Password Sniffing Using Wireshark

@mmar

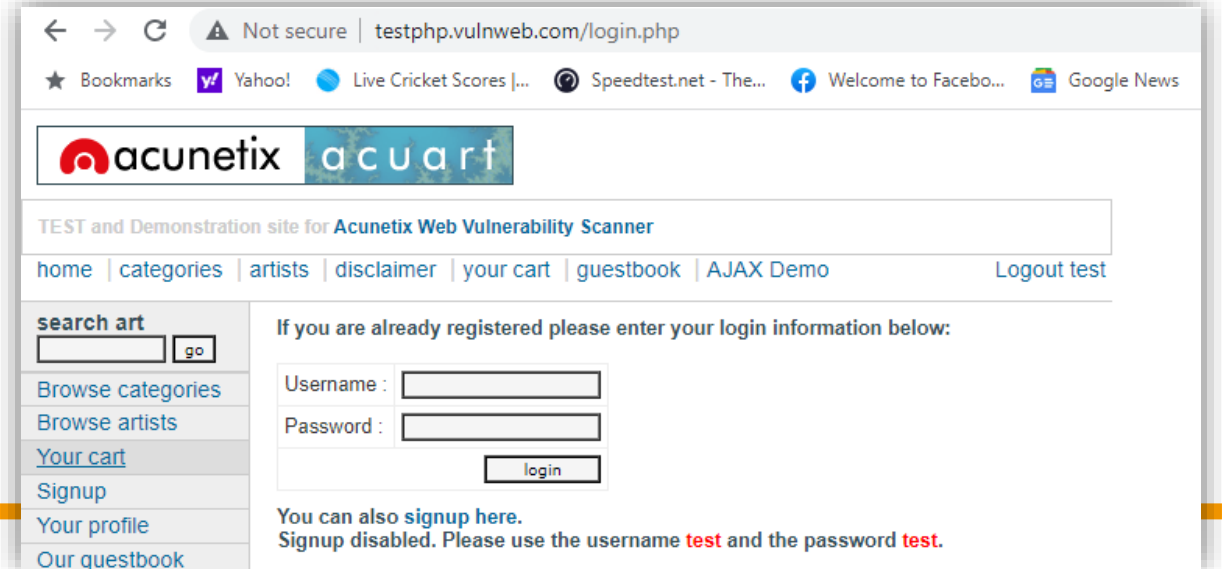
Http and **FTP** are both unencrypted protocols and if we are able to capture their traffic, we can extract the credentials from them

Analysing HTTP Traffic

Analyse HTTP

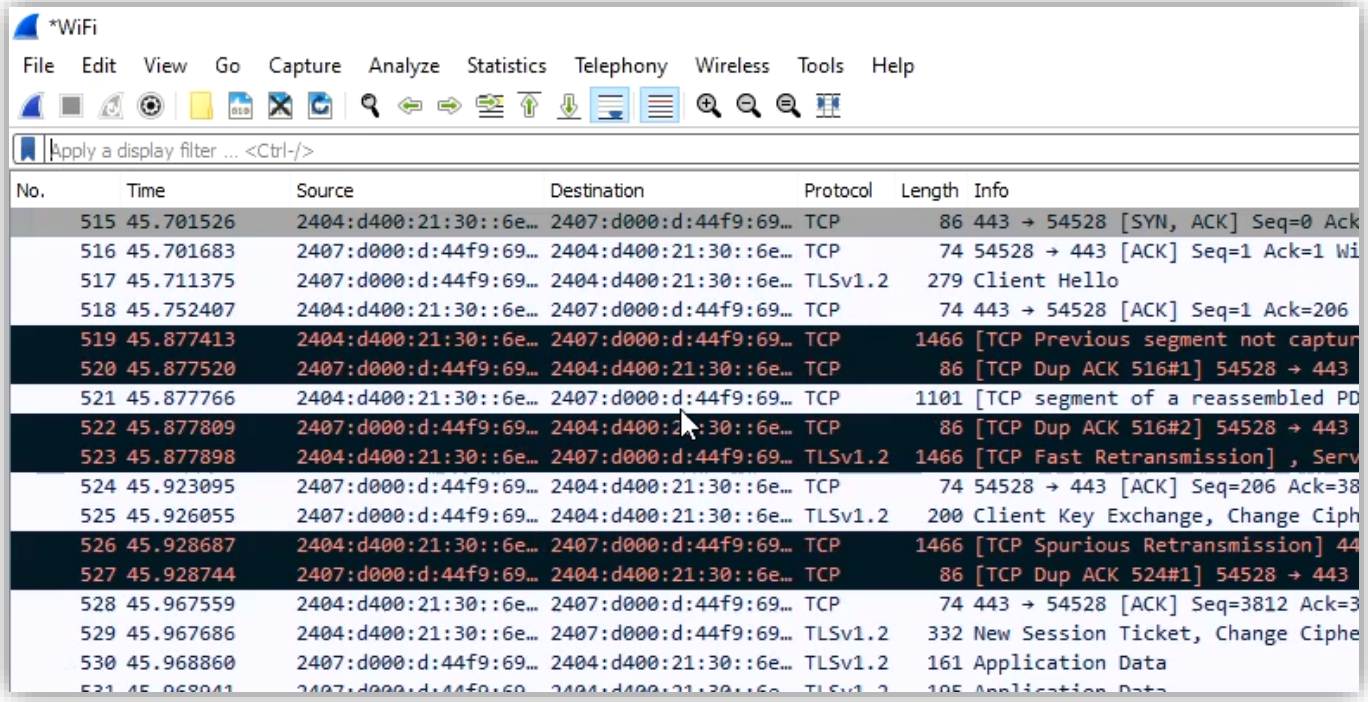
- Visit the following website. The site operates on Http only and thus allows us to capture traffic in plain text

http://testphp.vulnweb.com/



Analyse HTTP

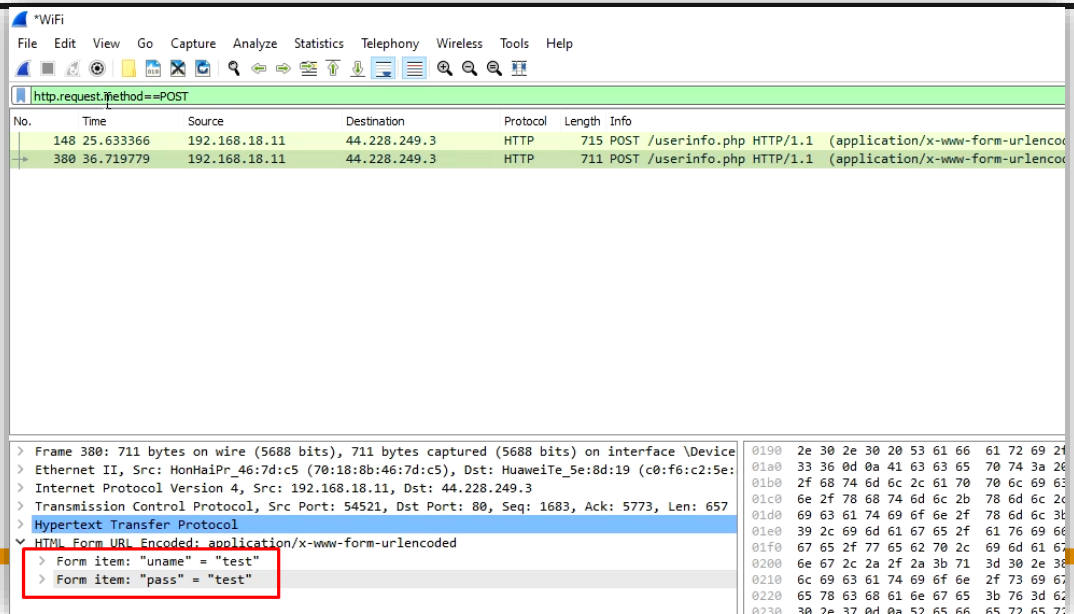
- Now Open Wireshark and capture the traffic. Now login on the site. The traffic will be captured in Wireshark



Analyse HTTP

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

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

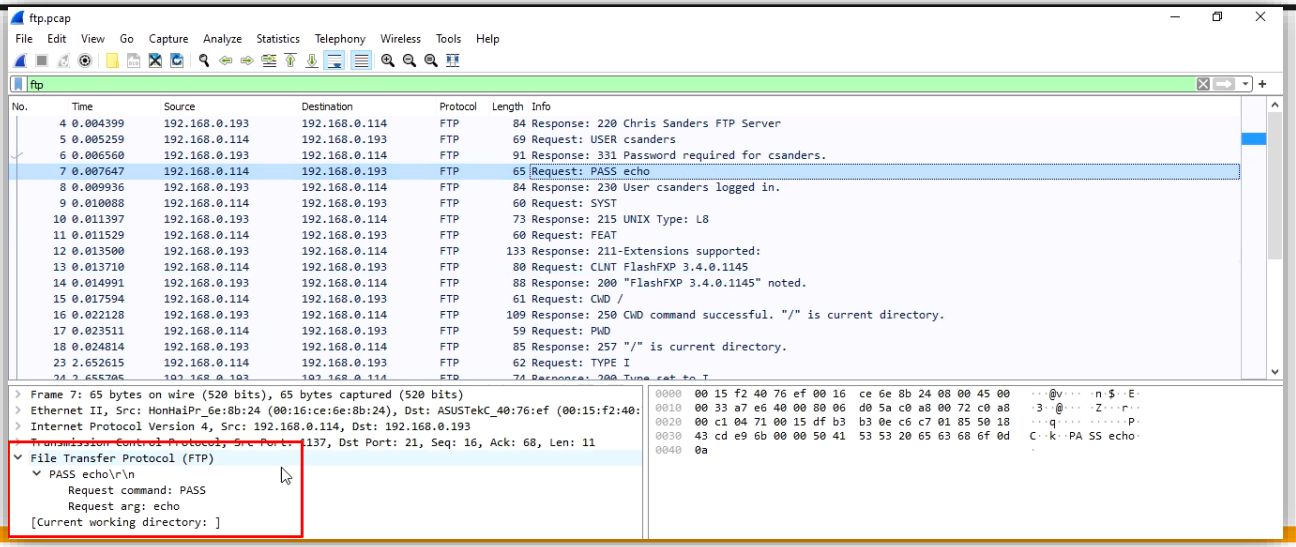


Analysing FTP Traffic

Analyse FTP

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

```
ftp
```



DEMO

THANKS