fails, the credentials are **transmitted** in the request.



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

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

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

Username : Tonystark_44
Password : •••••••••
login

You can also signup here.
Signup disabled. Please use the username test and the password test.

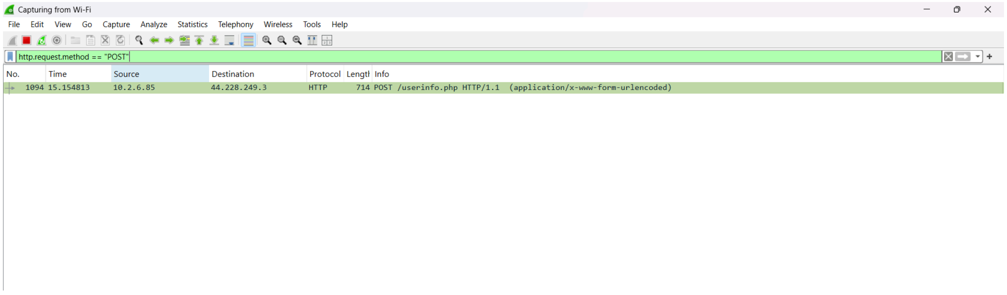
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Step 3: Stop Capture & Filter HTTP Traffic

- Stop the capture (click the **red square** button).
- In the display filter bar, type the following filter and press Enter:

```
http.request.method == "POST"
```



Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

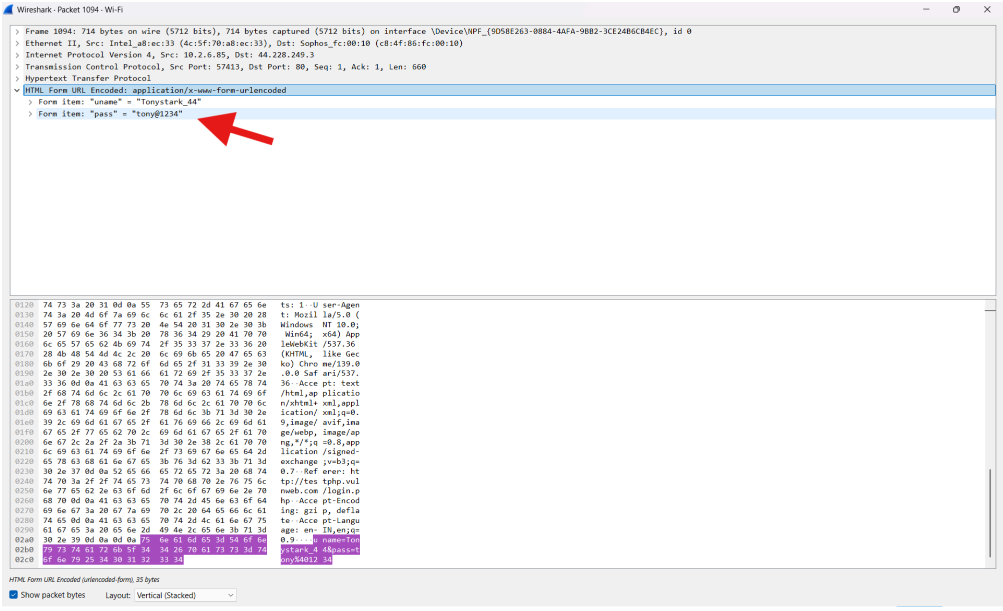
http.request.method == "POST"

No.	Time	Source	Destination	Protocol	Lengtl	Info
1094	15.154813	10.2.6.85	44.228.249.3	HTTP	714	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)

Step 4: Inspect the POST Packet

- From the filtered list, select the POST packet.
- Expand the following sections in the Packet Details Pane:
  - ->Hypertext Transfer Protocol
  - ->HTML Form URL Encoded

You will see the submitted credentials in plaintext: Form item: "uname" = "Tonystark_44" Form item: "pass" = "tony@1234"



Wireshark · Packet 1094 · Wi-Fi

```
> Frame 1094: 714 bytes on wire (5712 bits), 714 bytes captured (5712 bits) on interface \Device\NPF_{9D58E263-0884-4AFA-9BB2-3CE24B6CB4EC}, id 0
> Ethernet II, Src: Intel_a8:ec:33 (4c:5f:70:a8:ec:33), Dst: Sophos_fc:00:10 (c8:4f:86:fc:00:10)
> Internet Protocol Version 4, Src: 10.2.6.85, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 57413, Dst Port: 80, Seq: 1, Ack: 1, Len: 660
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "uname" = "Tonystark_44"
  > Form item: "pass" = "tony@1234"
```

```
0120  74 73 3a 20 31 0d 0a 55  73 65 72 2d 41 67 65 6e   ts: 1··U ser-Agen
0130  74 3a 20 4d 6f 7a 69 6c  6c 61 2f 35 2e 30 20 28   t: Mozil la/5.0 (
0140  57 69 6e 64 6f 77 73 20  4e 54 20 31 30 2e 30 3b   Windows  NT 10.0;
0150  20 57 69 6e 36 34 3b 20  78 36 34 29 20 41 70 70    Win64;  x64) App
0160  6c 65 57 65 62 4b 69 74  2f 35 33 37 2e 33 36 20   leWebKit /537.36 
0170  28 4b 48 54 4d 4c 2c 20  6c 69 6b 65 20 47 65 63   (KHTML,  like Gec
0180  6b 6f 29 20 43 68 72 6f  6d 65 2f 31 33 39 2e 30   ko) Chro me/139.0
0190  2e 30 2e 30 20 53 61 66  61 72 69 2f 35 33 37 2e   .0.0 Saf ari/537.
01a0  33 36 0d 0a 41 63 63 65  70 74 3a 20 74 65 78 74   36··Acce pt: text
01b0  2f 68 74 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   /html,ap plicatio
01c0  6e 2f 78 68 74 6d 6c 2b  78 6d 6c 2c 61 70 70 6c   n/xhtml+ xml,appl
01d0  69 63 61 74 69 6f 6e 2f  78 6d 6c 3b 71 3d 30 2e   ication/ xml;q=0.
01e0  39 2c 69 6d 61 67 65 2f  61 76 69 66 2c 69 6d 61   9,image/ avif,ima
01f0  67 65 2f 77 65 62 70 2c  69 6d 61 67 65 2f 61 70   ge/webp, image/ap
0200  6e 67 2c 2a 2f 2a 3b 71  3d 30 2e 38 2c 61 70 70   ng,*/*;q =0.8,app
0210  6c 69 63 61 74 69 6f 6e  2f 73 69 67 6e 65 64 2d   lication /signed-
0220  65 78 63 68 61 6e 67 65  3b 76 3d 62 33 3b 71 3d   exchange ;v=b3;q=
0230  30 2e 37 0d 0a 52 65 66  65 72 65 72 3a 20 68 74   0.7··Ref erer: ht
0240  74 70 3a 2f 2f 74 65 73  74 70 68 70 2e 76 75 6c   tp://tes tphp.vul
0250  6e 77 65 62 2e 63 6f 6d  2f 6c 6f 67 69 6e 2e 70   nweb.com /login.p
0260  68 70 0d 0a 41 63 63 65  70 74 2d 45 6e 63 6f 64   hp··Acce pt-Encod
0270  69 6e 67 3a 20 67 7a 69  70 2c 20 64 65 66 6c 61   ing: gzi p, defla
0280  74 65 0d 0a 41 63 63 65  70 74 2d 4c 61 6e 67 75   te··Acce pt-Langu
0290  61 67 65 3a 20 65 6e 2d  49 4e 2c 65 6e 3b 71 3d   age: en- IN,en;q=
02a0  30 2e 39 0d 0a 0d 0a 75  6e 61 6d 65 3d 54 6f 6e   0.9····u name=Ton
02b0  79 73 74 61 72 6b 5f 34  34 26 70 61 73 73 3d 74   ystark_4 4&pass=t
02c0  6f 6e 79 25 34 30 31 32  33 34                     ony%4012 34
```

HTML Form URL Encoded (urlencoded-form), 35 bytes

☑ Show packet bytes Layout: Vertical (Stacked)

Rubrics

Criteria	Mark Allotted	Mark Awarded
1. GitHub Activity & Submission Regularity	3	
2. Application of Forensic Tools & Practical Execution	3	
3. Documentation & Reporting	2	
4. Engagement, Problem-Solving & Team Collaboration	2	
Total	10	

Result

The experiment successfully captured **login credentials** transmitted via **HTTP**.
This demonstrates that **HTTP is insecure**, as sensitive information is sent in **plaintext**, making it easy for attackers to intercept.