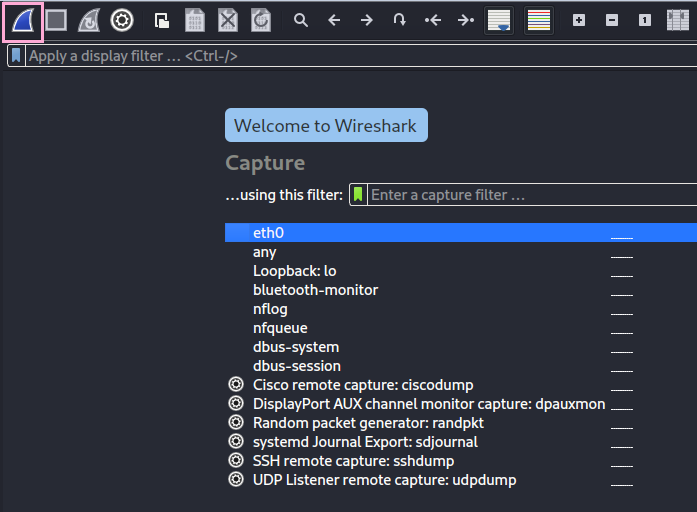
**💕Wireshark Packet Sniffing User and Password from HTTP Website.💕**

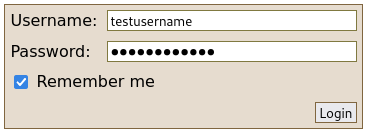
📌I used a HTTP webpage in this example, as it lacks SSL/TLS cryptography. This means the user and password can be captured in plain text and it's vulnerable to password and username sniffing attacks, like it's shown in this example.

📌The URL used is http://testaspnet.vulnweb.com/login.aspx , a vulnerable website created for security tests practice.

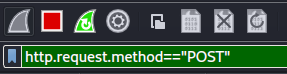
**Step 1:** Open Wireshark and start capturing packages on your ethernet or internet network interface:



**Step 2:** Access the chosen HTTP website and type and example username and password on the user login field:

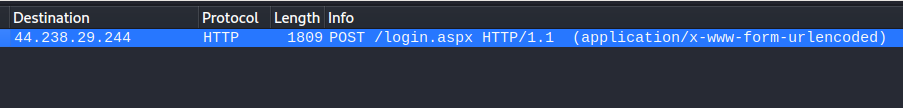


**Step 3:** Open Wireshark again, you’ll see there’s a lot of captured packages. Filter by HTTP request method POST so you can find the package you’re looking for faster:

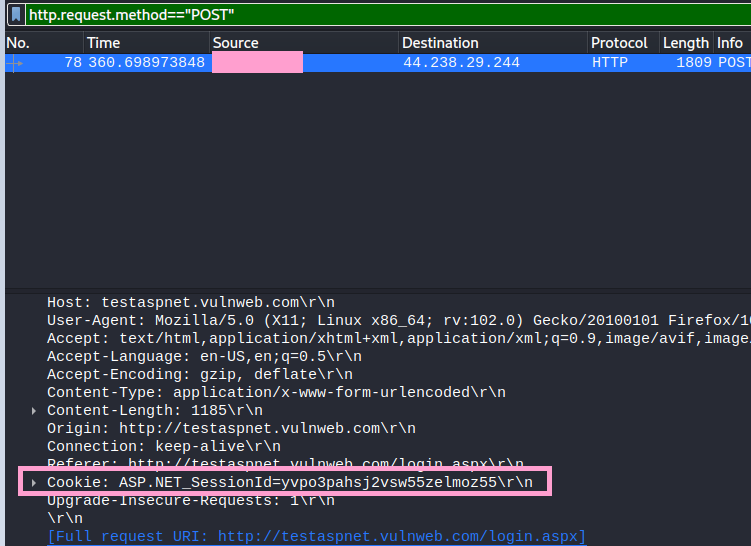


* Important: Browsers and Web Servers communicate with each other through HTTP request and HTTP response. When we logged in on the webpage, our browser sent a http request to the website’s web server to login on the page. One of the methods used in this communication is POST, which is a HTTP method used to send data to the web server.

After filtering, you’ll be able to see the package on Wireshark:

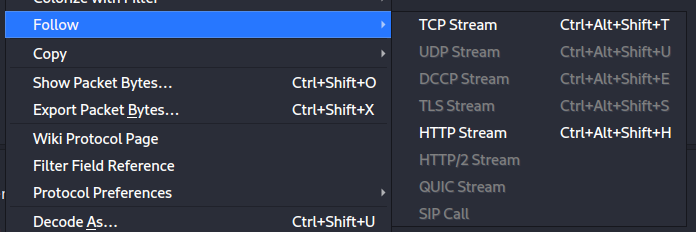


**Step 4:** Select the package and look for the Session Cookie:



* Important: Cookies are small pieces of data that store information, like username and password, to communicate with the web server.

**Step 5:** Right click the Cookie, select Follow and HTTP Stream



**Step 6:** If you analyze the HTTP Stream, you’ll be able to find the username and password used in plain text:

