EKETE
International Journal of Advanced Research

ISSN 3027-2513 (ONLINE) ISSN 3027-169X (PRINT) Volume 2 Number 2, March 2024
https://journals.journalsplace.org/index.php/Ekete

ENHANCING DATA SECURITY ANALYSIS ON THE AKANU IBIAM FEDERAL POLYTECHNIC UNWANA WEBSITE THROUGH WIRESHARK APPLICATION UTILIZATION

G.O. Asoronye[1]*, E. Okekenwa[2], B.O. Osuesu[3]
[1]Computer Engineering Department
[2&3]Electrical Electronic Engineering Department
Akanu Ibiam Federal Polytechnic Unwana, Ebonyi State.
*Corresponding email: *asorgay@gmail.com*

Abstract

In this era of digital communication, data security is of utmost importance particularly across networks. The proliferation of computer networks and open systems on the one hand has made accessibility more convenient on the other hand they have introduced vulnerabilities, exposing data transmission to risks from unauthorized interception or exploitation by malicious entities. Adware, Trojans and other categories of Malwares pose threats to software security, while internet protocols like Hyper Text Transfer Protocol (HTTP) are susceptible to exploitation, leading to data breaches and unauthorized access. This work focused on analyzing the security vulnerabilities within the Akanu Ibiam Federal Polytechnic (A.I.F.P.U.) website, a pivotal tool in managing and facilitating the learning process. Through the implementation of Wireshark, a network protocol analyzer, data packets transmitted via the HTTP protocol were captured and analyzed to identify potential risks, particularly regarding usernames and passwords. The discoveries highlight significant security gaps within the A.I.F.P.U. website, emphasizing the urgent need for enhanced security measures. Recommendations included the implementation of Hyper Text Transfer Protocol Secured (HTTPS) protocol, adoption of Multi-Factor Authentication (MFA), active monitoring of website logs, regular password changes, and hashing passwords before storage. Implementing these recommendations would significantly enhance the security posture of the A.I.F.P.U. website, mitigating potential risks of data breaches and unauthorized access. Furthermore, the study underscores the importance of utilizing tools like Wireshark for assessing data traffic security, thereby fortifying the overall security of web applications.

Keywords: Vulnerabilities, Security, Wireshark, A.I.F.P.U., Data security

Introduction

Ensuring data security is paramount in the realm of data and information communication across networks. With the proliferation of computer networks and the advent of open systems, accessibility to networks has become more convenient (Kim, Lee, & Lim., 2020). However, this accessibility also brings forth vulnerabilities, putting the transmission of data at risk from unauthorized interception or exploitation by malicious entities (Ahmad., 2020). Moreover, the security of software is equally crucial in maintaining data integrity. Software, which facilitates various tasks on computers, can also harbor threats such as malware, including categories like malware (44%), Adware (38%), and Trojans (18%) (Dodiya, & Singh, 2022; Varghese & Muniyal, 2021). These malicious software not only disrupt operations but also pose risks to the security of user data. Furthermore, internet protocols like HTTP, commonly used for accessing websites, are susceptible to exploitation. Despite its convenience, this technology presents security loopholes, often leading to data breaches and unauthorized access to user accounts (Malek & Amran. 2021). The A.I.F.P.U. website serves as a pivotal tool in managing and facilitating the learning process. It provides avenues for access to online real time course registration, fees payments, hostel allocation, results checking, e.t.c. Its flexibility allows users to engage anytime, anywhere, using diverse devices. Given the significance of data security, it is imperative to address potential vulnerabilities within the A.I.F.P.U. platform. Failure to do so may expose sensitive user data, thereby increasing the risk of data breaches and compromising campus data security. Consequently, conducting research on implementing security analysis tools like Wireshark on the A.I.F.P.U. website is crucial. The insights gleaned from such research can inform recommendations to bolster the platform's security measures and mitigate potential risks effectively. Therefore, prioritizing research in this area is paramount to safeguarding user data and maintaining the integrity of the A.I.F.P.U. platform.

Literature Review

A Portal refers to a technical tool designed to oversee and streamline the entirety of the online learning process (Wang, Xu & Yan. 2010). It serves as a software application utilized by educators within educational institutions such as universities, polytechnics, colleges, and high schools as internet-based applications processing platform. By using a portal, Staff and students can perform certain tasks real time from separate locations. The functions provided by a portal to educational institutions are managing user access rights, managing courses, managing activities, managing grades, displaying grades and transcripts and making payments so that it can be accessed using a web browser.

Hypertext Transfer Protocol (HTTP) stands as an application network protocol facilitating the transmission of information between server and client computers. Servers, repositories of diverse information, primarily serve to deliver services to connected clients (Ritinder. 2019). Clients, typically web browsers, access, receive, and display content retrieved from servers. HTTP stands as the predominant protocol on the internet, with abundant resources accessible online (Iqbal. & Naaz. 2019). However, HTTP lacks inherent security measures, posing risks such as data leakage. Implementing Secure Sockets Layer (SSL) certificates can enhance security, albeit potentially affecting accessibility and redirecting HTTP pages.

Sniffing represents a cybercrime tactic wherein perpetrators intentionally or unintentionally intercept others' usernames and passwords (Malek & Amran. 2021). Sniffing involves capturing data packets traversing a computer network, facilitating monitoring and capture of network traffic and potentially exposing confidential information like usernames and passwords. Effective network sniffing aids in optimizing network performance, identifying potential security breaches, and bolstering network security.

Wireshark, a network protocol analyzer, records and displays detailed packet data, primarily employed in network management to ensure functionality and monitor network activities (Ahmad. 2020; Iqbal & Naaz. 2019). Formerly known as Ethereum, Wireshark, developed by Gerald Combs in 1988, is renowned for its ability to capture and analyze packets across both wired and wireless networks. Administrators leverage Wireshark to monitor and analyze network data, benefiting from its capacity to save captured data for subsequent analysis across various network types, including Ethernet, IEEE 802.11, and Point-to-Point Protocol (PPP) (Kim, Lee & Lim. 2020).

Jaya, Dewi & Mahendra (2022) employed Wireshark to analyze a Learning Management System (LMS) website. By capturing network traffic, they identified the use of the unencrypted HTTP protocol, exposing the system to potential vulnerabilities. Their work further highlights Wireshark application's ability to detect the lack of secure protocols essential for protecting sensitive data transmission such as HTTPS.

Methodology

In this study, the authors use data collected by capturing packets using the Wireshark application. The data is accessed from the website of A.I.F.P.U., namely. akanuibiamfedpoly.net, using the HTTP protocol. Figure 1 shows the research flowchart on the implementation of the Wireshark application in data security analysis on the A.I.F.P.U. website carried out at akanuibiamfedpoly.net. The first process that must be done is to activate the Wireshark application by selecting a Wi-Fi network, then we must visit the website address after waiting for Wireshark to retrieve packets through the browser. Turn off or stop packet capture in Wireshark while packets are being fetched to make it easier to analyze the packets.

Filter using HTTP, then search for packages via the posting method and analyze the contents of those packages.

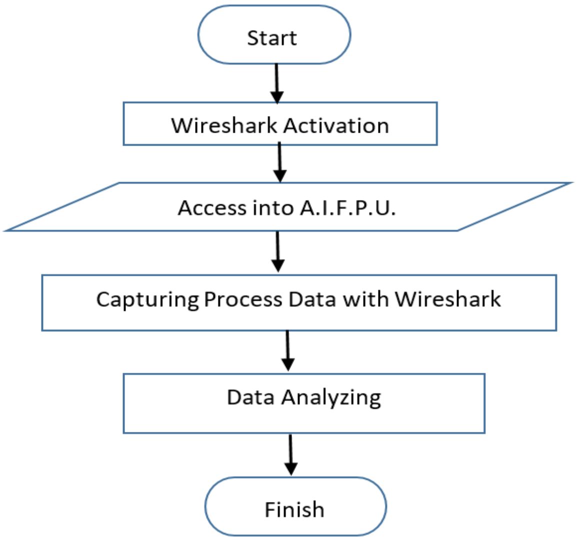
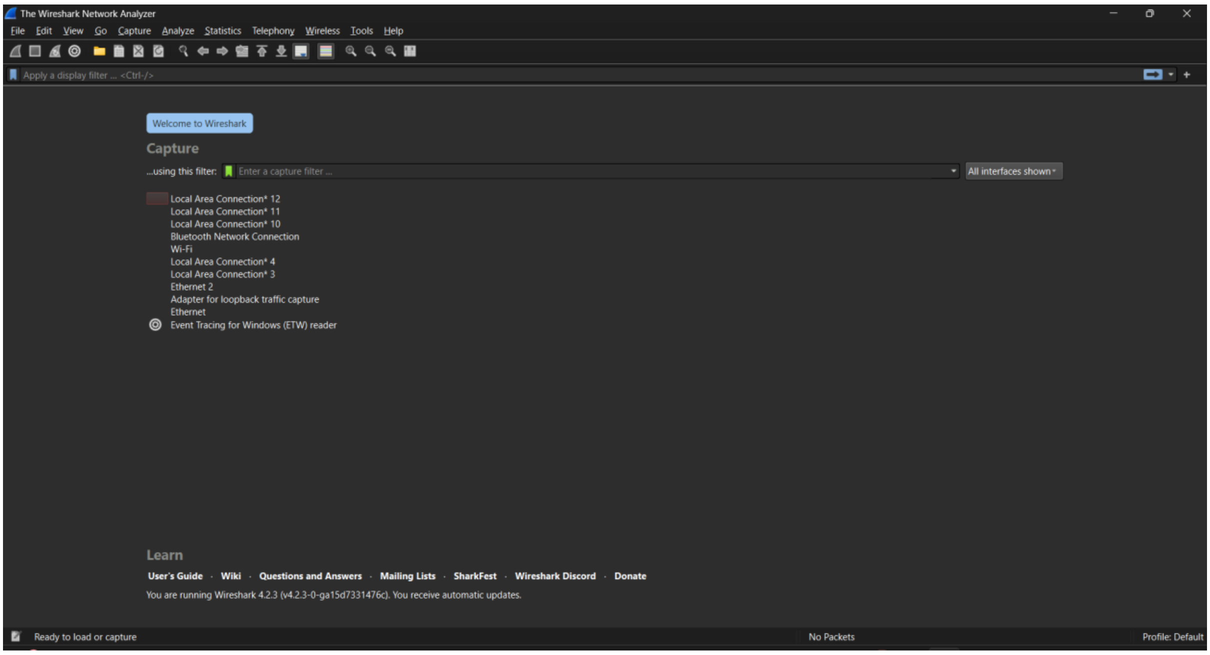


Figure 1: Research flowchart

Result

Implementing the Wireshark application for data security analysis on the A.I.F.P.U. website involves initially examining the website through HTTP and employing Wireshark for packet sniffing to acquire usernames and passwords. The process entails several specific steps. Firstly, the Wireshark application is launched. For this investigation, the authors utilize data obtained by packet capture using Wireshark. The data originates from the A.I.F.P.U. website, accessed via the HTTP protocol. The version of Wireshark employed is 4.2.3 on the Windows platform. Figure 2 below displays the initial interface of Wireshark version 4.2.3 Additionally, Figure 3 depicts the ping process on the A.I.F.P.U. page.

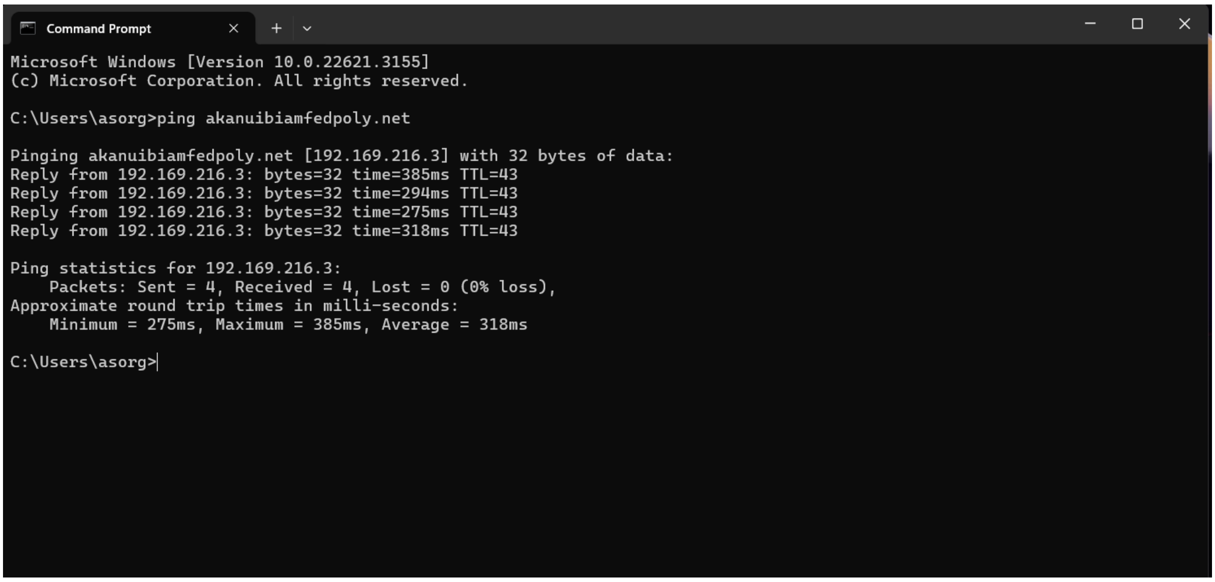

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Learn
User's Guide · Wiki · Questions and Answers · Mailing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

Local Area Connection* 12
Local Area Connection* 11
Local Area Connection* 10
Bluetooth Network Connection
Wi-Fi
Local Area Connection* 4
Local Area Connection* 3
Ethernet 2
Adapter for loopback traffic capture
Ethernet
Event Tracing for Windows (ETW) reader

You are running Wireshark 4.2.3 (v4.2.3-0-ga15d7331476c). You receive automatic updates.

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

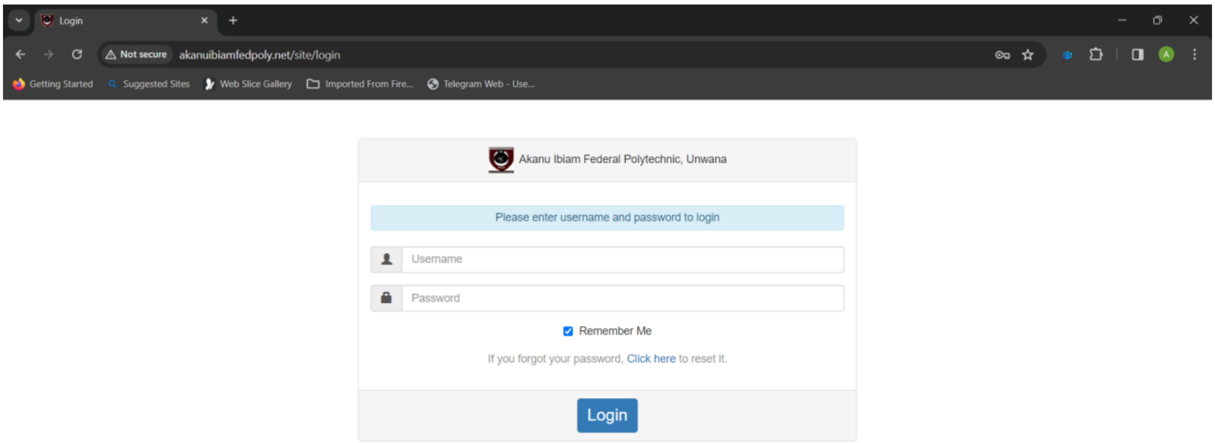
Figure 2: Initial display of Wireshark 4.2.3



```
Microsoft Windows [Version 10.0.22621.3155]
(c) Microsoft Corporation. All rights reserved.

C:\Users\asorg>ping akanuibiamfedpoly.net

Pinging akanuibiamfedpoly.net [192.169.216.3] with 32 bytes of data:
Reply from 192.169.216.3: bytes=32 time=385ms TTL=43
Reply from 192.169.216.3: bytes=32 time=294ms TTL=43
Reply from 192.169.216.3: bytes=32 time=275ms TTL=43
Reply from 192.169.216.3: bytes=32 time=318ms TTL=43

Ping statistics for 192.169.216.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 275ms, Maximum = 385ms, Average = 318ms

C:\Users\asorg>
```

Fig 3. Ping display on akanuibiamfedpoly.net using command prompt

The next step involves specifying the HTTP address, utilizing http://www.akanuibiamfedpoly.net/site/login for the sniffing process aimed at acquiring usernames and passwords. Figure 4 displays the appearance of the Akanu Ibiam Federal Polytechnic Unwana website page, while Figure 5 depicts the "not secure" view, resulting from the website's reliance on the HTTP protocol. This lack of security poses risks when accessing the Akanu Ibiam Federal Polytechnic Unwana website. To gain a comprehensive understanding of the underlying conditions behind the "not secure" status, Wireshark can be employed for sniffing actions on the Akanu Ibiam Federal Polytechnic Unwana website. This allows for a deeper examination of the potential vulnerabilities and insecurities present.

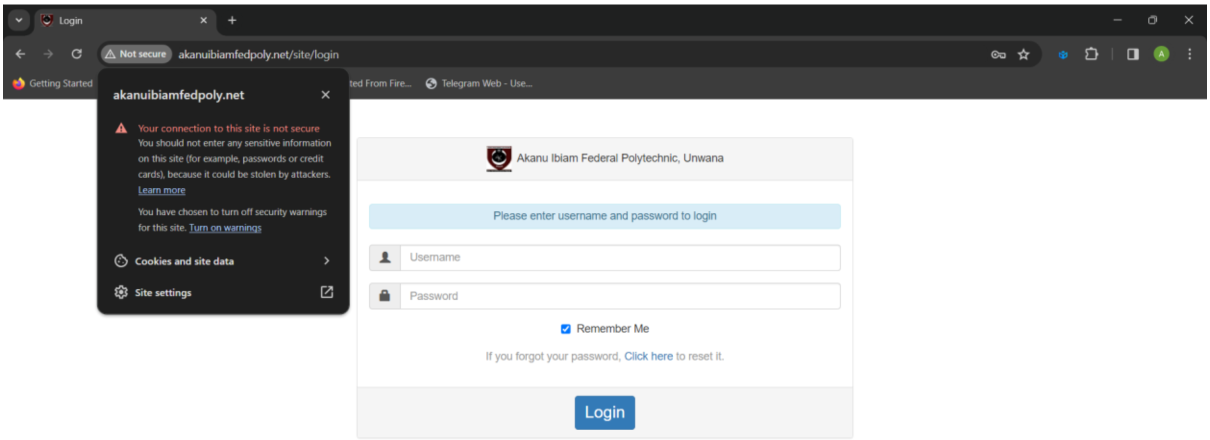


Please enter username and password to login

☑ Remember Me

If you forgot your password, Click here to reset it.

Fig 4. Akanu Ibiam Federal Polytechnic Unwana Website Page Display



Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

You have chosen to turn off security warnings for this site. Turn on warnings

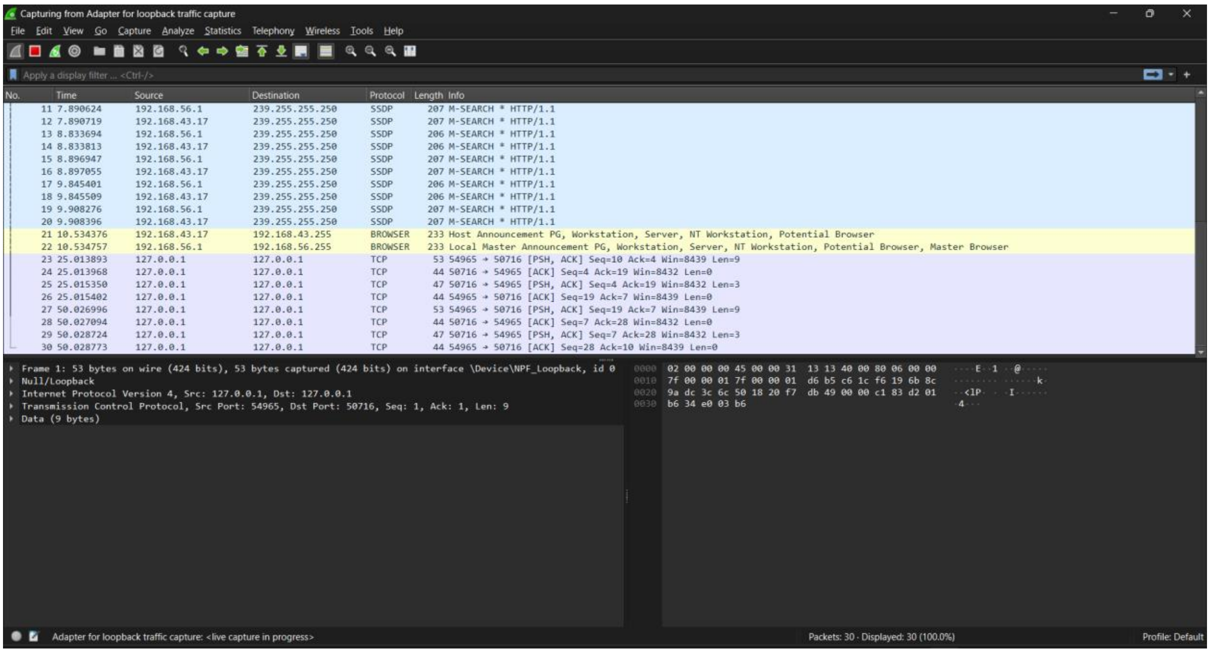
Please enter username and password to login

☑ Remember Me

If you forgot your password, Click here to reset it.

Fig 5. “Not secure” display on Akanu Ibiam Federal Polytechnic Unwana web page

The third step involves utilizing Wireshark to capture data. Upon launching the Wireshark application and configuring akanuibiamfedpoly.net access, it will commence capturing both incoming and outgoing data. The initial view of the data retrieval page (sniffing) in Wireshark is illustrated in Figure 6. Subsequently, Figure 7 displays the presentation of the data retrieval (sniffing) page within the Wireshark application.


Capturing from Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

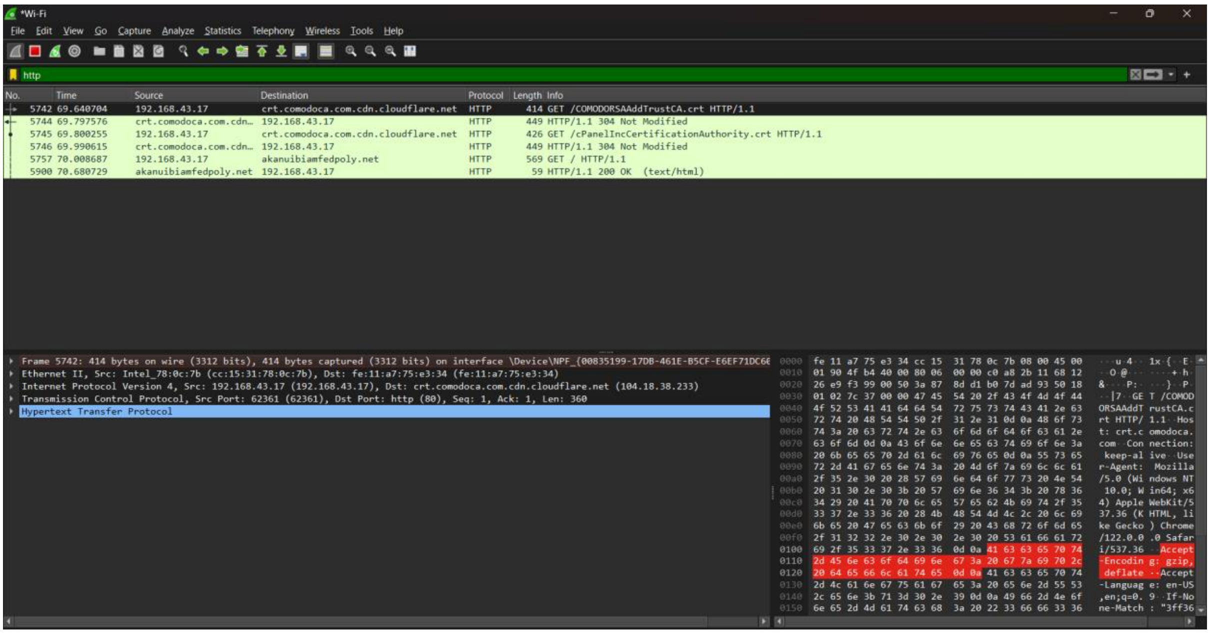
```
No.   Time        Source          Destination      Protocol Length Info
   11 7.890624    192.168.56.1    239.255.255.250  SSDP     207 M-SEARCH * HTTP/1.1
   12 7.890719    192.168.43.17   239.255.255.250  SSDP     207 M-SEARCH * HTTP/1.1
   13 8.833694    192.168.56.1    239.255.255.250  SSDP     206 M-SEARCH * HTTP/1.1
   14 8.833813    192.168.43.17   239.255.255.250  SSDP     206 M-SEARCH * HTTP/1.1
   15 8.896947    192.168.56.1    239.255.255.250  SSDP     207 M-SEARCH * HTTP/1.1
   16 8.897055    192.168.43.17   239.255.255.250  SSDP     207 M-SEARCH * HTTP/1.1
   17 9.845401    192.168.56.1    239.255.255.250  SSDP     206 M-SEARCH * HTTP/1.1
   18 9.845509    192.168.43.17   239.255.255.250  SSDP     206 M-SEARCH * HTTP/1.1
   19 9.908276    192.168.56.1    239.255.255.250  SSDP     207 M-SEARCH * HTTP/1.1
   20 9.908396    192.168.43.17   239.255.255.250  SSDP     207 M-SEARCH * HTTP/1.1
   21 10.534376   192.168.43.17   192.168.43.255   BROWSER  233 Host Announcement PG, Workstation, Server, NT Workstation, Potential Browser
   22 10.534757   192.168.56.1    192.168.56.255   BROWSER  233 Local Master Announcement PG, Workstation, Server, NT Workstation, Potential Browser, Master Browser
   23 25.013893   127.0.0.1       127.0.0.1        TCP       53 54965 → 50716 [PSH, ACK] Seq=10 Ack=4 Win=8439 Len=9
   24 25.013968   127.0.0.1       127.0.0.1        TCP       44 50716 → 54965 [ACK] Seq=4 Ack=19 Win=8432 Len=0
   25 25.015350   127.0.0.1       127.0.0.1        TCP       47 50716 → 54965 [PSH, ACK] Seq=4 Ack=19 Win=8432 Len=3
   26 25.015402   127.0.0.1       127.0.0.1        TCP       44 54965 → 50716 [ACK] Seq=19 Ack=7 Win=8439 Len=0
   27 50.026996   127.0.0.1       127.0.0.1        TCP       53 54965 → 50716 [PSH, ACK] Seq=19 Ack=7 Win=8439 Len=9
   28 50.027094   127.0.0.1       127.0.0.1        TCP       44 50716 → 54965 [ACK] Seq=7 Ack=28 Win=8432 Len=0
   29 50.028724   127.0.0.1       127.0.0.1        TCP       47 50716 → 54965 [PSH, ACK] Seq=7 Ack=28 Win=8432 Len=3
   30 50.028773   127.0.0.1       127.0.0.1        TCP       44 54965 → 50716 [ACK] Seq=28 Ack=10 Win=8439 Len=0
```

```
Frame 1: 53 bytes on wire (424 bits), 53 bytes captured (424 bits) on interface \Device\NPF_Loopback, id 0
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 54965, Dst Port: 50716, Seq: 1, Ack: 1, Len: 9
Data (9 bytes)
```

```
0000  02 00 00 00 45 00 00 31  13 13 40 00 80 06 00 00   ····E··1 ··@·····
0010  7f 00 00 01 7f 00 00 01  d6 b5 c6 1c f6 19 6b 8c   ········ ······k·
0020  9a dc 3c 6c 50 18 20 f7  db 49 00 00 c1 83 d2 01   ··<lP· · ·I······
0030  b6 34 e0 03 b6                                      ·4···
```

```
Adapter for loopback traffic capture: <live capture in progress>    Packets: 30 · Displayed: 30 (100.0%)    Profile: Default
```

Fig 6. Initial View of the Data Capture (Sniffing) Page Using Wireshark


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

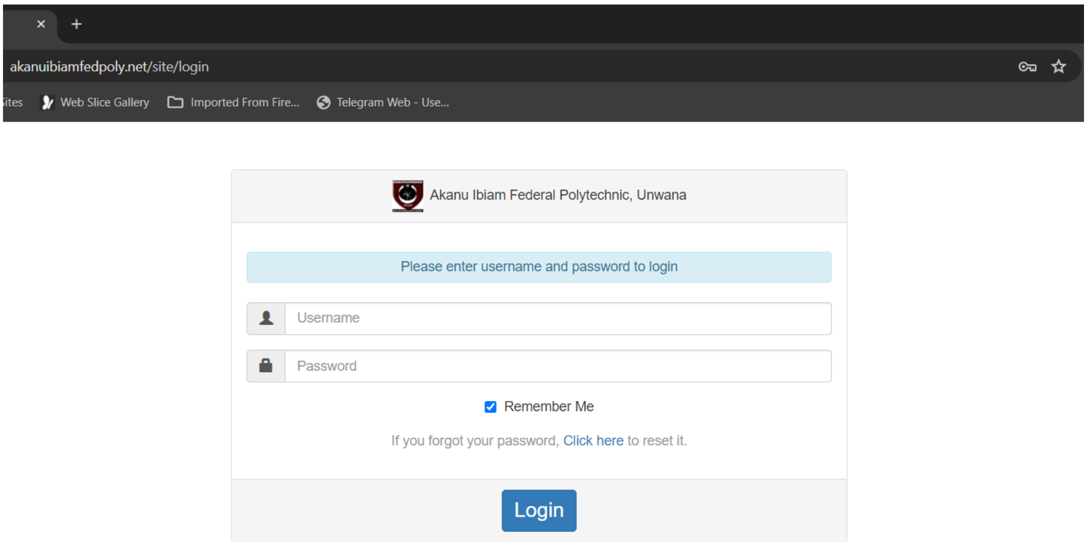
```
No.     Time        Source                  Destination                          Protocol Length Info
   5742 69.640704   192.168.43.17           crt.comodoca.com.cdn.cloudflare.net  HTTP     414 GET /COMODORSAAddTrustCA.crt HTTP/1.1
   5744 69.797576   crt.comodoca.com.cdn…   192.168.43.17                        HTTP     449 HTTP/1.1 304 Not Modified
   5745 69.800255   192.168.43.17           crt.comodoca.com.cdn.cloudflare.net  HTTP     426 GET /cPanelIncCertificationAuthority.crt HTTP/1.1
   5746 69.990615   crt.comodoca.com.cdn…   192.168.43.17                        HTTP     449 HTTP/1.1 304 Not Modified
   5757 70.008687   192.168.43.17           akanuibiamfedpoly.net                HTTP     569 GET / HTTP/1.1
   5900 70.680729   akanuibiamfedpoly.net   192.168.43.17                        HTTP      59 HTTP/1.1 200 OK  (text/html)
```

```
Frame 5742: 414 bytes on wire (3312 bits), 414 bytes captured (3312 bits) on interface \Device\NPF_{00835199-17DB-461E-B5CF-E6EF71DC6E
Ethernet II, Src: Intel_78:0c:7b (cc:15:31:78:0c:7b), Dst: fe:11:a7:75:e3:34 (fe:11:a7:75:e3:34)
Internet Protocol Version 4, Src: 192.168.43.17 (192.168.43.17), Dst: crt.comodoca.com.cdn.cloudflare.net (104.18.38.233)
Transmission Control Protocol, Src Port: 62361 (62361), Dst Port: http (80), Seq: 1, Ack: 1, Len: 360
Hypertext Transfer Protocol
```

```
0000  fe 11 a7 75 e3 34 cc 15  31 78 0c 7b 08 00 45 00   ···u·4·· 1x·{··E·
0010  01 90 4f b4 40 00 80 06  00 00 c0 a8 2b 11 68 12   ··O·@··· ····+·h·
0020  26 e9 f3 99 00 50 3a 87  8d d1 b0 7d ad 93 50 18   &····P:· ···}··P·
0030  01 02 7c 37 00 00 47 45  54 20 2f 43 4f 4d 4f 44   ··|7··GE T /COMOD
0040  4f 52 53 41 41 64 64 54  72 75 73 74 43 41 2e 63   ORSAAddT rustCA.c
0050  72 74 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73   rt HTTP/ 1.1··Hos
0060  74 3a 20 63 72 74 2e 63  6f 6d 6f 64 6f 63 61 2e   t: crt.c omodoca.
0070  63 6f 6d 0d 0a 43 6f 6e  6e 65 63 74 69 6f 6e 3a   com··Con nection:
0080  20 6b 65 65 70 2d 61 6c  69 76 65 0d 0a 55 73 65    keep-al ive··Use
0090  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
00a0  2f 35 2e 30 20 28 57 69  6e 64 6f 77 73 20 4e 54   /5.0 (Wi ndows NT
00b0  20 31 30 2e 30 3b 20 57  69 6e 36 34 3b 20 78 36    10.0; W in64; x6
00c0  34 29 20 41 70 70 6c 65  57 65 62 4b 69 74 2f 35   4) Apple WebKit/5
00d0  33 37 2e 33 36 20 28 4b  48 54 4d 4c 2c 20 6c 69   37.36 (K HTML, li
00e0  6b 65 20 47 65 63 6b 6f  29 20 43 68 72 6f 6d 65   ke Gecko ) Chrome
00f0  2f 31 32 32 2e 30 2e 30  2e 30 20 53 61 66 61 72   /122.0.0 .0 Safar
0100  69 2f 35 33 37 2e 33 36  0d 0a 41 63 63 65 70 74   i/537.36 ··Accept
0110  2d 45 6e 63 6f 64 69 6e  67 3a 20 67 7a 69 70 2c   -Encodin g: gzip,
0120  20 64 65 66 6c 61 74 65  0d 0a 41 63 63 65 70 74    deflate ··Accept
0130  2d 4c 61 6e 67 75 61 67  65 3a 20 65 6e 2d 55 53   -Languag e: en-US
0140  2c 65 6e 3b 71 3d 30 2e  39 0d 0a 49 66 2d 4e 6f   ,en;q=0. 9··If-No
0150  6e 65 2d 4d 61 74 63 68  3a 20 22 33 66 66 33 36   ne-Match : "3ff36
```

Fig 7. Process Display of the Capture Data (Sniffing) Page Using Wireshark

The fourth step involves testing. Once the Wireshark application has been used for the sniffing process, the researchers proceeded to access the akanuibiamfedpoly.net website. Entered the username and password on the designated fields provided. Figure 8 illustrates the appearance of the username and password page on the akanuibiamfedpoly.net website. Upon successful login, Figure 9 depicts the dashboard page display.



akanuibiamfedpoly.net/site/login

Akanu Ibiam Federal Polytechnic, Unwana

Please enter username and password to login

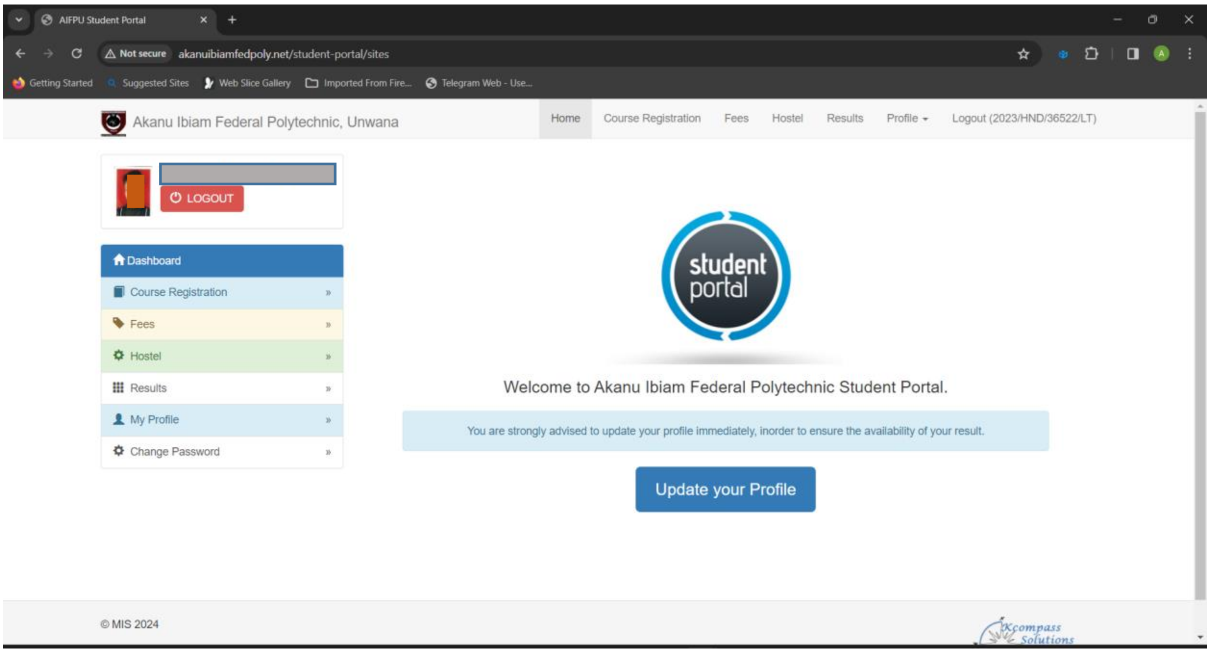
Username

Password

☑ Remember Me

If you forgot your password, Click here to reset it.

Fig 8. Username and Password Page Display on Akanu Ibiam Federal Polytechnic Unwana web page



akanuibiamfedpoly.net/student-portal/sites

Akanu Ibiam Federal Polytechnic, Unwana

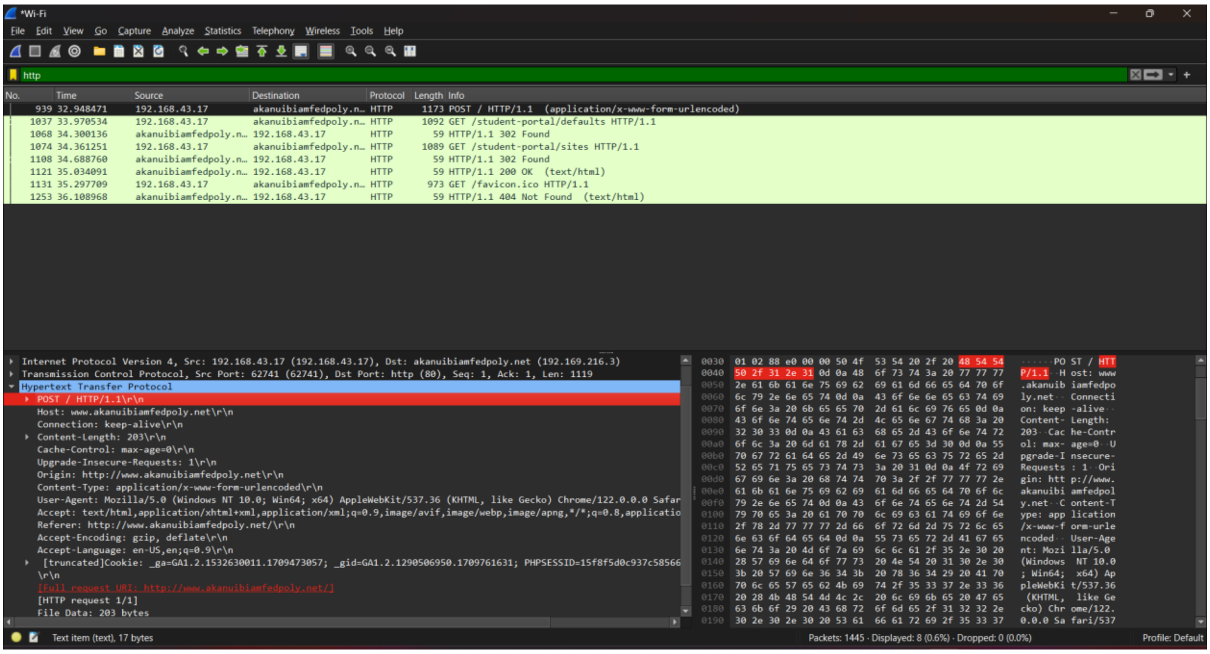
[redacted]

Welcome to Akanu Ibiam Federal Polytechnic Student Portal.

You are strongly advised to update your profile immediately, inorder to ensure the availability of your result.

Fig 9. Dashboard Page Display When Successfully Logged into akanuibiamfedpoly.net

The fifth step involves stopping the data collection process. To do this, the researchers navigated back to the Wireshark application and terminated the ongoing capture by selecting "stop capture". Next, inputted the HTTP command in the filter and choose "POST" from the info section. Once the data collection was finished, the researchers proceeded to search for relevant information. Within the POST data, details such as the source IP address (192.168.43.17) and destination IP address (192.169.213.3) were found. Additionally, various information are present within the HTTP data. To locate the previously entered username and password, focus on the HTML form. The analysis of POST packet during the login process is illustrated in Figure 10.


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

```
http
No.   Time       Source              Destination         Protocol Length Info
  939 32.948471  192.168.43.17       akanuibiamfedpoly.n… HTTP    1173 POST / HTTP/1.1  (application/x-www-form-urlencoded)
 1037 33.970534  192.168.43.17       akanuibiamfedpoly.n… HTTP    1092 GET /student-portal/defaults HTTP/1.1
 1068 34.300136  akanuibiamfedpoly.n… 192.168.43.17      HTTP      59 HTTP/1.1 302 Found
 1074 34.361251  192.168.43.17       akanuibiamfedpoly.n… HTTP    1089 GET /student-portal/sites HTTP/1.1
 1108 34.688760  akanuibiamfedpoly.n… 192.168.43.17      HTTP      59 HTTP/1.1 302 Found
 1121 35.034091  akanuibiamfedpoly.n… 192.168.43.17      HTTP      59 HTTP/1.1 200 OK  (text/html)
 1131 35.297709  192.168.43.17       akanuibiamfedpoly.n… HTTP     973 GET /favicon.ico HTTP/1.1
 1253 36.108968  akanuibiamfedpoly.n… 192.168.43.17      HTTP      59 HTTP/1.1 404 Not Found  (text/html)
```

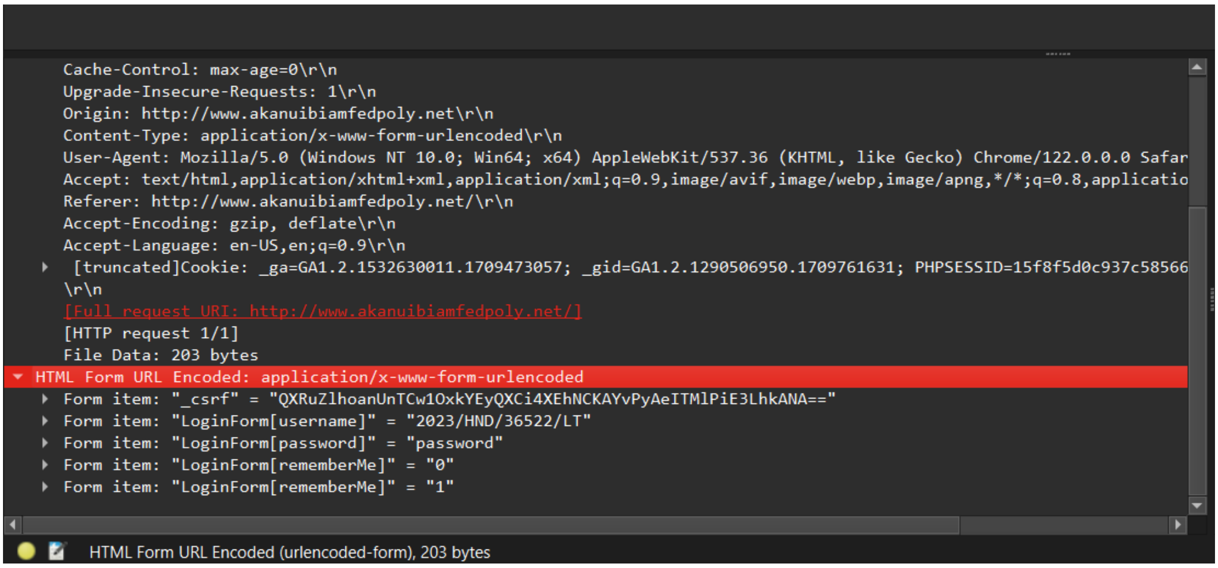
```
▸ Internet Protocol Version 4, Src: 192.168.43.17 (192.168.43.17), Dst: akanuibiamfedpoly.net (192.169.216.3)
▸ Transmission Control Protocol, Src Port: 62741 (62741), Dst Port: http (80), Seq: 1, Ack: 1, Len: 1119
▾ Hypertext Transfer Protocol
  ▸ POST / HTTP/1.1\r\n
    Host: www.akanuibiamfedpoly.net\r\n
    Connection: keep-alive\r\n
  ▸ Content-Length: 203\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Origin: http://www.akanuibiamfedpoly.net\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safar
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicatio
    Referer: http://www.akanuibiamfedpoly.net/\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
  ▸  [truncated]Cookie: _ga=GA1.2.1532630011.1709473057; _gid=GA1.2.1290506950.1709761631; PHPSESSID=15f8f5d0c937c58566
    \r\n
    [Full request URI: http://www.akanuibiamfedpoly.net/]
    [HTTP request 1/1]
    File Data: 203 bytes
```

```
0030  01 02 88 e0 00 00 50 4f  53 54 20 2f 20 48 54 54   ······PO ST / HTT
0040  50 2f 31 2e 31 0d 0a 48  6f 73 74 3a 20 77 77 77   P/1.1··H ost: www
0050  2e 61 6b 61 6e 75 69 62  69 61 6d 66 65 64 70 6f   .akanuib iamfedpo
0060  6c 79 2e 6e 65 74 0d 0a  43 6f 6e 6e 65 63 74 69   ly.net·· Connecti
0070  6f 6e 3a 20 6b 65 65 70  2d 61 6c 69 76 65 0d 0a   on: keep -alive··
0080  43 6f 6e 74 65 6e 74 2d  4c 65 6e 67 74 68 3a 20   Content- Length: 
0090  32 30 33 0d 0a 43 61 63  68 65 2d 43 6f 6e 74 72   203··Cac he-Contr
00a0  6f 6c 3a 20 6d 61 78 2d  61 67 65 3d 30 0d 0a 55   ol: max- age=0··U
00b0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-
00c0  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 4f 72 69   Requests : 1··Ori
00d0  67 69 6e 3a 20 68 74 74  70 3a 2f 2f 77 77 77 2e   gin: htt p://www.
00e0  61 6b 61 6e 75 69 62 69  61 6d 66 65 64 70 6f 6c   akanuibi amfedpol
00f0  79 2e 6e 65 74 0d 0a 43  6f 6e 74 65 6e 74 2d 54   y.net··C ontent-T
0100  79 70 65 3a 20 61 70 70  6c 69 63 61 74 69 6f 6e   ype: app lication
0110  2f 78 2d 77 77 77 2d 66  6f 72 6d 2d 75 72 6c 65   /x-www-f orm-urle
0120  6e 63 6f 64 65 64 0d 0a  55 73 65 72 2d 41 67 65   ncoded·· User-Age
0130  6e 74 3a 20 4d 6f 7a 69  6c 6c 61 2f 35 2e 30 20   nt: Mozi lla/5.0 
0140  28 57 69 6e 64 6f 77 73  20 4e 54 20 31 30 2e 30   (Windows  NT 10.0
0150  3b 20 57 69 6e 36 34 3b  20 78 36 34 29 20 41 70   ; Win64;  x64) Ap
0160  70 6c 65 57 65 62 4b 69  74 2f 35 33 37 2e 33 36   pleWebKi t/537.36
0170  20 28 4b 48 54 4d 4c 2c  20 6c 69 6b 65 20 47 65    (KHTML,  like Ge
0180  63 6b 6f 29 20 43 68 72  6f 6d 65 2f 31 32 32 2e   cko) Chr ome/122.
0190  30 2e 30 2e 30 20 53 61  66 61 72 69 2f 35 33 37   0.0.0 Sa fari/537
```

```
Text item (text), 17 bytes    Packets: 1445 · Displayed: 8 (0.6%) · Dropped: 0 (0.0%)    Profile: Default
```

Fig 10. Analysis of Login POST Packages

The final phase involves examining the outcomes. The utilization of the Wireshark application for sniffing usernames and passwords has proven effective. By scrutinizing the captured data within the designated network, it's possible to discern the username and password within the POST data packet. The encryption-protected HTML page exhibiting the retrieved username and password is illustrated in Figure 11.



```
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Origin: http://www.akanuibiamfedpoly.net\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safar
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicatio
    Referer: http://www.akanuibiamfedpoly.net/\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9\r\n
  ▸  [truncated]Cookie: _ga=GA1.2.1532630011.1709473057; _gid=GA1.2.1290506950.1709761631; PHPSESSID=15f8f5d0c937c58566
    \r\n
    [Full request URI: http://www.akanuibiamfedpoly.net/]
    [HTTP request 1/1]
    File Data: 203 bytes
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "_csrf" = "QXRuZlhoanUnTCw1OxkYEyQXCi4XEhNCKAYvPyAeITMlPiE3LhkANA=="
  ▸ Form item: "LoginForm[username]" = "2023/HND/36522/LT"
  ▸ Form item: "LoginForm[password]" = "password"
  ▸ Form item: "LoginForm[rememberMe]" = "0"
  ▸ Form item: "LoginForm[rememberMe]" = "1"
```

```
HTML Form URL Encoded (urlencoded-form), 203 bytes
```

Fig 11. HTML Page Display Showing Username and Password Visible Without Encryption.

Conclusion and Recommendations

The findings reveal that the Wireshark application is effective in identifying vulnerabilities within the akanuibiamfedpoly.net infrastructure owned by Akanu Ibiam Federal Polytechnic Unwana, Afikpo, Ebonyi State of Nigeria. Analysis conducted through Wireshark on akanuibiamfedpoly.net, utilizing the HTTP protocol, clearly exposes the absence of encryption, posing a significant risk to user data security. To mitigate these vulnerabilities and enhance the protection of sensitive information within the Akanu Ibiam Federal Polytechnic Unwana web portal, several recommendations are proposed:

1. Implementation of the Hypertext Transfer Protocol Secure (HTTPS) protocol: This would bolster communication security by encrypting data transmitted between users and web servers, thus safeguarding against potential leaks of confidential information like usernames and passwords.

2. Adoption of Multi-Factor Authentication (MFA): Integrating MFA into the login process adds an extra layer of security, making unauthorized access to devices, networks, databases, or sensitive data more challenging for malicious actors.

3. Active monitoring of website logs: By continuously monitoring and analyzing various logs, including database logs, web server logs, firewall logs, and intrusion prevention system (IPS)/intrusion detection system (IDS) logs, anomalies in system access can be promptly identified and addressed.

4. Regular password changes: Enforcing periodic password updates helps maintain data security by reducing the risk of unauthorized access. Additionally, implementing standardized password requirements, such as a minimum length of 12 characters and inclusion of uppercase letters, lowercase letters, numbers, and special characters, ensures passwords offer adequate protection against potential breaches.

5. Hashing passwords before storage: By hashing passwords before storing them in the database, sensitive information remains secure even in the event of a database breach, as the original passwords are not easily decipherable.

Implementing these recommendations would significantly enhance the security posture of the Akanu Ibiam Federal Polytechnic Unwana web portal, safeguarding against potential data breaches and unauthorized access. Furthermore, it is advisable for website developers to utilize Wireshark to assess data traffic security, thereby fortifying the application's overall security deportment.

References

Ahmad, M. (2020). Forensic Analysis of Peer-to-Peer Network Traffic with Wireshark. Sule Lamido University Journal of Science and Technology, 1(2), pp. 92-99

Dodiya, B., & Singh, U. (2022). Malicious Traffic analysis using Wireshark by collection of Indicators of Compromise. International Journal of Computer Applications. 183(53) 975-8887

Iqbal, H., & Naaz, S. (2019). Wireshark as a Tool for Detection of Various LAN Attacks. *International Journal of Computer Sciences and Engineering*, *7*(5), 833–837

Jaya, K. N. A., Dewi, I. A. U., & Mahendra, G. S. (2022). Implementation of Wireshark Application in Data Security Analysis on LMS Website. *Journal of Computer Networks, Architecture and High Performance Computing,* 4(1), 79-86

Kim, H., Lee, H., & Lim, H. (2020). Performance of Packet Analysis between Observer and WireShark, International Conference on Advanced Communication Technology (ICACT), Phoenix Park, Korea (South), 2020, pp. 268-271

Malek, M. S. A., & Amran, A. R. (2021). A Study of Packet Sniffing as an Imperative Security Solution in Cybersecurity. *Journal of Engineering Technology*, 9(1), pp. 96–101

Ritinder, K. (2019). Investigating Network Traffic using Packet Sniffing Tool-Wireshark. *Journal of Emerging Technologies and Innovative Research*, 6(1), pp. 181-186

Varghese, J.E., & Muniyal, B. (2021). A Pilot Study in Software-Defined Networking Using Wireshark for Analyzing Network Parameters to Detect DDoS Attacks. In: Kaiser, M.S., Xie, J., Rathore, V.S. (eds) Information and Communication Technology for Competitive Strategies (ICTCS 2020). Lecture Notes in Networks and Systems, Vol 190. Springer, Singapore

Wang, S., Xu, D., & Yan, S. (2010). Analysis and application of Wireshark in TCP/IP protocol teaching. In International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT) Shenzhen, pp. 269-272