WIRESHARK (TASK 10)

Project report (CA3) submitted in fulfilment of the requirements for the Degree of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

By

SAMAKSH BANSAL

(11912543)

Roll No. 35

SUBJECT

INT301 – OPEN-SOURCE TECHNOLOGIES

School of Computer Science and Engineering
Lovely Professional University
Phagwara, Punjab (India)

Month April Year 2023

LIST OF CONTENTS

1. INTRODUCTION

1.1 OBJECTIVE OF THE PROJECT

In this project, the objective is to inspect HTTP traffic and retrieve the username and password from the BSNL website using an appropriate tool. The project aims to demonstrate how an attacker can exploit the security vulnerabilities in the website and gain access to sensitive information.

1.2 DESCRIPTION OF THE PROJECT

The project involves the use of Wireshark, a popular network protocol analyzer tool, to capture and analyze HTTP traffic between the user's computer and the BSNL website. The tool will allow us to inspect the packets and extract the username and password sent by the user to the website.

The project will focus on identifying the security weaknesses in the website's login process that allow an attacker to intercept and steal the user's credentials. It will involve analyzing the HTTP packets for any unencrypted data and looking for patterns that indicate the username and password.

1.3 SCOPE OF THE PROJECT:

The scope of the project is limited to the BSNL website and its login process. The project will not involve any actual hacking or exploitation of the website's security vulnerabilities. Instead, it will focus on demonstrating how an attacker can use Wireshark to intercept and retrieve sensitive information from the website's traffic.

The project will provide insights into the importance of secure website design and the use of encryption to protect sensitive user data. It will also demonstrate the need for users to be cautious when entering their credentials on websites and the importance of using strong and unique passwords.

2. SYSTEM DESCRIPTION

2.1 TARGET SYSTEM DESCRIPTION:

The target system for this project is the BSNL website's login process. The website uses HTTP protocol to transmit data between the user's computer and the website's servers. The login process involves the user entering their username and password into a form on the website, which is then transmitted to the server for authentication.

2.2 ASSUMPTIONS AND DEPENDENCIES:

The assumptions for this project include:

i. The user is using an unsecured Wi-Fi network, which can be intercepted by an attacker.
ii. The website does not use any encryption or security protocols to protect the user's credentials during transmission.
iii. The user's computer is not infected with any malware that can intercept and steal their credentials.
iv. The dependencies for this project include:
v. Wireshark, the network protocol analyzer tool used to capture and analyze the website's traffic.
vi. An internet connection to access the BSNL website.
vii. A web browser to access the BSNL website and enter the login credentials.

2.3 **FUNCTIONAL/NON-FUNCTIONAL DEPENDENCIES:**

i. The functional dependencies for this project include:
ii. The ability of Wireshark to capture and analyze HTTP traffic between the user's computer and the BSNL website.
iii. The user's ability to access the BSNL website and enter their login credentials.
iv. The non-functional dependencies for this project include:
v. The speed and reliability of the user's internet connection.
vi. The compatibility of Wireshark with the user's operating system and hardware.

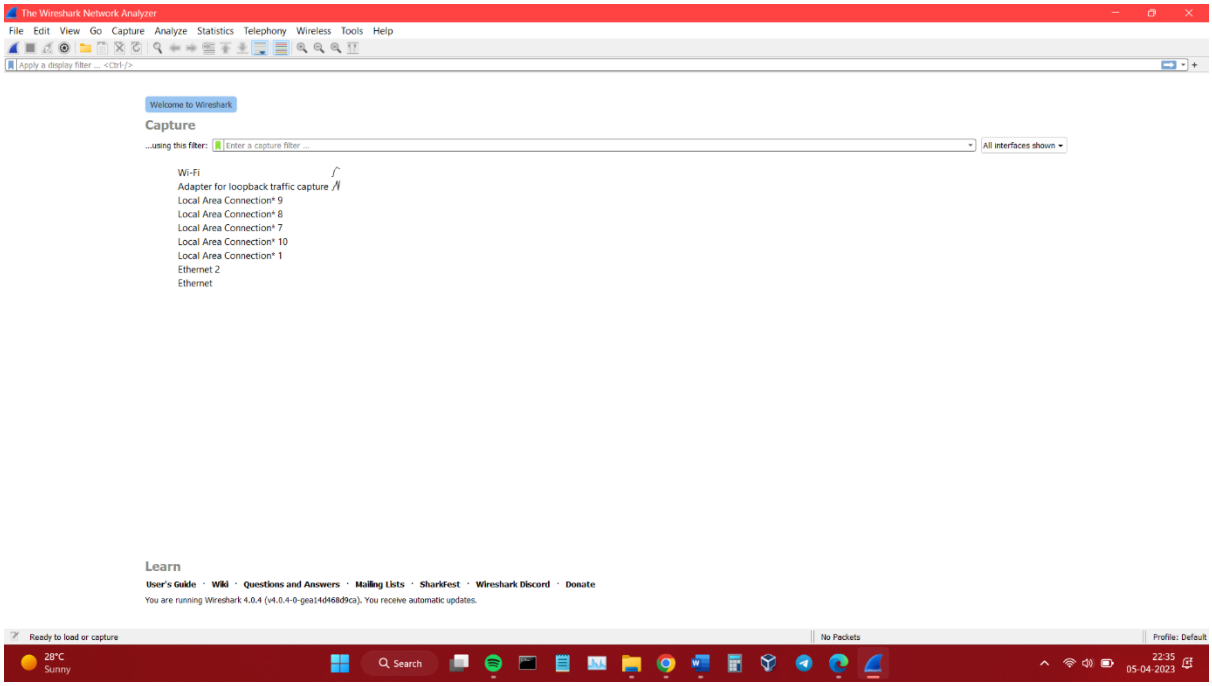
2.4 DATA SET USED IN SUPPORT OF YOUR PROJECT:

This project focuses on capturing and analyzing live HTTP traffic between the user's computer and the BSNL website, without the need for a specific data set. The main objective is to extract the username and password from the traffic, and to demonstrate the techniques used through sample data. The process involves analyzing the data packets sent and received during the login process and identifying the relevant fields containing the login credentials. The project aims to provide insight into the vulnerabilities present in HTTP traffic, and to raise awareness about the importance of secure communication protocols in online transactions.

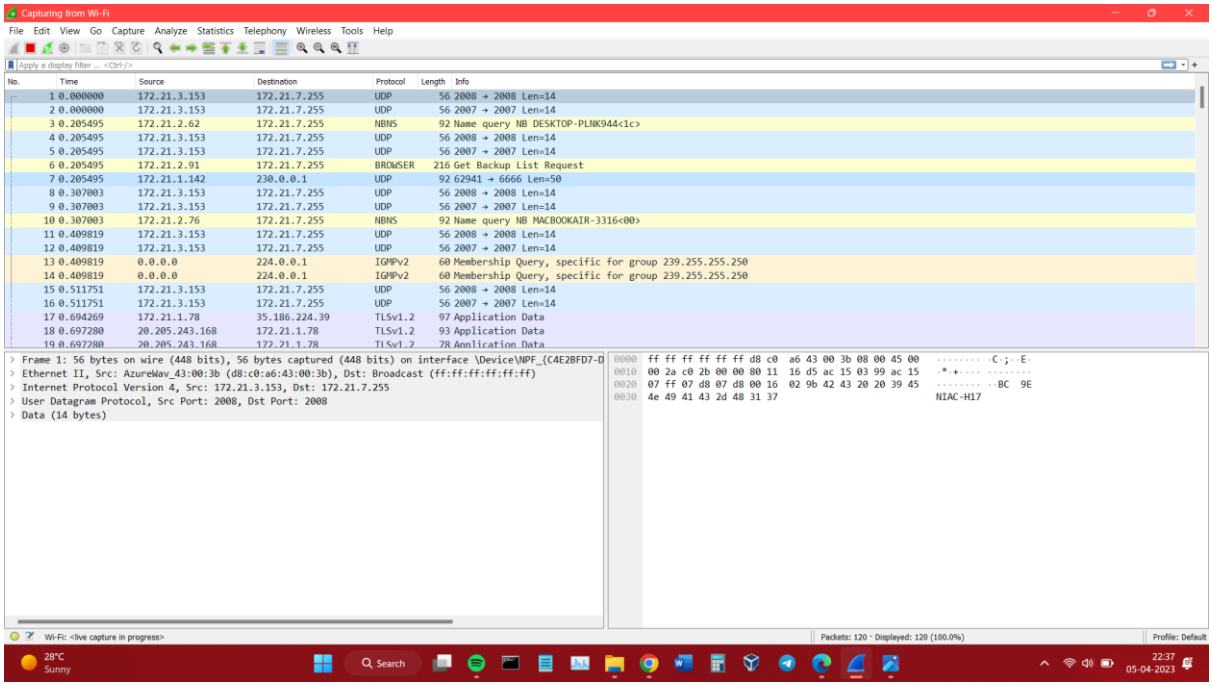
3. ANALYSIS REPORT

3.1 SYSTEM SNAPSHOTS AND FULL ANALYSIS REPORT

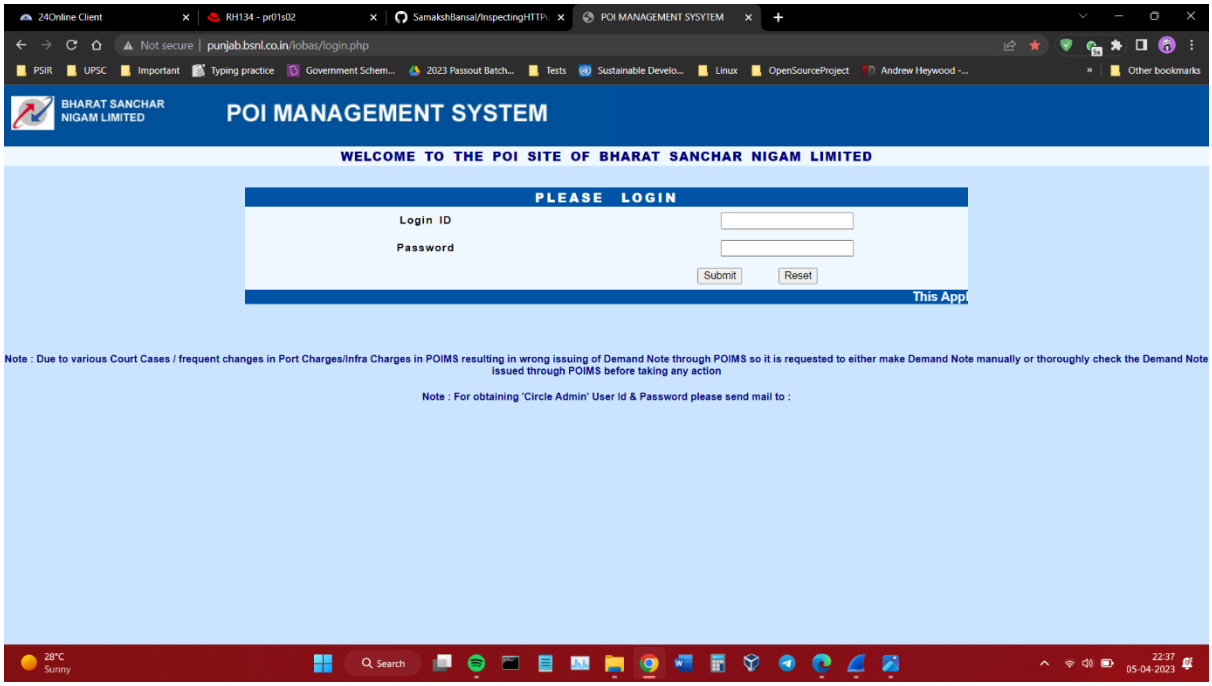
1.



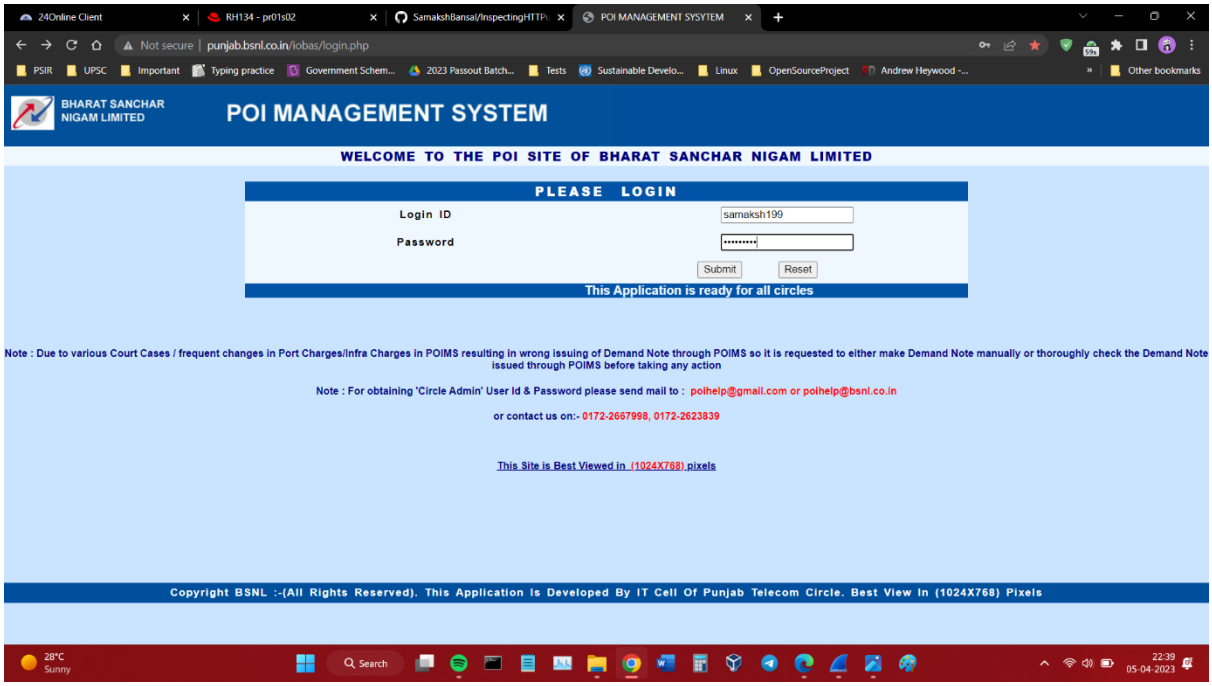
2.



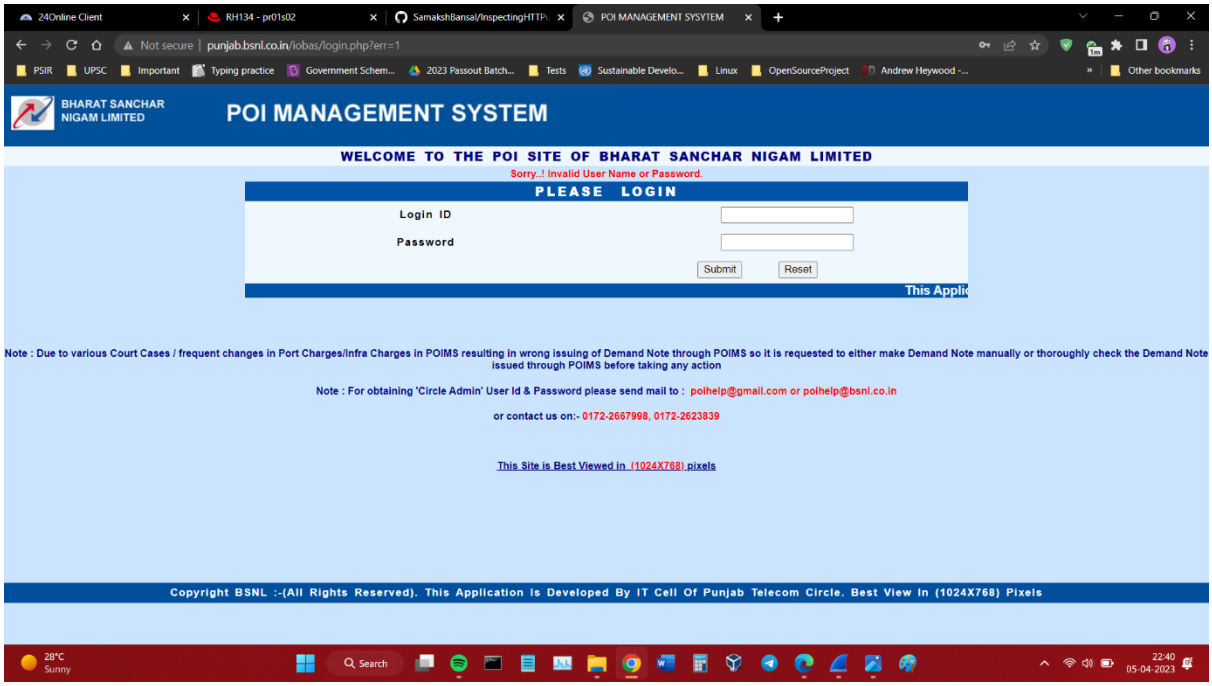
3.


POI MANAGEMENT SYSYTEM
punjab.bsnl.co.in/iobas/login.php
BHARAT SANCHAR NIGAM LIMITED
POI MANAGEMENT SYSTEM
WELCOME TO THE POI SITE OF BHARAT SANCHAR NIGAM LIMITED
PLEASE LOGIN
Login ID
Password
Submit
Reset
This Appl
Note : Due to various Court Cases / frequent changes in Port Charges/Infra Charges in POIMS resulting in wrong issuing of Demand Note through POIMS so it is requested to either make Demand Note manually or thoroughly check the Demand Note issued through POIMS before taking any action
Note : For obtaining 'Circle Admin' User Id & Password please send mail to :

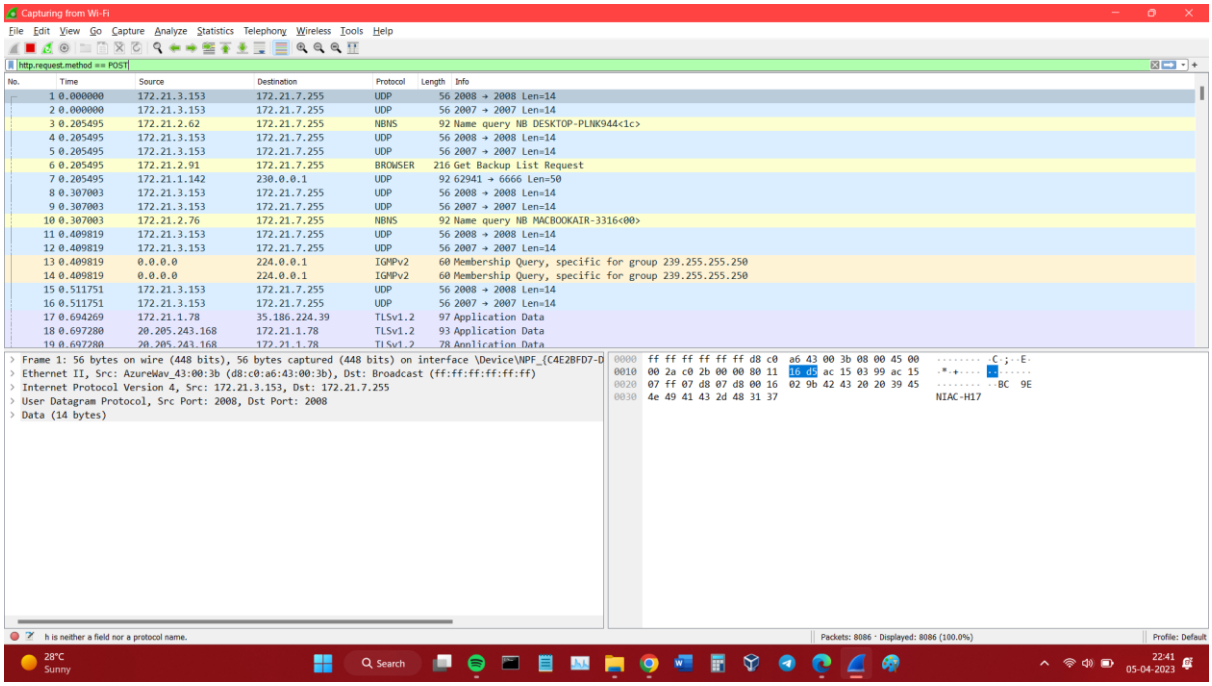
4.


POI MANAGEMENT SYSYTEM
punjab.bsnl.co.in/iobas/login.php
BHARAT SANCHAR NIGAM LIMITED
POI MANAGEMENT SYSTEM
WELCOME TO THE POI SITE OF BHARAT SANCHAR NIGAM LIMITED
PLEASE LOGIN
Login ID
samaksh199
Password
Submit
Reset
This Application is ready for all circles
Note : Due to various Court Cases / frequent changes in Port Charges/Infra Charges in POIMS resulting in wrong issuing of Demand Note through POIMS so it is requested to either make Demand Note manually or thoroughly check the Demand Note issued through POIMS before taking any action
Note : For obtaining 'Circle Admin' User Id & Password please send mail to : poihelp@gmail.com or poihelp@bsnl.co.in
or contact us on:- 0172-2667998, 0172-2623839
This Site is Best Viewed in (1024X768) pixels
Copyright BSNL :-(All Rights Reserved). This Application Is Developed By IT Cell Of Punjab Telecom Circle. Best View In (1024X768) Pixels

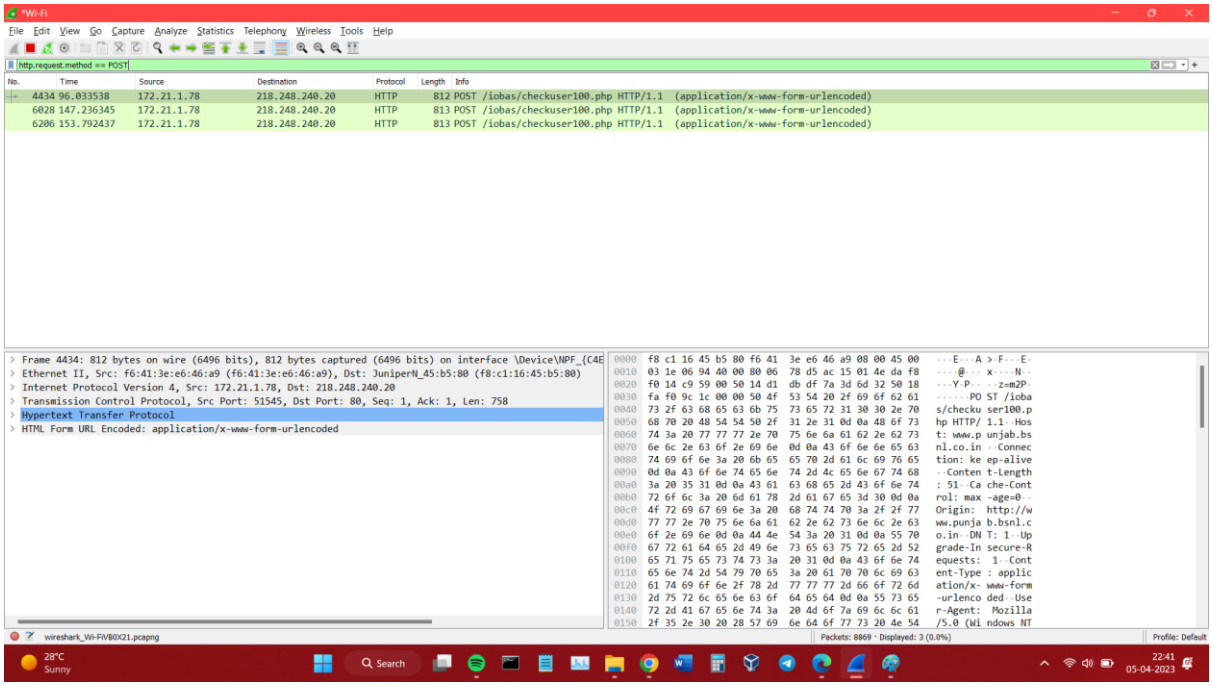
5.


POI MANAGEMENT SYSTEM
BHARAT SANCHAR NIGAM LIMITED
WELCOME TO THE POI SITE OF BHARAT SANCHAR NIGAM LIMITED
Sorry..! Invalid User Name or Password.
PLEASE LOGIN
Login ID
Password
Submit
Reset
Note : Due to various Court Cases / frequent changes in Port Charges/Infra Charges in POIMS resulting in wrong issuing of Demand Note through POIMS so it is requested to either make Demand Note manually or thoroughly check the Demand Note issued through POIMS before taking any action
Note : For obtaining 'Circle Admin' User Id & Password please send mail to : poihelp@gmail.com or poihelp@bsnl.co.in
or contact us on:- 0172-2667998, 0172-2623839
This Site is Best Viewed in (1024X768) pixels
Copyright BSNL :-(All Rights Reserved). This Application Is Developed By IT Cell Of Punjab Telecom Circle. Best View In (1024X768) Pixels

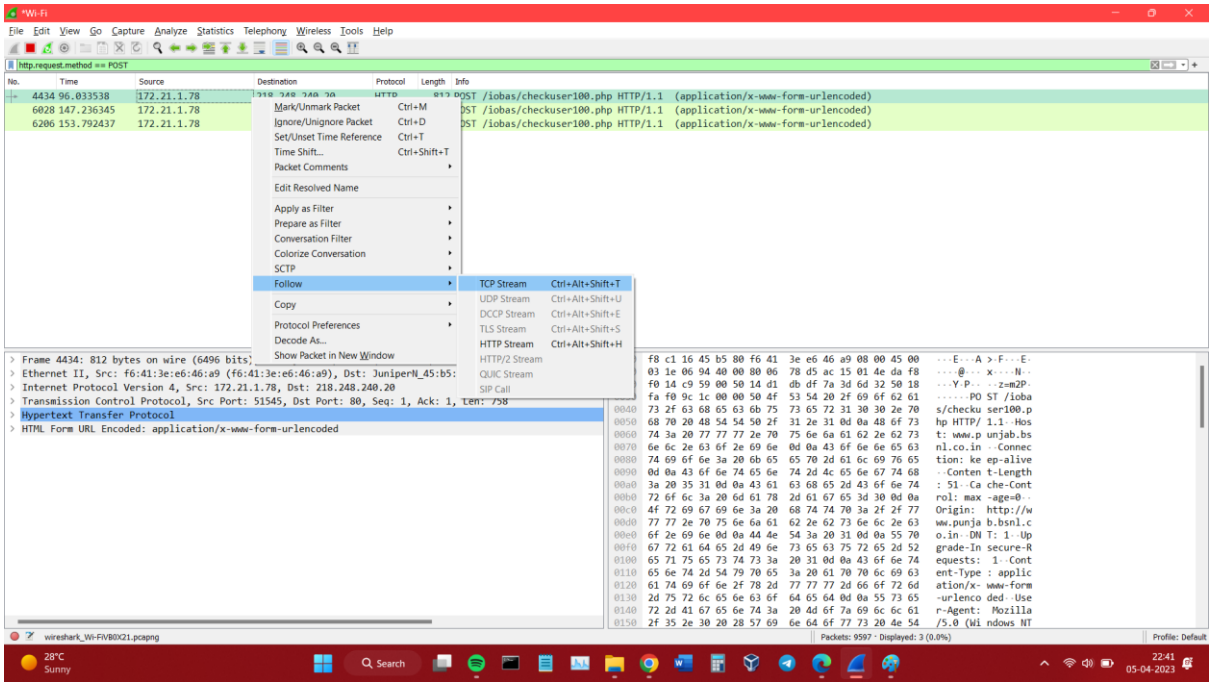
6.


Capturing from Wi-Fi
http.request.method == POST
Frame 1: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF_{C4E2BFD7-D
Ethernet II, Src: AzureWav_43:00:3b (d8:c0:a6:43:00:3b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 172.21.3.153, Dst: 172.21.7.255
User Datagram Protocol, Src Port: 2008, Dst Port: 2008
Data (14 bytes)

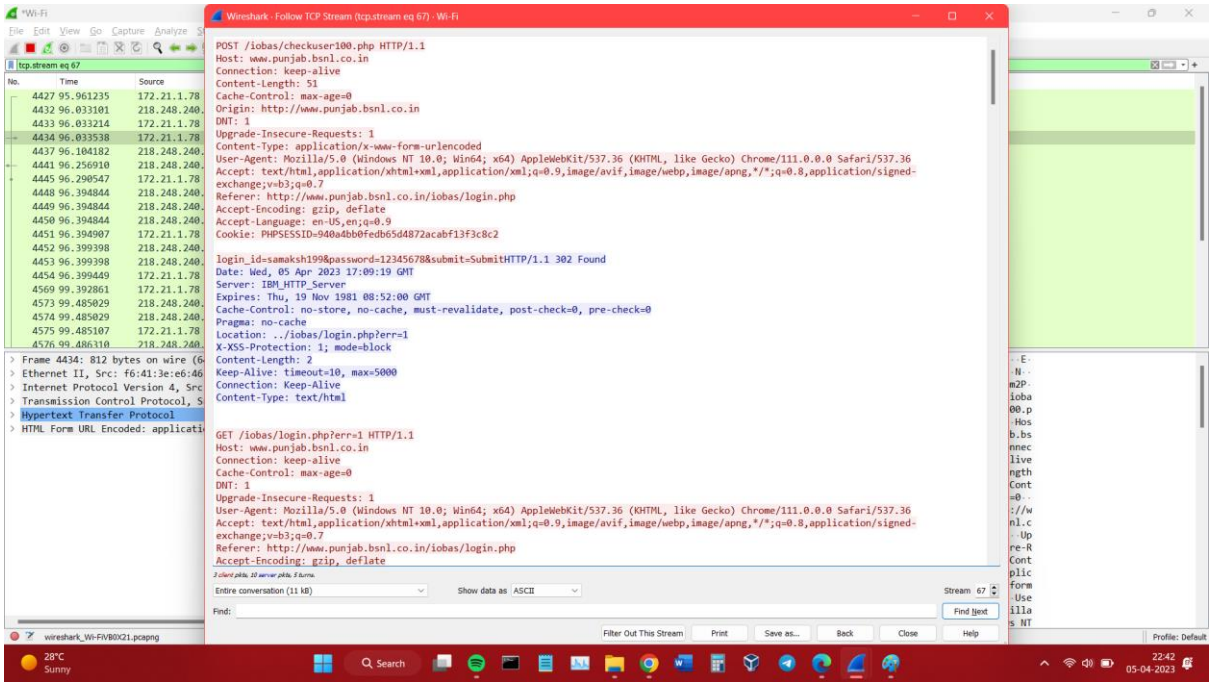
7.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.method == POST
No. Time Source Destination Protocol Length Info
4434 96.033538 172.21.1.78 218.248.240.20 HTTP 812 POST /iobas/checkuser100.php HTTP/1.1 (application/x-www-form-urlencoded)
6028 147.236345 172.21.1.78 218.248.240.20 HTTP 813 POST /iobas/checkuser100.php HTTP/1.1 (application/x-www-form-urlencoded)
6206 153.792437 172.21.1.78 218.248.240.20 HTTP 813 POST /iobas/checkuser100.php HTTP/1.1 (application/x-www-form-urlencoded)
Frame 4434: 812 bytes on wire (6496 bits), 812 bytes captured (6496 bits) on interface \Device\NPF_{C4E
Ethernet II, Src: f6:41:3e:e6:46:a9 (f6:41:3e:e6:46:a9), Dst: JuniperN_45:b5:80 (f8:c1:16:45:b5:80)
Internet Protocol Version 4, Src: 172.21.1.78, Dst: 218.248.240.20
Transmission Control Protocol, Src Port: 51545, Dst Port: 80, Seq: 1, Ack: 1, Len: 758
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
wireshark_Wi-FiVB0X21.pcapng
Packets: 8869 · Displayed: 3 (0.0%)
Profile: Default
28°C Sunny
Search
22:41 05-04-2023

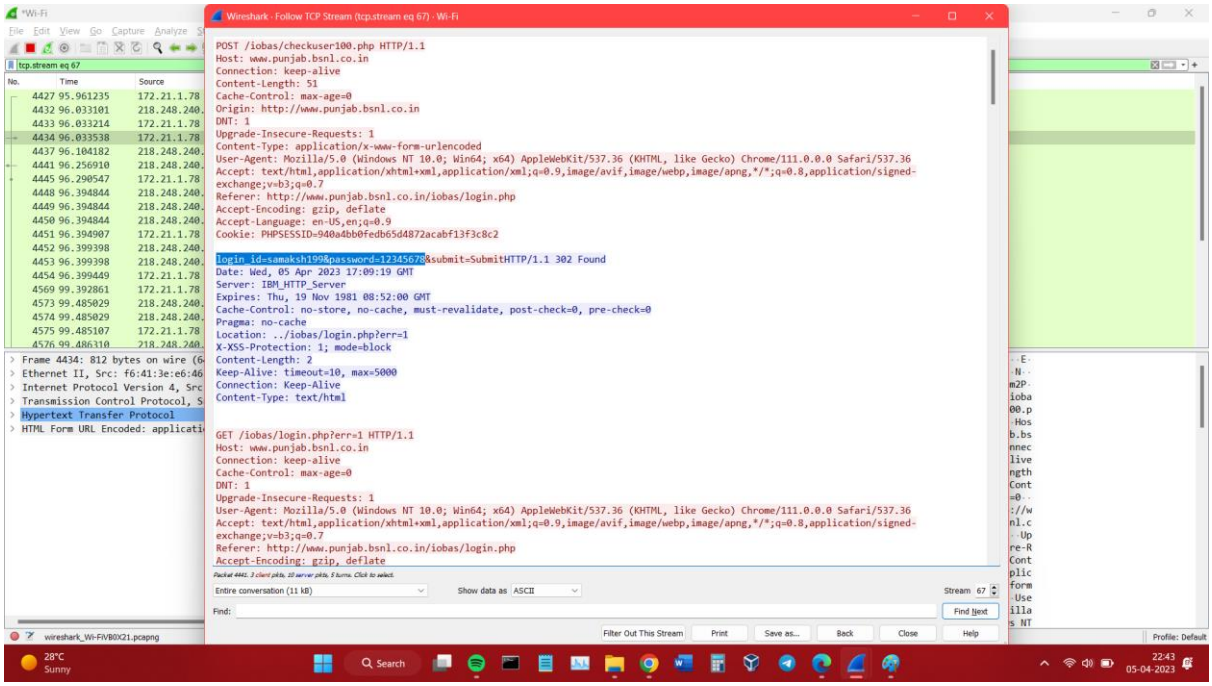
8.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.method == POST
No. Time Source Destination Protocol Length Info
4434 96.033538 172.21.1.78
6028 147.236345 172.21.1.78
6206 153.792437 172.21.1.78
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
Frame 4434: 812 bytes on wire (6496 bits)
Ethernet II, Src: f6:41:3e:e6:46:a9 (f6:41:3e:e6:46:a9), Dst: JuniperN_45:b5:
Internet Protocol Version 4, Src: 172.21.1.78, Dst: 218.248.240.20
Transmission Control Protocol, Src Port: 51545, Dst Port: 80, Seq: 1, Ack: 1, Len: 758
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
wireshark_Wi-FiVB0X21.pcapng
Packets: 9597 · Displayed: 3 (0.0%)
Profile: Default
28°C Sunny
Search
22:41 05-04-2023

9.


Wireshark · Follow TCP Stream (tcp.stream eq 67) · Wi-Fi
POST /iobas/checkuser100.php HTTP/1.1
Host: www.punjab.bsnl.co.in
Connection: keep-alive
Content-Length: 51
Cache-Control: max-age=0
Origin: http://www.punjab.bsnl.co.in
DNT: 1
Upgrade-Insecure-Requests: 1
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/111.0.0.0 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://www.punjab.bsnl.co.in/iobas/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=940a4bb0fedb65d4872acabf13f3c8c2
login_id=samaksh199&password=12345678&submit=SubmitHTTP/1.1 302 Found
Date: Wed, 05 Apr 2023 17:09:19 GMT
Server: IBM_HTTP_Server
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Location: ../iobas/login.php?err=1
X-XSS-Protection: 1; mode=block
Content-Length: 2
Keep-Alive: timeout=10, max=5000
Connection: Keep-Alive
Content-Type: text/html
GET /iobas/login.php?err=1 HTTP/1.1
Host: www.punjab.bsnl.co.in
Connection: keep-alive
Cache-Control: max-age=0
DNT: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 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://www.punjab.bsnl.co.in/iobas/login.php
Accept-Encoding: gzip, deflate
Entire conversation (11 kB)
Show data as ASCII
Stream 67
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

10.


Wireshark · Follow TCP Stream (tcp.stream eq 67) · Wi-Fi
POST /iobas/checkuser100.php HTTP/1.1
Host: www.punjab.bsnl.co.in
Connection: keep-alive
Content-Length: 51
Cache-Control: max-age=0
Origin: http://www.punjab.bsnl.co.in
DNT: 1
Upgrade-Insecure-Requests: 1
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/111.0.0.0 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://www.punjab.bsnl.co.in/iobas/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=940a4bb0fedb65d4872acabf13f3c8c2
login_id=samaksh199&password=12345678&submit=SubmitHTTP/1.1 302 Found
Date: Wed, 05 Apr 2023 17:09:19 GMT
Server: IBM_HTTP_Server
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Location: ../iobas/login.php?err=1
X-XSS-Protection: 1; mode=block
Content-Length: 2
Keep-Alive: timeout=10, max=5000
Connection: Keep-Alive
Content-Type: text/html
GET /iobas/login.php?err=1 HTTP/1.1
Host: www.punjab.bsnl.co.in
Connection: keep-alive
Cache-Control: max-age=0
DNT: 1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 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://www.punjab.bsnl.co.in/iobas/login.php
Accept-Encoding: gzip, deflate
Entire conversation (11 kB)
Show data as ASCII
Stream 67
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

4. GITHUB LINK

- **LINK:**

https://github.com/SamakshBansal/InspectingHTTPusingWireShark

5. REFERENCE AND BIBLOGRAPHY

i. Wireshark - Go deep. (n.d.). Retrieved March 26, 2023, from https://www.wireshark.org/

ii. BSNL. (n.d.). Retrieved March 26, 2023, from https://www.bsnl.co.in/

iii. M. M. Adeel Arif, N. M. Arif, & A. H. Malik. (2017). Security assessment of web applications: An insight into OWASP top 10 vulnerabilities. Journal of King Saud University - Computer and Information Sciences, 29(4), 512-525.

iv. Shobha, B. R., & Shylaja, B. S. (2015). Analysis of web application security vulnerabilities using OWASP. Procedia Computer Science, 45, 697-706.

v. OWASP Top Ten Project. (n.d.). Retrieved March 26, 2023, from https://owasp.org/www-project-top-ten/

vi. HTTP/1.1: Authentication. (n.d.). Retrieved March 26, 2023, from https://tools.ietf.org/html/rfc7235#section-4

vii. Singh, S., & Singh, S. P. (2013). Web application security: A review of the state of the art. International Journal of Computer Applications, 78(8), 10-15.