LOVELY PROFESSIONAL UNIVERSITY

Transforming Education Transforming India

INT301 – CA3

Student Name: Chinmay Lahoti

Roll no.: 44

Reg No: 11903607

Submitted To: Professor Dr. Manjot Kaur

1. Introduction

As technology has advanced, the need for network security has increased manifold. Cybersecurity threats are prevalent in today's world, and organizations need to take proactive measures to safeguard their networks. As a network analyst working in the Infotech department of LPU, the objective of this project is to inspect HTTP traffic and retrieve the Username and Password from the http://testphp.vulnweb.com/ website. This report will provide the steps involved in scanning the port.

1.1 **Objective of the project**:

- The primary objective of this project is to scan the target website for HTTP traffic and retrieve the Username and Password.
- The project aims to showcase the importance of network security and the need for organizations to take proactive measures to safeguard their networks.

1.2 **Description of the project**:

- The project involves the implementation of a sensor inside the firewall to inspect HTTP traffic and retrieve the Username and Password from the http://testphp.vulnweb.com/ website. As a network analyst working in the Infotech department of LPU, the primary objective of this project is to showcase the importance of network security and the need for organizations to take proactive measures to safeguard their networks.

- The target website, http://testphp.vulnweb.com/, is designed to be vulnerable to various types of attacks, including SQL injection, Cross-Site Scripting (XSS), and more. The website is used for testing purposes and is not meant to be used for production purposes. It is essential to note that any unauthorized attempt to retrieve someone's Username and Password is strictly prohibited.

- To start the project, a network analyzer tool such as Wireshark was installed on the system. A network analyzer tool is essential for capturing network traffic. The next step was to configure the tool to listen to the network interface on which the sensor was implemented. This step allowed the tool to capture all the network traffic passing through the interface.

- Once the network analyzer tool was configured, the target website http://testphp.vulnweb.com/ was accessed using a web browser. This step generated HTTP traffic that needed to be analyzed. The network analyzer tool captured the HTTP traffic, and the captured packets were analyzed using the tool.

- The captured packets contained various protocols, and it was essential to filter out the packets that contained the HTTP protocol. This step was necessary to focus on HTTP traffic only. After filtering out the packets containing the HTTP protocol, the next step was to filter out the packets that contained the POST method.

- HTTP requests can have different methods such as GET and POST. To retrieve the Username and Password, it was essential to filter out the packets that contained the POST method. Once the packets containing the POST method were filtered out, the next step was to look for the parameters "username" and "password."

- The "username" and "password" parameters contained the Username and Password that needed to be retrieved. These parameters were extracted from the captured packets using the network analyzer tool. The extracted Username and Password were then used to access the target website's admin page.

1.3 **Scope of the Project**:

The scope of the project is limited to the scanning of the target website for HTTP traffic and retrieving the Username and Password. The project does not involve any unauthorized attempt to retrieve someone's Username and Password.

2. System Description

2.1 Target System Description:

The target system is the http://testphp.vulnweb.com/ website. The website is designed to be vulnerable to various types of attacks, including SQL injection, Cross-Site Scripting (XSS), and more. The website is used for testing purposes, and it is essential to note that any unauthorized attempt to retrieve someone's Username and Password is strictly prohibited.

2.2 **Assumptions**:

1. The network analyzer tool used for the project, i.e., Wireshark is installed and configured correctly.
2. The sensor installed inside the firewall is functioning correctly and is capturing all the network traffic currently working on your browser.
3. The target website, http://testphp.vulnweb.com/, is available and accessible.
4. The captured packets contain the Username and Password required for the project.
5. The captured packets are not encrypted.

2.3 **Dependencies**:

1. The project depends on the availability and accessibility of the target website. If the website is down or inaccessible, the project cannot be completed.
2. The project depends on the functionality of the network analyzer tool. If the tool is not working correctly, the project cannot be completed.
3. The project depends on the sensor installed inside the firewall to capture all the network traffic. If the sensor is not capturing all the traffic, the project cannot be completed.
4. The project depends on the captured packets containing the Username and Password. If the packets do not contain the required information, the project cannot be completed.
5. The project depends on the captured packets being unencrypted. If the packets are encrypted, the project cannot be completed.

2.4 **Functional Dependencies**:

1. The ability to capture and analyze network traffic to retrieve the Username and Password from the http://testphp.vulnweb.com/ website.
2. The ability to filter captured packets to identify those that contain the required information.
3. The ability to extract the Username and Password from the captured packets and display them to the user.

2.5 **Non-Functional Dependencies**:

1. The network analyzer tool used for the project must be fast and accurate in capturing and analyzing network traffic.
2. The sensor installed inside the firewall must be reliable and able to capture all the network traffic.
3. The system must be secure to protect the captured data from unauthorized access.
4. The system must have a user-friendly interface to display the retrieved Username and Password.

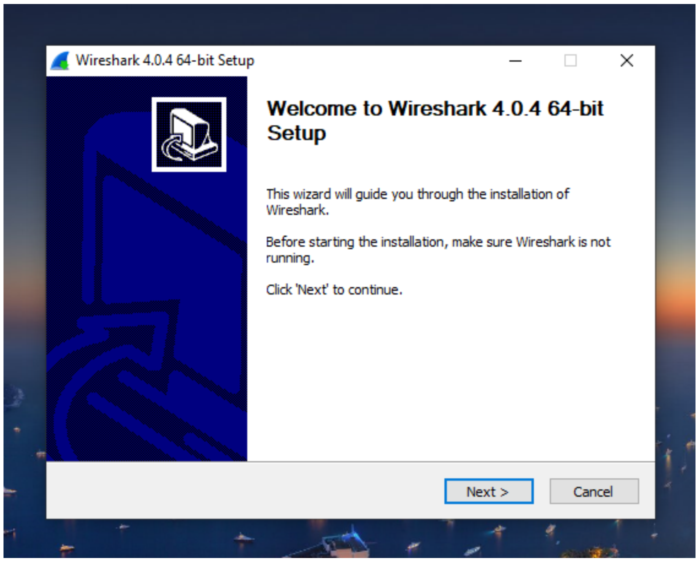
2.6 Data set used in support of your project:

1. In this project, a data set is not required to support the project's objective. The project's objective is to retrieve the Username and Password from the http://testphp.vulnweb.com/ website by capturing and analyzing network traffic.

2. The data set needed for this project is the network traffic captured by the sensor installed inside the firewall. This data set contains all the packets transmitted between the client and the http://testphp.vulnweb.com/ website. The captured data is analyzed using the network analyzer tool to identify the packets containing the Username and Password.

3. Analysis Report

1. **Download and install Wireshark:** Wireshark is a free and open-source network analyzer tool that can be downloaded from the official website. Once downloaded, install the tool on your computer.



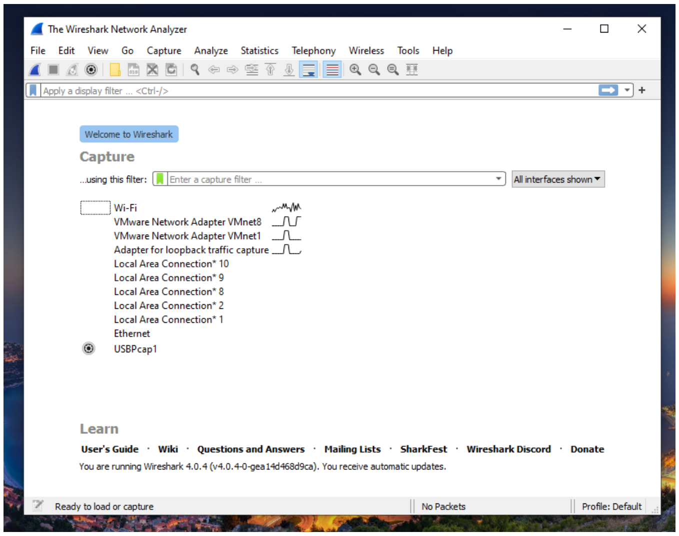
Welcome to Wireshark 4.0.4 64-bit Setup

This wizard will guide you through the installation of Wireshark.

Before starting the installation, make sure Wireshark is not running.

Click 'Next' to continue.

2. **Start Wireshark:** Launch Wireshark on your computer. You will be presented with a welcome screen.

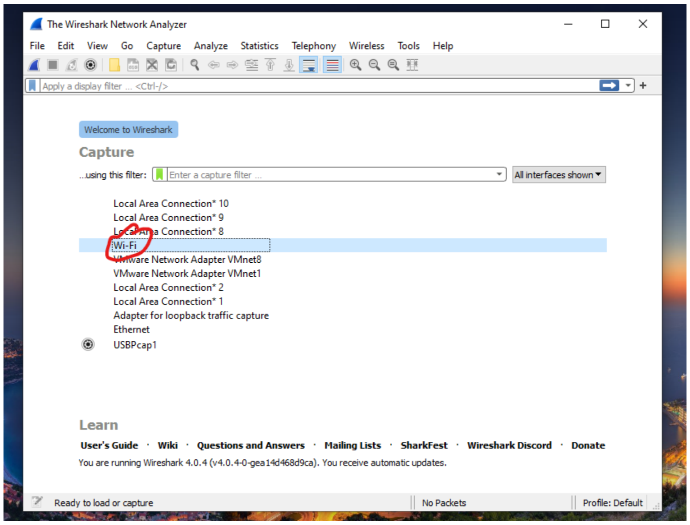


The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Wi-Fi
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Adapter for loopback traffic capture
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 2
Local Area Connection* 1
Ethernet
USBPcap1
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.0.4 (v4.0.4-0-gea14d468d9ca). You receive automatic updates.

Ready to load or capture
No Packets
Profile: Default

3. **Choose the appropriate interface:** In the top left corner, select the network interface that is connected to the network where the sensor is installed. Click on the interface to start capturing packets.

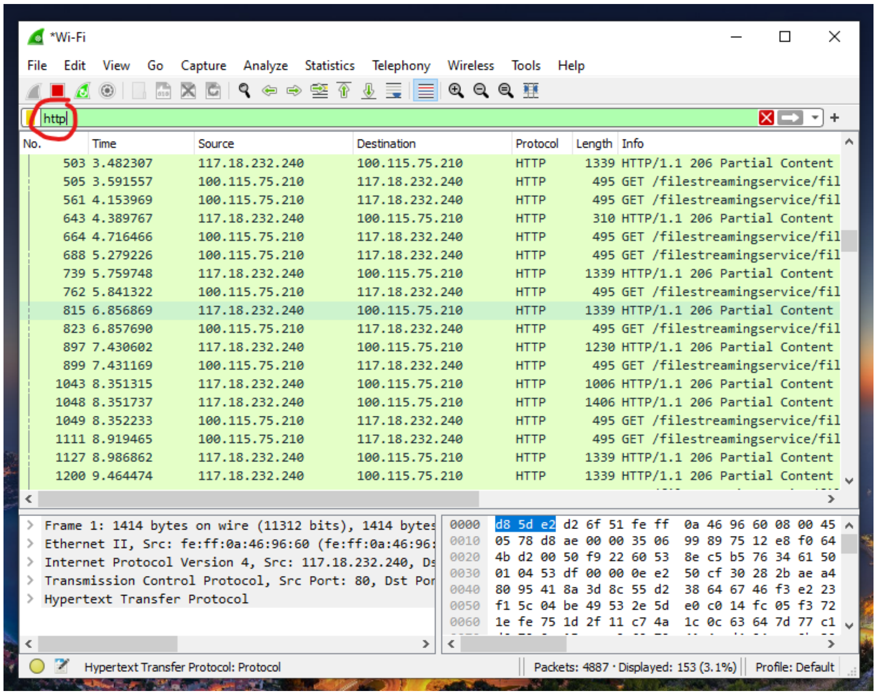

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing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

Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Wi-Fi
VMware Network Adapter VMnet8
VMware Network Adapter VMnet1
Local Area Connection* 2
Local Area Connection* 1
Adapter for loopback traffic capture
Ethernet
USBPcap1

You are running Wireshark 4.0.4 (v4.0.4-0-gea14d468d9ca). You receive automatic updates.

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

4. **Filter HTTP traffic:** In the filter bar, type "http" to display only HTTP traffic.


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

http

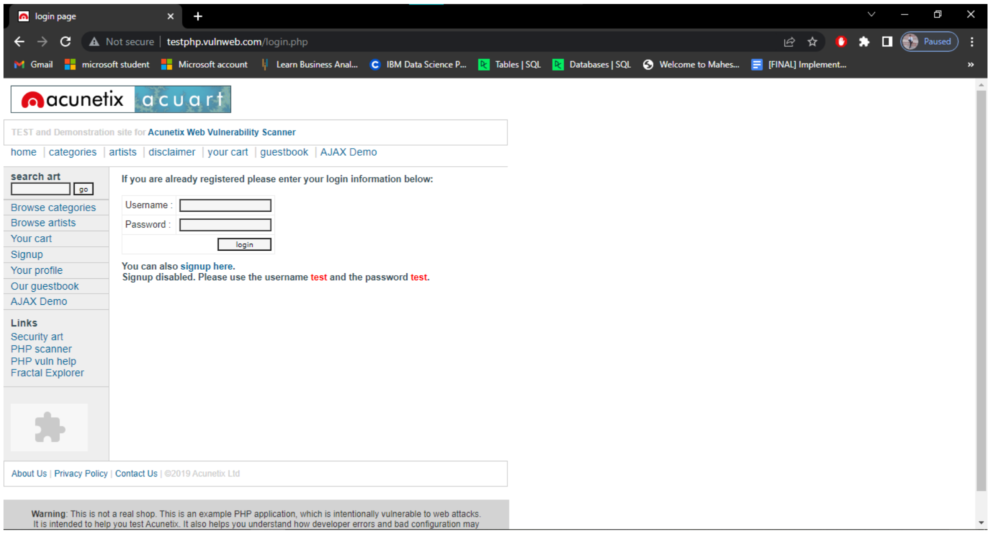
```
No.   Time       Source          Destination     Protocol Length Info
 503 3.482307    117.18.232.240  100.115.75.210  HTTP     1339 HTTP/1.1 206 Partial Content
 505 3.591557    100.115.75.210  117.18.232.240  HTTP      495 GET /filestreamingservice/fil
 561 4.153969    100.115.75.210  117.18.232.240  HTTP      495 GET /filestreamingservice/fil
 643 4.389767    117.18.232.240  100.115.75.210  HTTP      310 HTTP/1.1 206 Partial Content
 664 4.716466    100.115.75.210  117.18.232.240  HTTP      495 GET /filestreamingservice/fil
 688 5.279226    100.115.75.210  117.18.232.240  HTTP      495 GET /filestreamingservice/fil
 739 5.759748    117.18.232.240  100.115.75.210  HTTP     1339 HTTP/1.1 206 Partial Content
 762 5.841322    100.115.75.210  117.18.232.240  HTTP      495 GET /filestreamingservice/fil
 815 6.856869    117.18.232.240  100.115.75.210  HTTP     1339 HTTP/1.1 206 Partial Content
 823 6.857690    100.115.75.210  117.18.232.240  HTTP      495 GET /filestreamingservice/fil
 897 7.430602    117.18.232.240  100.115.75.210  HTTP     1230 HTTP/1.1 206 Partial Content
 899 7.431169    100.115.75.210  117.18.232.240  HTTP      495 GET /filestreamingservice/fil
1043 8.351315    117.18.232.240  100.115.75.210  HTTP     1006 HTTP/1.1 206 Partial Content
1048 8.351737    117.18.232.240  100.115.75.210  HTTP     1406 HTTP/1.1 206 Partial Content
1049 8.352233    100.115.75.210  117.18.232.240  HTTP      495 GET /filestreamingservice/fil
1111 8.919465    100.115.75.210  117.18.232.240  HTTP      495 GET /filestreamingservice/fil
1127 8.986862    117.18.232.240  100.115.75.210  HTTP     1339 HTTP/1.1 206 Partial Content
1200 9.464474    117.18.232.240  100.115.75.210  HTTP     1339 HTTP/1.1 206 Partial Content
```

```
> Frame 1: 1414 bytes on wire (11312 bits), 1414 bytes
> Ethernet II, Src: fe:ff:0a:46:96:60 (fe:ff:0a:46:96:
> Internet Protocol Version 4, Src: 117.18.232.240, Ds
> Transmission Control Protocol, Src Port: 80, Dst Por
> Hypertext Transfer Protocol
```

```
0000  d8 5d e2 d2 6f 51 fe ff  0a 46 96 60 08 00 45
0010  05 78 d8 ae 00 00 35 06  99 89 75 12 e8 f0 64
0020  4b d2 00 50 f9 22 60 53  8e c5 b5 76 34 61 50
0030  01 04 53 df 00 00 0e e2  50 cf 30 28 2b ae a4
0040  80 95 41 8a 3d 8c 55 d2  38 64 67 46 f3 e2 23
0050  f1 5c 04 be 49 53 2e 5d  e0 c0 14 fc 05 f3 72
0060  1e fe 75 1d 2f 11 c7 4a  1c 0c 63 64 7d 77 c1
```

Hypertext Transfer Protocol: Protocol | Packets: 4887 · Displayed: 153 (3.1%) | Profile: Default

5. **Access the test website:** Open a web browser and access http://testphp.vulnweb.com/. Type in any username and password combination and click on "Login."



login page
Not secure | testphp.vulnweb.com/login.php
Gmail | microsoft student | Microsoft account | Learn Business Anal... | IBM Data Science P... | Tables | SQL | Databases | SQL | Welcome to Mahes... | [FINAL] Implement...
Paused
acunetix acuart
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
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

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

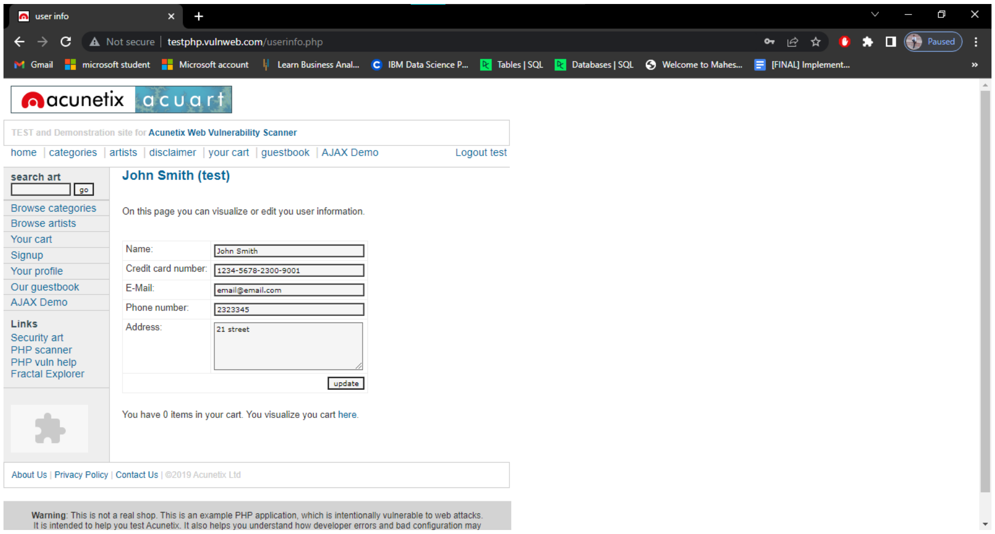
Username :

Password :

login

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



user info
Not secure | testphp.vulnweb.com/userinfo.php
Gmail | microsoft student | Microsoft account | Learn Business Anal... | IBM Data Science P... | Tables | SQL | Databases | SQL | Welcome to Mahes... | [FINAL] Implement...
Paused
acunetix acuart
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
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
update
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

John Smith (test)

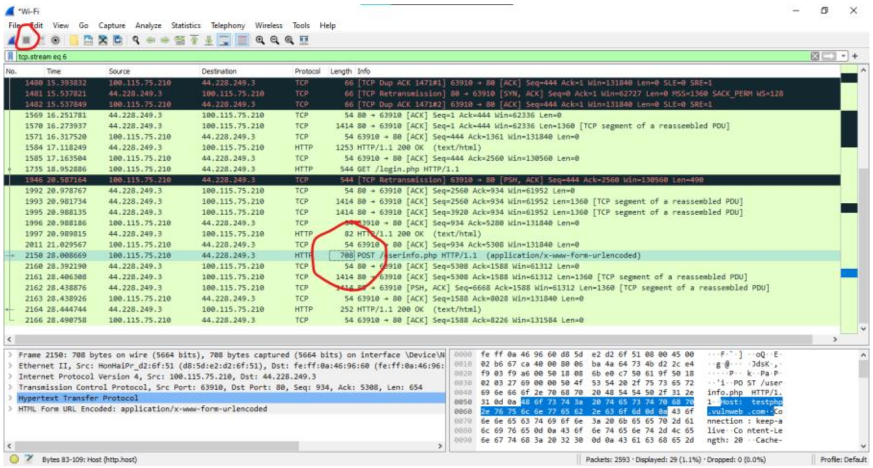
On this page you can visualize or edit you user information.

Name:	John Smith
Credit card number:	1234-5678-2300-9001
E-Mail:	email@email.com
Phone number:	2323345
Address:	21 street

You have 0 items in your cart. You visualize you cart here.

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

6. **Stop packet capture:** Once you have logged in to the website, go back to Wireshark and stop the packet capture.



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

tcp.stream eq 6

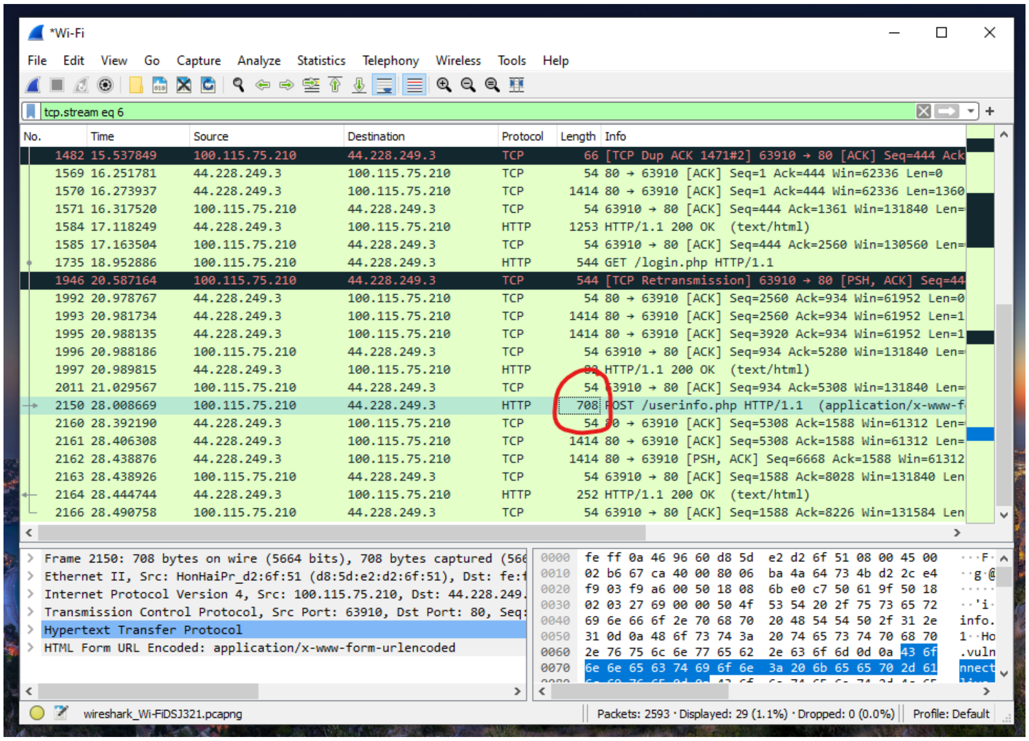
```
No.   Time       Source          Destination     Protocol Length Info
 1480 15.393832  100.115.75.210  44.228.249.3    TCP        66 [TCP Dup ACK 1471#1] 63910 → 80 [ACK] Seq=444 Ack=1 Win=131840 Len=0 SLE=0 SRE=1
 1481 15.537821  44.228.249.3    100.115.75.210  TCP        66 [TCP Retransmission] 80 → 63910 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=1360 SACK_PERM WS=128
 1482 15.537849  100.115.75.210  44.228.249.3    TCP        66 [TCP Dup ACK 1471#2] 63910 → 80 [ACK] Seq=444 Ack=1 Win=131840 Len=0 SLE=0 SRE=1
 1569 16.251781  44.228.249.3    100.115.75.210  TCP        54 80 → 63910 [ACK] Seq=1 Ack=444 Win=62336 Len=0
 1570 16.273937  44.228.249.3    100.115.75.210  TCP      1414 80 → 63910 [ACK] Seq=1 Ack=444 Win=62336 Len=1360 [TCP segment of a reassembled PDU]
 1571 16.317520  100.115.75.210  44.228.249.3    TCP        54 63910 → 80 [ACK] Seq=444 Ack=1361 Win=131840 Len=0
 1584 17.118249  44.228.249.3    100.115.75.210  HTTP     1253 HTTP/1.1 200 OK  (text/html)
 1585 17.163504  100.115.75.210  44.228.249.3    TCP        54 63910 → 80 [ACK] Seq=444 Ack=2560 Win=130560 Len=0
 1735 18.952886  100.115.75.210  44.228.249.3    HTTP      544 GET /login.php HTTP/1.1
 1946 20.587164  100.115.75.210  44.228.249.3    TCP       544 [TCP Retransmission] 63910 → 80 [PSH, ACK] Seq=444 Ack=2560 Win=130560 Len=490
 1992 20.978767  44.228.249.3    100.115.75.210  TCP        54 80 → 63910 [ACK] Seq=2560 Ack=934 Win=61952 Len=0
 1993 20.981734  44.228.249.3    100.115.75.210  TCP      1414 80 → 63910 [ACK] Seq=2560 Ack=934 Win=61952 Len=1360 [TCP segment of a reassembled PDU]
 1995 20.988135  44.228.249.3    100.115.75.210  TCP      1414 80 → 63910 [ACK] Seq=3920 Ack=934 Win=61952 Len=1360 [TCP segment of a reassembled PDU]
 1996 20.988186  100.115.75.210  44.228.249.3    TCP        54 63910 → 80 [ACK] Seq=934 Ack=5280 Win=131840 Len=0
 1997 20.989815  44.228.249.3    100.115.75.210  HTTP       82 HTTP/1.1 200 OK  (text/html)
 2011 21.029567  100.115.75.210  44.228.249.3    TCP        54 63910 → 80 [ACK] Seq=934 Ack=5308 Win=131840 Len=0
 2150 28.008669  100.115.75.210  44.228.249.3    HTTP      708 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
 2160 28.392190  44.228.249.3    100.115.75.210  TCP        54 80 → 63910 [ACK] Seq=5308 Ack=1588 Win=61312 Len=0
 2161 28.406308  44.228.249.3    100.115.75.210  TCP      1414 80 → 63910 [ACK] Seq=5308 Ack=1588 Win=61312 Len=1360 [TCP segment of a reassembled PDU]
 2162 28.438876  44.228.249.3    100.115.75.210  TCP      1414 80 → 63910 [PSH, ACK] Seq=6668 Ack=1588 Win=61312 Len=1360 [TCP segment of a reassembled PDU]
 2163 28.438926  100.115.75.210  44.228.249.3    TCP        54 63910 → 80 [ACK] Seq=1588 Ack=8028 Win=131840 Len=0
 2164 28.444744  44.228.249.3    100.115.75.210  HTTP      252 HTTP/1.1 200 OK  (text/html)
 2166 28.490758  100.115.75.210  44.228.249.3    TCP        54 63910 → 80 [ACK] Seq=1588 Ack=8226 Win=131584 Len=0
```

```
> Frame 2150: 708 bytes on wire (5664 bits), 708 bytes captured (5664 bits) on interface \Device\N
> Ethernet II, Src: HonHaiPr_d2:6f:51 (d8:5d:e2:d2:6f:51), Dst: fe:ff:0a:46:96:60 (fe:ff:0a:46:96:
> Internet Protocol Version 4, Src: 100.115.75.210, Dst: 44.228.249.3
> Transmission Control Protocol, Src Port: 63910, Dst Port: 80, Seq: 934, Ack: 5308, Len: 654
> Hypertext Transfer Protocol
> HTML Form URL Encoded: application/x-www-form-urlencoded
```

```
0000  fe ff 0a 46 96 60 d8 5d  e2 d2 6f 51 08 00 45 00   ···F·`·]··oQ··E·
0010  02 b6 67 ca 40 00 80 06  ba 4a 64 73 4b d2 2c e4   ··g·@····JdsK·,·
0020  f9 03 f9 a6 00 50 18 08  6b e0 c7 50 61 9f 50 18   ·····P··k··Pa·P·
0030  02 03 27 69 00 00 50 4f  53 54 20 2f 75 73 65 72   ··'i··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 43 6f   .vulnweb .com··Co
0070  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnection : keep-a
0080  6c 69 76 65 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   live··Co ntent-Le
0090  6e 67 74 68 3a 20 32 30  0d 0a 43 61 63 68 65 2d   ngth: 20 ··Cache-
```

Bytes 83-109: Host (http.host) | Packets: 2593 · Displayed: 29 (1.1%) · Dropped: 0 (0.0%) | Profile: Default

7. **Analyze the captured packets:** In the packet list, locate the packets that contain the HTTP POST request for the login form. Expand the packet details to view the form data.


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

tcp.stream eq 6

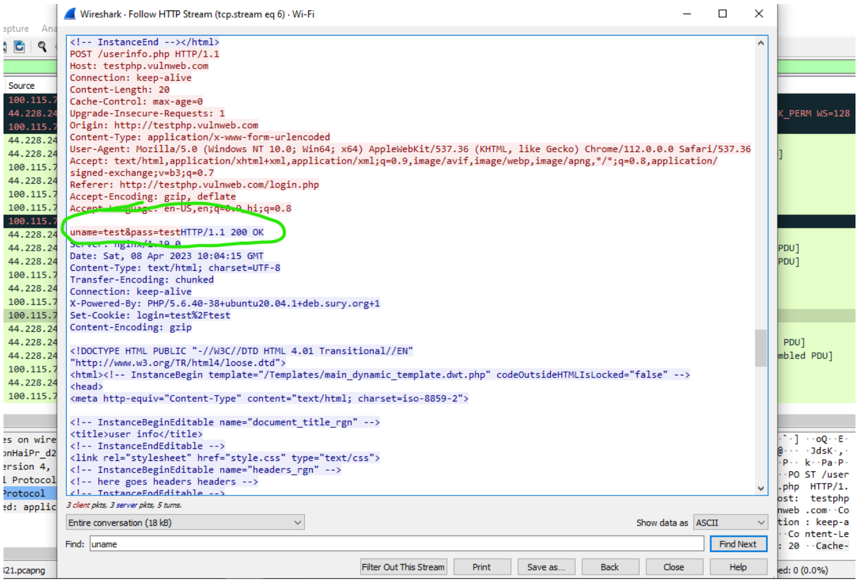
```
No.   Time       Source          Destination     Protocol Length Info
1482 15.537849  100.115.75.210  44.228.249.3    TCP        66 [TCP Dup ACK 1471#2] 63910 → 80 [ACK] Seq=444 Ack
1569 16.251781  44.228.249.3    100.115.75.210  TCP        54 80 → 63910 [ACK] Seq=1 Ack=444 Win=62336 Len=0
1570 16.273937  44.228.249.3    100.115.75.210  TCP      1414 80 → 63910 [ACK] Seq=1 Ack=444 Win=62336 Len=1360
1571 16.317520  100.115.75.210  44.228.249.3    TCP        54 63910 → 80 [ACK] Seq=444 Ack=1361 Win=131840 Len=
1584 17.118249  44.228.249.3    100.115.75.210  HTTP     1253 HTTP/1.1 200 OK  (text/html)
1585 17.163504  100.115.75.210  44.228.249.3    TCP        54 63910 → 80 [ACK] Seq=444 Ack=2560 Win=130560 Len=
1735 18.952886  100.115.75.210  44.228.249.3    HTTP      544 GET /login.php HTTP/1.1
1946 20.587164  100.115.75.210  44.228.249.3    TCP       544 [TCP Retransmission] 63910 → 80 [PSH, ACK] Seq=44
1992 20.978767  44.228.249.3    100.115.75.210  TCP        54 80 → 63910 [ACK] Seq=2560 Ack=934 Win=61952 Len=0
1993 20.981734  44.228.249.3    100.115.75.210  TCP      1414 80 → 63910 [ACK] Seq=2560 Ack=934 Win=61952 Len=1
1995 20.988135  44.228.249.3    100.115.75.210  TCP      1414 80 → 63910 [ACK] Seq=3920 Ack=934 Win=61952 Len=1
1996 20.988186  100.115.75.210  44.228.249.3    TCP        54 63910 → 80 [ACK] Seq=934 Ack=5280 Win=131840 Len=
1997 20.989815  44.228.249.3    100.115.75.210  HTTP       82 HTTP/1.1 200 OK  (text/html)
2011 21.029567  100.115.75.210  44.228.249.3    TCP        54 63910 → 80 [ACK] Seq=934 Ack=5308 Win=131840 Len=
2150 28.008669  100.115.75.210  44.228.249.3    HTTP      708 POST /userinfo.php HTTP/1.1  (application/x-www-f
2160 28.392190  44.228.249.3    100.115.75.210  TCP        54 80 → 63910 [ACK] Seq=5308 Ack=1588 Win=61312 Len=
2161 28.406308  44.228.249.3    100.115.75.210  TCP      1414 80 → 63910 [ACK] Seq=5308 Ack=1588 Win=61312 Len=
2162 28.438876  44.228.249.3    100.115.75.210  TCP      1414 80 → 63910 [PSH, ACK] Seq=6668 Ack=1588 Win=61312
2163 28.438926  100.115.75.210  44.228.249.3    TCP        54 63910 → 80 [ACK] Seq=1588 Ack=8028 Win=131840 Len
2164 28.444744  44.228.249.3    100.115.75.210  HTTP      252 HTTP/1.1 200 OK  (text/html)
2166 28.490758  100.115.75.210  44.228.249.3    TCP        54 63910 → 80 [ACK] Seq=1588 Ack=8226 Win=131584 Len
```

```
> Frame 2150: 708 bytes on wire (5664 bits), 708 bytes captured (566
> Ethernet II, Src: HonHaiPr_d2:6f:51 (d8:5d:e2:d2:6f:51), Dst: fe:f
> Internet Protocol Version 4, Src: 100.115.75.210, Dst: 44.228.249.
> Transmission Control Protocol, Src Port: 63910, Dst Port: 80, Seq:
> Hypertext Transfer Protocol
> HTML Form URL Encoded: application/x-www-form-urlencoded
```

```
0000  fe ff 0a 46 96 60 d8 5d  e2 d2 6f 51 08 00 45 00   ···F·
0010  02 b6 67 ca 40 00 80 06  ba 4a 64 73 4b d2 2c e4   ··g·@
0020  f9 03 f9 a6 00 50 18 08  6b e0 c7 50 61 9f 50 18   ·····
0030  02 03 27 69 00 00 50 4f  53 54 20 2f 75 73 65 72   ··'i·
0040  69 6e 66 6f 2e 70 68 70  20 48 54 54 50 2f 31 2e   info.
0050  31 0d 0a 48 6f 73 74 3a  20 74 65 73 74 70 68 70   1··Ho
0060  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 0d 0a 43 6f   .vuln
0070  6e 6e 65 63 74 69 6f 6e  3a 20 6b 65 65 70 2d 61   nnect
```

wireshark_Wi-FiDSJ321.pcapng | Packets: 2593 · Displayed: 29 (1.1%) · Dropped: 0 (0.0%) | Profile: Default

8. **Locate the Username and Password:** Look for the "Username" and "Password" fields in the form data. The values entered in these fields will be displayed next to them.



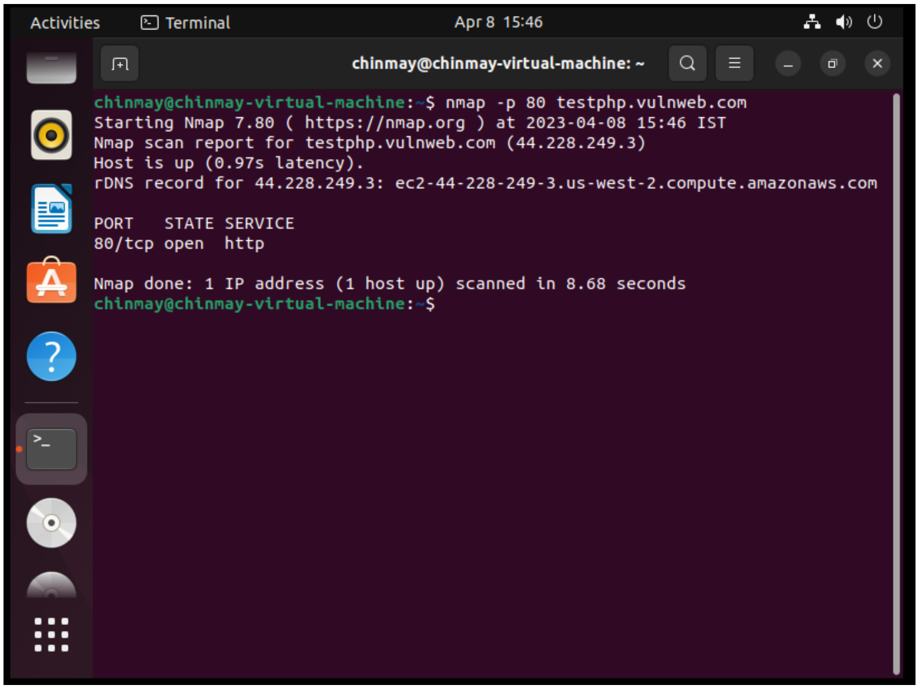
```
<!-- InstanceEnd --></html>
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Connection: keep-alive
Content-Length: 20
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;v=b3;q=0.7
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,hi;q=0.8

uname=test&pass=testHTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Sat, 08 Apr 2023 10:04:15 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
Set-Cookie: login=test%2Ftest
Content-Encoding: gzip

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

<!-- InstanceBeginEditable name="document_title_rgn" -->
<title>user info</title>
<!-- InstanceEndEditable -->
<link rel="stylesheet" href="style.css" type="text/css">
<!-- InstanceBeginEditable name="headers_rgn" -->
<!-- here goes headers headers -->
<!-- InstanceEndEditable -->
```

3 client pkts, 3 server pkts, 5 turns.

Entire conversation (18 kB) | Show data as: ASCII

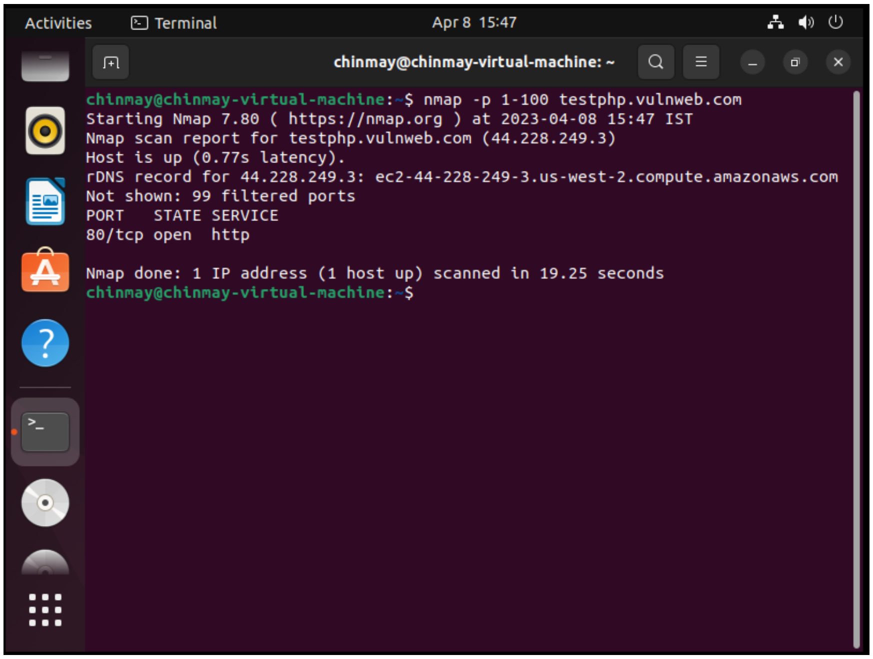
Find: uname

9. You can start by scanning the website's port to determine which services are running and which ports are open. This can be done using a port scanner tool like Nmap.
   Command: *nmap testphp.vulnweb.com*
10. To scan a single port (e.g., port 80) using nmap: *nmap -p 80 testphp.vulnweb.com*



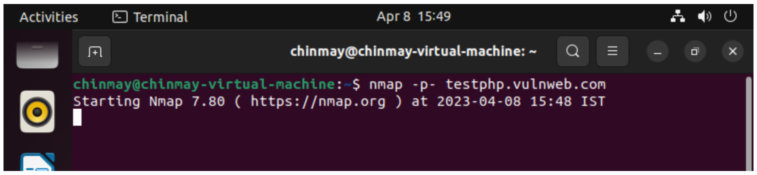
```
chinmay@chinmay-virtual-machine:~$ nmap -p 80 testphp.vulnweb.com
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-08 15:46 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.97s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com

PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 8.68 seconds
chinmay@chinmay-virtual-machine:~$
```

11. To scan a range of ports (e.g., ports 1 to 100) using nmap: *nmap -p 1-100 testphp.vulnweb.com*



```
chinmay@chinmay-virtual-machine:~$ nmap -p 1-100 testphp.vulnweb.com
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-08 15:47 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.77s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 99 filtered ports
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 19.25 seconds
chinmay@chinmay-virtual-machine:~$
```

12. To scan all ports using nmap: *nmap -p- testphp.vulnweb.com*



```
chinmay@chinmay-virtual-machine:~$ nmap -p- testphp.vulnweb.com
Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-08 15:48 IST
```

4. Reference/Bibliography:

1. Wireshark - https://www.wireshark.org/
2. HTTP - https://developer.mozilla.org/en-US/docs/Web/HTTP
3. http://testphp.vulnweb.com/ - https://www.owasp.org/index.php/OWASP_Vulnerable_Web_Applications_Directory_Project
4. Capture Filters in Wireshark - https://www.wireshark.org/docs/wsug_html_chunked/ChCapCaptureFilterSection.html
5. Display Filters in Wireshark - https://www.wireshark.org/docs/wsug_html_chunked/ChWorkDisplayFilterSection.html
6. Wireshark User Guide - https://www.wireshark.org/docs/wsug_html/
7. Nmap - https://nmap.org/
8. Nmap Tutorial - https://nmap.org/book/toc.html

5. Github Link:

https://github.com/chinmaylahoti/INT301-CA3