CA3

INT 301

OPEN SOURCE TECHNOLOGIES

NAME: SUDHARSAN G **REG. NO.: 11903724**

ROLL NO.: 44 **SECTION: KE022**

INTRODUCTION:

1.1 OBJECTIVE OF THE PROJECT

The main objective is to examine HTTP traffic and try to retrieve usernames and passwords in order to evaluate the security of a website's authentication methods. Penetration testing, vulnerability analysis, and security audits are just a few reasons why this might be done. The project's objective should be consistent with moral principles, and any action should be allowed by law and carried out with the website owner's permission. Illegal access to a network or website is prohibited and may have legal repercussions.

The owner of the website should be informed of any vulnerabilities or flaws found, and they should be handled responsibly and expertly. We can contribute to enhancing the website's security posture and preventing potential security breaches by carrying out this project in an ethical and responsible manner.

Once the ports have been determined, examine the HTTP traffic to extract usernames and passwords. Tools that collect and analyse network traffic, like Wireshark, can be used for this. We can locate any sensitive information, such as usernames and passwords, being communicated over the network by looking at HTTP traffic. The security posture of the website may then be evaluated using this information, and any holes in the authentication process can be found.

1.2 SCOPE OF THE PROJECT

The project's scope would entail getting the website owner's right permission and consent, as well as making sure that all legal and moral requirements are met. The task would entail locating the IP address and open ports of the target website, examining HTTP activity, and making an effort to retrieve users name and passwords.

The project's scope would include locating any holes or flaws in the website's authentication procedures and informing the website owner of them. The scope would also include recommending appropriate fixes for any found flaws or vulnerabilities and collaborating with the website's owner to put such fixes into practise.

In conclusion, the scope of this project would entail evaluating HTTP traffic to determine a website's security posture and attempting to obtain usernames and passwords with the appropriate authorization and consent. The scope would involve locating any holes or weak points in the website's authentication procedures, recommending workable fixes, and collaborating with the website owner to make those fixes in a respectable and morally sound way.

SYSTEM DESCRIPTION

2.1 TARGETED SYSTEM DESCRIPTION

The objective system would include examining HTTP traffic and attempting to acquire users and passwords in order to evaluate the security posture of a website's authentication systems. A website that needs authentication to access sensitive information would be the intended system. The website might have a login page where users can input their login information to access the data or services the website provides.

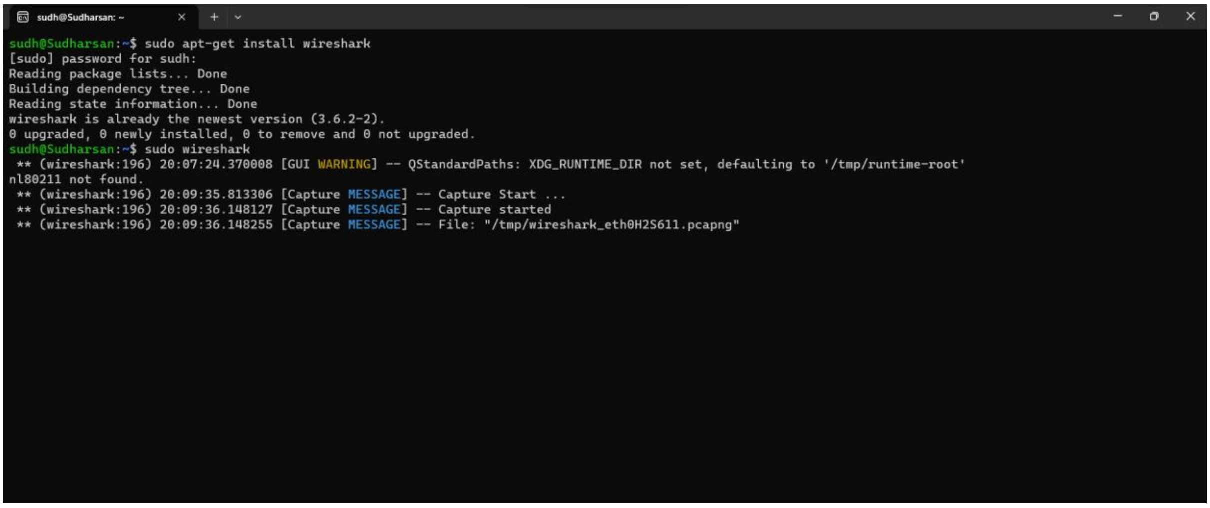
The project's target system would analyse HTTP traffic and try to extract users and passwords in order to evaluate the authentication mechanisms on a website's security posture. The project plan would precisely explain the system architecture and authentication processes of the target system, which would be a website that needs authentication to access sensitive information.

ANALYSIS REPORT

3.1 SYSTEM SNAPSHOTS AND FULL ANALYSIS REPORT

WIRESHARK:
Wireshark is a free and open-source network protocol analyser that captures and inspects network traffic. It supports a wide range of protocols, filters traffic, provides detailed packet-level analysis, and has a rich graphical user interface. It's useful for troubleshooting network issues, analysing network performance, and monitoring network security. Wireshark allows users to decrypt encrypted network traffic if the user has access to the decryption keys.

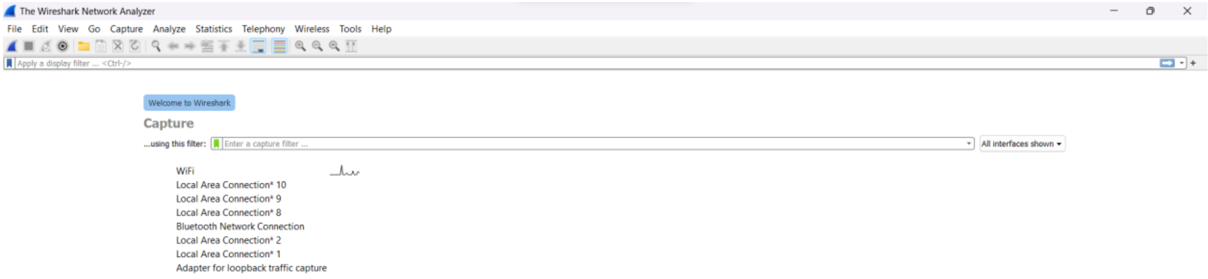
STEP – 1:



```
sudh@Sudharsan:~$ sudo apt-get install wireshark
[sudo] password for sudh:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
wireshark is already the newest version (3.6.2-2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
sudh@Sudharsan:~$ sudo wireshark
 ** (wireshark:196) 20:07:24.370008 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'
nl80211 not found.
 ** (wireshark:196) 20:09:35.813306 [Capture MESSAGE] -- Capture Start ...
 ** (wireshark:196) 20:09:36.148127 [Capture MESSAGE] -- Capture started
 ** (wireshark:196) 20:09:36.148255 [Capture MESSAGE] -- File: "/tmp/wireshark_eth0H2S611.pcapng"
```

Download and install the wireshark, through which we will inspect the website. After installing the wireshark open it. A wireshark application window will open.

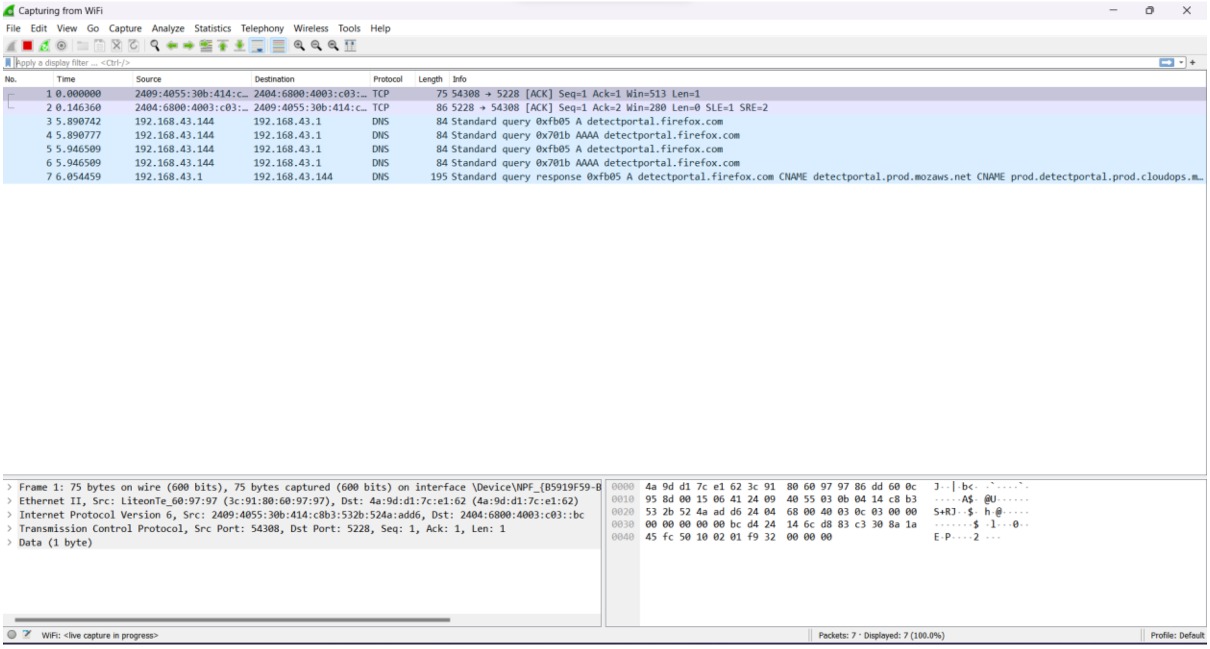
STEP – 2:



The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
WiFi
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Bluetooth Network Connection
Local Area Connection* 2
Local Area Connection* 1
Adapter for loopback traffic capture

Wireshark application will be launched where we will perform the action to inspect the http traffic and retrieve the usernames and passwords the are entered on the website.

STEP – 3:


Capturing from WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source               Destination          Protocol Length Info
   1 0.000000  2409:4055:30b:414:c… 2404:6800:4003:c03:… TCP       75 54308 → 5228 [ACK] Seq=1 Ack=1 Win=513 Len=1
   2 0.146360  2404:6800:4003:c03:… 2409:4055:30b:414:c… TCP       86 5228 → 54308 [ACK] Seq=1 Ack=2 Win=280 Len=0 SLE=1 SRE=2
   3 5.890742  192.168.43.144       192.168.43.1         DNS       84 Standard query 0xfb05 A detectportal.firefox.com
   4 5.890777  192.168.43.144       192.168.43.1         DNS       84 Standard query 0x701b AAAA detectportal.firefox.com
   5 5.946509  192.168.43.144       192.168.43.1         DNS       84 Standard query 0xfb05 A detectportal.firefox.com
   6 5.946509  192.168.43.144       192.168.43.1         DNS       84 Standard query 0x701b AAAA detectportal.firefox.com
   7 6.054459  192.168.43.1         192.168.43.144       DNS      195 Standard query response 0xfb05 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME prod.detectportal.prod.cloudops.m…
```

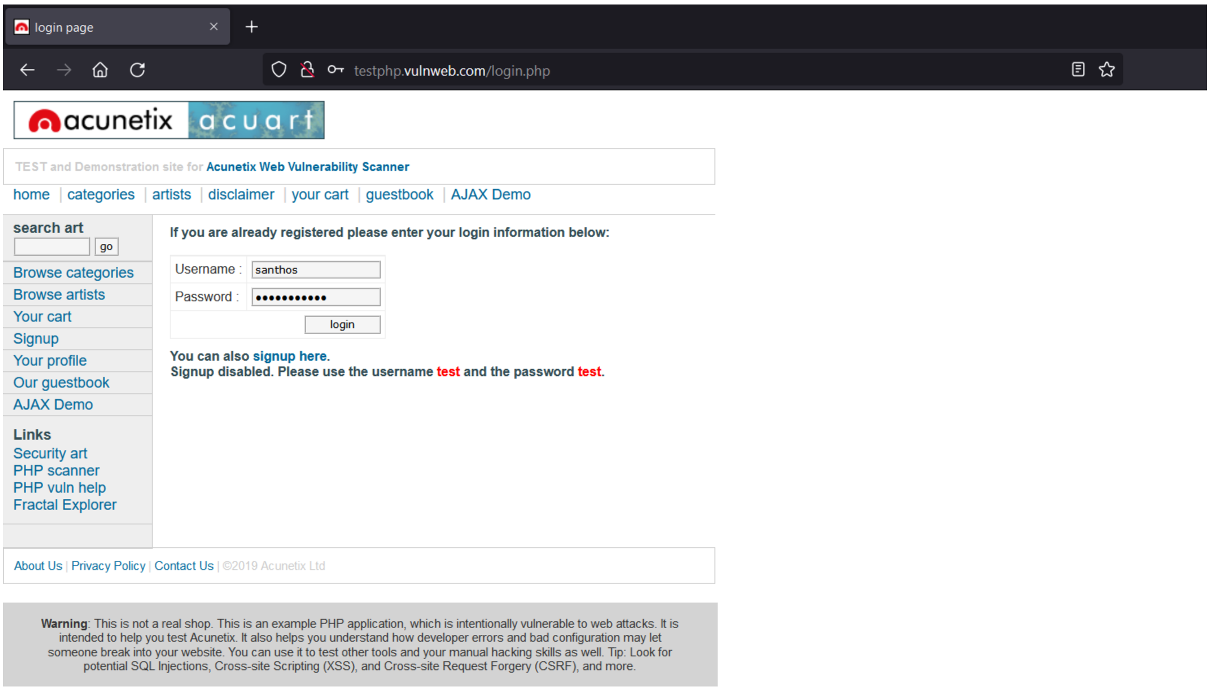
```
> Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{B5919F59-B
> Ethernet II, Src: LiteonTe_60:97:97 (3c:91:80:60:97:97), Dst: 4a:9d:d1:7c:e1:62 (4a:9d:d1:7c:e1:62)
> Internet Protocol Version 6, Src: 2409:4055:30b:414:c8b3:532b:524a:add6, Dst: 2404:6800:4003:c03::bc
> Transmission Control Protocol, Src Port: 54308, Dst Port: 5228, Seq: 1, Ack: 1, Len: 1
> Data (1 byte)
```

```
0000  4a 9d d1 7c e1 62 3c 91  80 60 97 97 86 dd 60 0c   J··|·b<· ·`····`·
0010  95 8d 00 15 06 41 24 09  40 55 03 0b 04 14 c8 b3   ·····A$· @U······
0020  53 2b 52 4a ad d6 24 04  68 00 40 03 0c 03 00 00   S+RJ··$· h·@·····
0030  00 00 00 00 00 bc d4 24  14 6c d8 83 c3 30 8a 1a   ·······$ ·l···0··
0040  45 fc 50 10 02 01 f9 32  00 00 00                  E·P····2 ···
```

WiFi: <live capture in progress>
Packets: 7 · Displayed: 7 (100.0%)
Profile: Default

To start capturing the website data, firstly we have to choose the network. Here, I have chosen the wifi network. After the choosing the network, wireshark will start capturing the http traffic the websites.

STEP – 4:


login page
testphp.vulnweb.com/login.php
acunetix acuart
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
login
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

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

Username : santhos

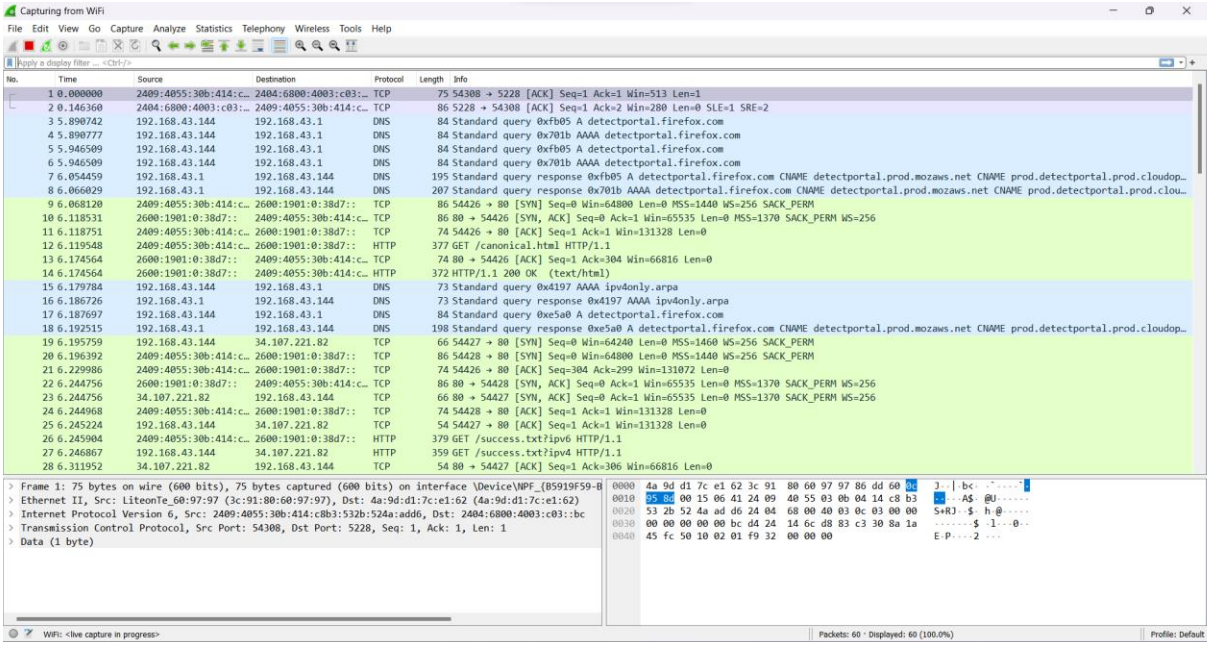
Password : •••••••••••

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

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.

Then go to the browser, enter the website which you have to inspect and retrieve the username and password. Here I have taken the http://testphp.vulnweb.com/ website. After that enter the username and password.

STEP – 5:


Capturing from WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source                  Destination             Protocol Length Info
   1 0.000000  2409:4055:30b:414:c…    2404:6800:4003:c03:…    TCP       75 54308 → 5228 [ACK] Seq=1 Ack=1 Win=513 Len=1
   2 0.146360  2404:6800:4003:c03:…    2409:4055:30b:414:c…    TCP       86 5228 → 54308 [ACK] Seq=1 Ack=2 Win=280 Len=0 SLE=1 SRE=2
   3 5.890742  192.168.43.144          192.168.43.1            DNS       84 Standard query 0xfb05 A detectportal.firefox.com
   4 5.890777  192.168.43.144          192.168.43.1            DNS       84 Standard query 0x701b AAAA detectportal.firefox.com
   5 5.946509  192.168.43.144          192.168.43.1            DNS       84 Standard query 0xfb05 A detectportal.firefox.com
   6 5.946509  192.168.43.144          192.168.43.1            DNS       84 Standard query 0x701b AAAA detectportal.firefox.com
   7 6.054459  192.168.43.1            192.168.43.144          DNS      195 Standard query response 0xfb05 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME prod.detectportal.prod.cloudop…
   8 6.066029  192.168.43.1            192.168.43.144          DNS      207 Standard query response 0x701b AAAA detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME prod.detectportal.prod.clou…
   9 6.068120  2409:4055:30b:414:c…    2600:1901:0:38d7::      TCP       86 54426 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
  10 6.118531  2600:1901:0:38d7::      2409:4055:30b:414:c…    TCP       86 80 → 54426 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1370 SACK_PERM WS=256
  11 6.118751  2409:4055:30b:414:c…    2600:1901:0:38d7::      TCP       74 54426 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  12 6.119548  2409:4055:30b:414:c…    2600:1901:0:38d7::      HTTP     377 GET /canonical.html HTTP/1.1
  13 6.174564  2600:1901:0:38d7::      2409:4055:30b:414:c…    TCP       74 80 → 54426 [ACK] Seq=1 Ack=304 Win=66816 Len=0
  14 6.174564  2600:1901:0:38d7::      2409:4055:30b:414:c…    HTTP     372 HTTP/1.1 200 OK  (text/html)
  15 6.179784  192.168.43.144          192.168.43.1            DNS       73 Standard query 0x4197 AAAA ipv4only.arpa
  16 6.186726  192.168.43.1            192.168.43.144          DNS       73 Standard query response 0x4197 AAAA ipv4only.arpa
  17 6.187697  192.168.43.144          192.168.43.1            DNS       84 Standard query 0xe5a0 A detectportal.firefox.com
  18 6.192515  192.168.43.1            192.168.43.144          DNS      198 Standard query response 0xe5a0 A detectportal.firefox.com CNAME detectportal.prod.mozaws.net CNAME prod.detectportal.prod.cloudop…
  19 6.195759  192.168.43.144          34.107.221.82           TCP       66 54427 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  20 6.196392  2409:4055:30b:414:c…    2600:1901:0:38d7::      TCP       86 54428 → 80 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
  21 6.229986  2409:4055:30b:414:c…    2600:1901:0:38d7::      TCP       74 54426 → 80 [ACK] Seq=304 Ack=299 Win=131072 Len=0
  22 6.244756  2600:1901:0:38d7::      2409:4055:30b:414:c…    TCP       86 80 → 54428 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1370 SACK_PERM WS=256
  23 6.244756  34.107.221.82           192.168.43.144          TCP       66 80 → 54427 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1370 SACK_PERM WS=256
  24 6.244968  2409:4055:30b:414:c…    2600:1901:0:38d7::      TCP       74 54428 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  25 6.245224  192.168.43.144          34.107.221.82           TCP       54 54427 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
  26 6.245904  2409:4055:30b:414:c…    2600:1901:0:38d7::      HTTP     379 GET /success.txt?ipv6 HTTP/1.1
  27 6.246867  192.168.43.144          34.107.221.82           HTTP     359 GET /success.txt?ipv4 HTTP/1.1
  28 6.311952  34.107.221.82           192.168.43.144          TCP       54 80 → 54427 [ACK] Seq=1 Ack=306 Win=66816 Len=0
```

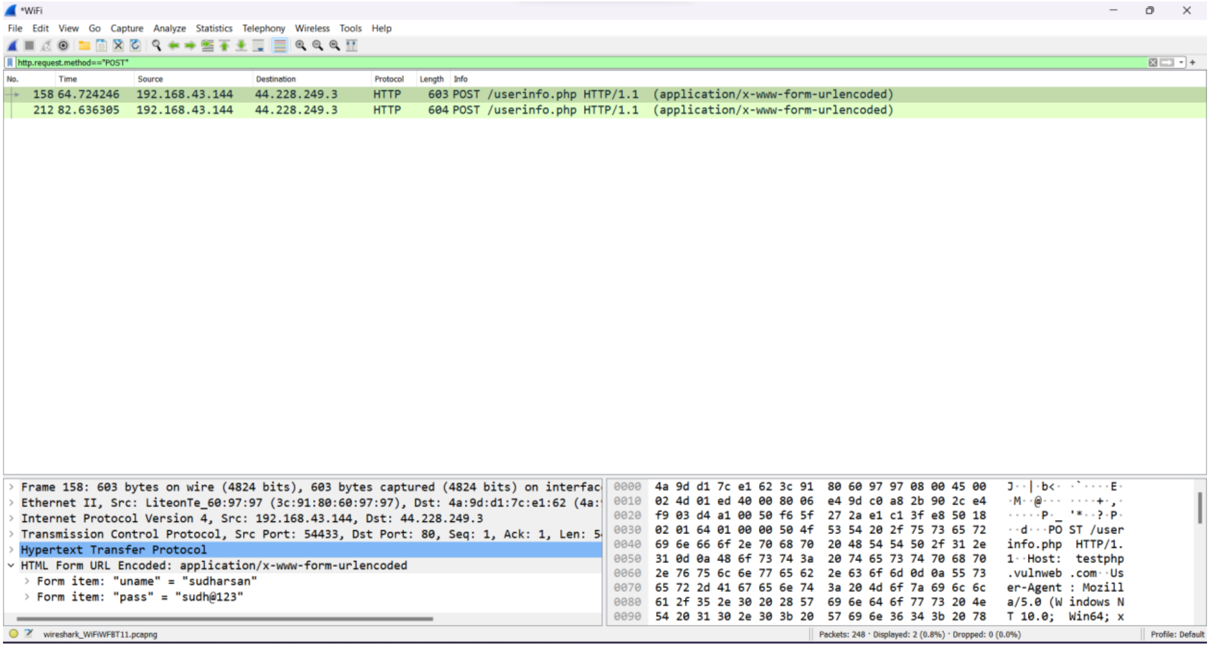
```
> Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{B5919F59-B
> Ethernet II, Src: LiteonTe_60:97:97 (3c:91:80:60:97:97), Dst: 4a:9d:d1:7c:e1:62 (4a:9d:d1:7c:e1:62)
> Internet Protocol Version 6, Src: 2409:4055:30b:414:c8b3:532b:524a:add6, Dst: 2404:6800:4003:c03::bc
> Transmission Control Protocol, Src Port: 54308, Dst Port: 5228, Seq: 1, Ack: 1, Len: 1
> Data (1 byte)
```

```
0000  4a 9d d1 7c e1 62 3c 91  80 60 97 97 86 dd 60 0c   J··|·b<· ·`····`·
0010  95 8d 00 15 06 41 24 09  40 55 03 0b 04 14 c8 b3   ·····A$· @U······
0020  53 2b 52 4a ad d6 24 04  68 00 40 03 0c 03 00 00   S+RJ··$· h·@·····
0030  00 00 00 00 00 bc d4 24  14 6c d8 83 c3 30 8a 1a   ·······$ ·l···0··
0040  45 fc 50 10 02 01 f9 32  00 00 00                  E·P····2 ···
```

WiFi: <live capture in progress>
Packets: 60 · Displayed: 60 (100.0%)
Profile: Default

Return to wireshark, stop capturing the http traffic. There will be many http traffic captured. We have to filter it by two methods.

STEP – 5.1:


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.method=="POST"

```
No.  Time       Source          Destination   Protocol Length Info
 158 64.724246  192.168.43.144  44.228.249.3  HTTP      603 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
 212 82.636305  192.168.43.144  44.228.249.3  HTTP      604 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
```

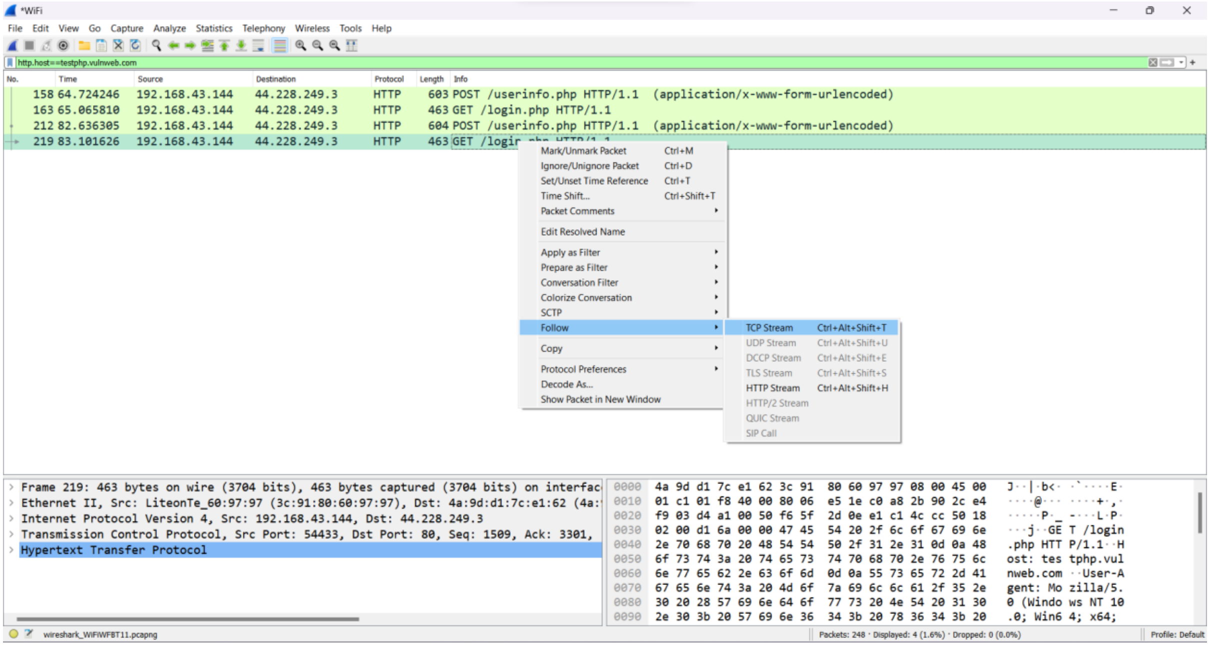
```
> Frame 158: 603 bytes on wire (4824 bits), 603 bytes captured (4824 bits) on interfac
> Ethernet II, Src: LiteonTe_60:97:97 (3c:91:80:60:97:97), Dst: 4a:9d:d1:7c:e1:62 (4a:
> Internet Protocol Version 4, Src: 192.168.43.144, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 54433, Dst Port: 80, Seq: 1, Ack: 1, Len: 5
> Hypertext Transfer Protocol
v HTML Form URL Encoded: application/x-www-form-urlencoded
  > Form item: "uname" = "sudharsan"
  > Form item: "pass" = "sudh@123"
```

```
0000  4a 9d d1 7c e1 62 3c 91  80 60 97 97 08 00 45 00   J··|·b<· ·`····E·
0010  02 4d 01 ed 40 00 80 06  e4 9d c0 a8 2b 90 2c e4   ·M··@··· ····+·,·
0020  f9 03 d4 a1 00 50 f6 5f  27 2a e1 c1 3f e8 50 18   ·····P·_ '*··?·P·
0030  02 01 64 01 00 00 50 4f  53 54 20 2f 75 73 65 72   ··d···PO ST /user
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.php  HTTP/1.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Host:  testphp
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 55 73   .vulnweb .com··Us
0070  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
0080  61 2f 35 2e 30 20 28 57  69 6e 64 6f 77 73 20 4e   a/5.0 (W indows N
0090  54 20 31 30 2e 30 3b 20  57 69 6e 36 34 3b 20 78   T 10.0;  Win64; x
```

wireshark_WiFiWFBT11.pcapng
Packets: 248 · Displayed: 2 (0.8%) · Dropped: 0 (0.0%)
Profile: Default

First is by the request method. At top there will be a box where you have to enter http.request.method==”POST”. Down there will be a option “HTML form URL Encoded”. Frome there we will get the username and password, either as plain text or encrypted text.

STEP – 5.2:



```
http.host==testphp.vulnweb.com

No.  Time          Source          Destination    Protocol Length Info
158 64.724246 192.168.43.144 44.228.249.3 HTTP  603 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
163 65.065810 192.168.43.144 44.228.249.3 HTTP  463 GET /login.php HTTP/1.1
212 82.636305 192.168.43.144 44.228.249.3 HTTP  604 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
219 83.101626 192.168.43.144 44.228.249.3 HTTP  463 GET /logir
```

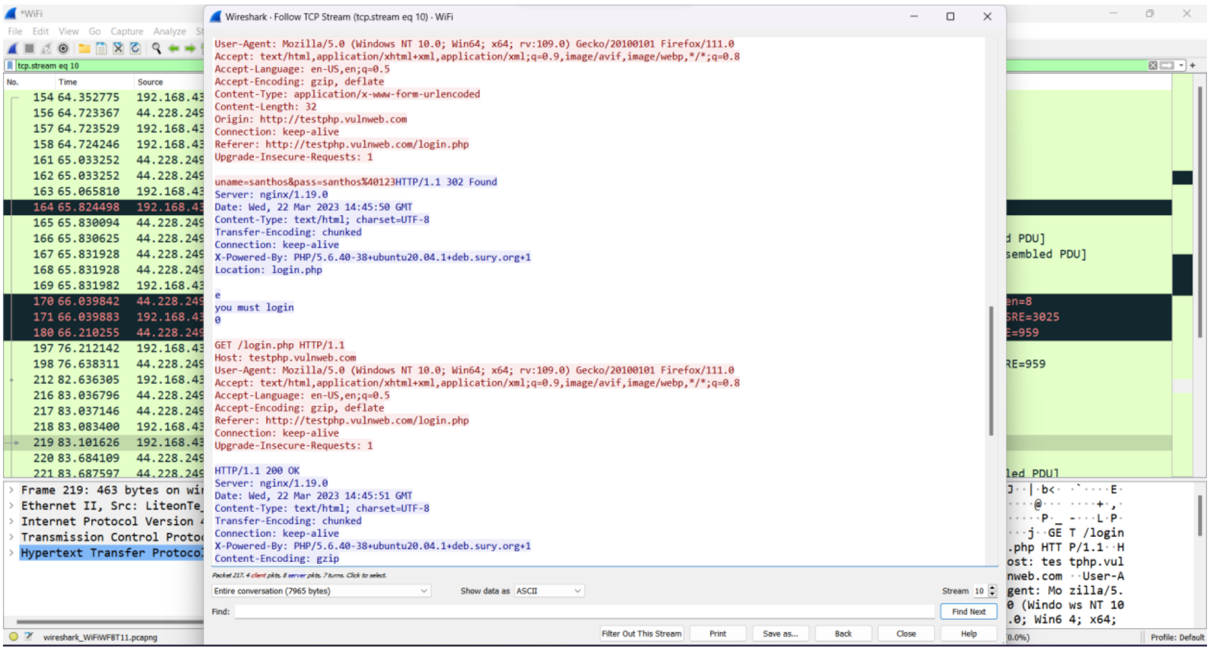
```
> Frame 219: 463 bytes on wire (3704 bits), 463 bytes captured (3704 bits) on interfac
> Ethernet II, Src: LiteonTe_60:97:97 (3c:91:80:60:97:97), Dst: 4a:9d:d1:7c:e1:62 (4a:
> Internet Protocol Version 4, Src: 192.168.43.144, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 54433, Dst Port: 80, Seq: 1509, Ack: 3301,
> Hypertext Transfer Protocol
```

```
0000  4a 9d d1 7c e1 62 3c 91  80 60 97 97 08 00 45 00   J··|·b<· ·`····E·
0010  01 c1 01 f8 40 00 80 06  e5 1e c0 a8 2b 90 2c e4   ····@··· ····+·,·
0020  f9 03 d4 a1 00 50 f6 5f  2d 0e e1 c1 4c cc 50 18   ·····P·_ -···L·P·
0030  02 00 d1 6a 00 00 47 45  54 20 2f 6c 6f 67 69 6e   ···j··GE T /login
0040  2e 70 68 70 20 48 54 54  50 2f 31 2e 31 0d 0a 48   .php HTT P/1.1··H
0050  6f 73 74 3a 20 74 65 73  74 70 68 70 2e 76 75 6c   ost: tes tphp.vul
0060  6e 77 65 62 2e 63 6f 6d  0d 0a 55 73 65 72 2d 41   nweb.com ··User-A
0070  67 65 6e 74 3a 20 4d 6f  7a 69 6c 6c 61 2f 35 2e   gent: Mo zilla/5.
0080  30 20 28 57 69 6e 64 6f  77 73 20 4e 54 20 31 30   0 (Windo ws NT 10
0090  2e 30 3b 20 57 69 6e 36  34 3b 20 78 36 34 3b 20   .0; Win6 4; x64; 
```

wireshark_WiFiWFBT11.pcapng | Packets: 248 · Displayed: 4 (1.6%) · Dropped: 0 (0.0%) | Profile: Default

*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
DCCP Stream Ctrl+Alt+Shift+E
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream
SIP Call

Next method is by using the website hostname. For this, we have to enter http.host==testphp.vulnweb.com . From there select the TCP stream which will open new dialogue box. In that dialogue box you get the usernames and passwords that had been entered.



Wireshark · Follow TCP Stream (tcp.stream eq 10) · WiFi

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 32
Origin: http://testphp.vulnweb.com
Connection: keep-alive
Referer: http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1

uname=santhos&pass=santhos%40123HTTP/1.1 302 Found
Server: nginx/1.19.0
Date: Wed, 22 Mar 2023 14:45:50 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Location: login.php

e
you must login
0

GET /login.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://testphp.vulnweb.com/login.php
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Wed, 22 Mar 2023 14:45:51 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Content-Encoding: gzip
```

Packet 217. 4 client pkts, 8 server pkts, 7 turns. Click to select.

Entire conversation (7965 bytes) | Show data as: ASCII | Stream 10

This is the window where we will get the username and passwords that are entered. We can also save these captured http traffics to use later.

REFERENCE/ BIBLIOGRAPHY

1. http://testphp.vulnweb.com/
2. https://www.youtube.com/
3. https://github.com/

GITHUB

https://github.com/sudharsang0/int301_ca3