International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 10, Issue 1 (2024)
https://doi.org/10.31436/ijpcc.v10i1.461

Examining Potential Threats of Eavesdropping in TCP Stream of Personal Interactive Transmission Session

Adamu Abubakar*, Nadhirah Muhammed Najmuddin, Rabiatul Adawiyah Mohd Alwi, Nur Amirotul Izzah Mohamad Faizal,

Department of Computer Science, KICT, International Islamic University Malaysia.

*Corresponding author: adamu@iium.edu.my
(Received: 12th May 2023; Accepted: 23th December 2023; Published on-line: 28th January 2024)

Abstract— This study establishes that Personal Interactive Transmission Sessions conducted using TCP streams provide exceptional convenience and immediacy. However, they also provide noteworthy challenges and considerations, especially in terms of security, integrity, and performance. This study investigates the security weaknesses present in potential eavesdropping threats on TCP Streams during personal interactive transmission sessions. An experimental analysis was carried out, by doing a comprehensive analysis of network traffic using Wireshark. The investigation reveals a notable vulnerability in the management of user-provided data, together with the possible risks of eavesdropping, emphasizing the urgent need for enhanced security measures. The findings underscore the need of proactive cybersecurity strategies, such as frequent security audits, vulnerability assessments, and the implementation of robust encryption methods, to safeguard user privacy and ensure data integrity. To enhance risk mitigation, data protection, and user confidence in the digital environment, organizations should prioritize addressing potential eavesdropping threats during transmission sessions that involve sensitive personal data.

Keywords— Personal Interactive Transmission Session, Eavesdropping, TCP Stream, Security threats

I. INTRODUCTION

Personal Interactive Transmission refers to the process of exchanging information between individuals in a direct and interactive manner [1]. A session is the act of visiting customised online pages and engaging with them throughout a web session. This can be accomplished through several approaches, including the use of session-specific IDs, shared storage, and databases offered by server systems on the network site [2]. The objective is to deliver a tailored and effective user experience by gathering user interaction data and use it to individualise the communication and engagement with the user. This include the process of directing telephone calls, exchanging pleasantries, presenting product or service options, and several other modes of communication. Behaviour monitoring and matching engines can optimise the interactive experience by adapting the communication session in real-time according to the user's behaviour and

A TCP stream in networking represents the continuous and organised flow of data between two devices via a TCP connection. The term "TCP stream of Personal Interactive Transmission Session" refers to the flow of data sent via the Transmission Control Protocol (TCP) during a personalised and interactive communication session. Hyper Text Transmission Protocol (HTTP) transmission can be used for personal interactive transmission sessions. The method involves sending requests and receiving responses through the HTTP protocol [3]. Within the framework of a "Personal Interactive Transmission Session," we are referring to a kind of communication that is customised for individual users, wherein information is sent in a dynamic and real-time manner [4]. During these sessions, examining the TCP stream entails analysing the attributes, security implications, and performance factors of the data being communicated [5]. The objective is to ensure a reliable and protected interactive encounter, taking into account aspects such as the integrity of data, the delay in transmission, and the general efficiency of managing personalised communication via a TCP connection [6].

Engaging in Personal Interactive Transmission Sessions via TCP streams may introduce difficulties concerning the security of transmitting personal data, the integrity of communication, and possible limitations in performance [7]. The Common Weakness Enumeration (CWE) 319: "Cleartext Transmission of Sensitive Information" Web Application Vulnerabilities Index focuses on the possible risk of personal or confidential data being transmitted without encryption, which could result in the data being exposed in cleartext or plaintext and susceptible to eavesdropping by unauthorised

individuals [8]. The index also revealed that even if the information is encoded in a manner that is not easily readable by humans, specific procedures can be employed to decode any data that is safeguarded inside the material. Therefore, the team has discovered the capacity to identify the encoding technique and subsequently decipher the information.

The specific challenge in analysing TCP streams in a Personal Interactive Transmission Session lies in achieving a harmonious equilibrium between the need for surveillance and the safeguarding of privacy and security. The main focus involves overseeing the ethical, legal, and technical aspects to ensure a responsible examination of communication data. This includes dealing with matters such as encryption, acquiring user consent, and the potential for unintentional privacy violations. Concurrently, it necessitates an attentive strategy towards potential future risks and the advancement of communication technologies.

The research challenge emphasised, about the meticulous analysis of TCP streams within personal interactive transmission sessions. While, CWE 319 focuses on the specific vulnerability of transferring personal or confidential data without encryption, which leaves it vulnerable to being disclosed in a readable form, sometimes referred to as cleartext or plaintext, that still does not mean it cannot be eavesdropped. This vulnerability allows unauthorised individuals to intercept the conversation. Similarly, despite information being encoded in a manner that is not readily legible to humans, there are specific techniques available that could enable unauthorised individuals to decipher the safeguarded data. Given these vulnerabilities, this research examines the importance of implementing comprehensive solutions, such as encryption mechanisms, to address the potential risk of sensitive data being exposed during Personal Interactive Transmission Sessions. This is consistent with the overarching goal of enhancing security and privacy in communication protocols.

In addition, the paper is structured as follows, with the exception of this section that provides a thorough overview of the research: A thorough description of the relevant studies and research is provided in Section 2. Section 3 describes the methodology used for the study. A comprehensive analysis and presentation of the results are provided in Section 4. The conclusions and results of the study are detailed in Section 5.

II. RELATED WORK

Threats to eavesdropping that are present in the Transmission Control Protocol (TCP) stream of personal interactive transmission sessions have been recognised and investigated in a number of studies. An anti-eavesdropping proportional fairness (APF) method is proposed in one academic work [9]. This mechanism takes into account the likelihood of eavesdroppers and imposes fines in order to minimise the amount of time they are scheduled to listen in. The various steganographic approaches that can be applied to TCP and that constitute a danger to network security are described in another paper [10]. Additionally, there is a study that examines security vulnerabilities to TCP and suggests solutions to mitigate these threats by utilising approaches from the TCP Specification Errata and Issues memo [11]. This article is available for download here. The necessity of tackling eavesdropping concerns in TCP is brought to light in these publications, which also offer insights into potential remedies and advances to security.

In the study of, Nafea et al. [12] it was revealed that an innovative architecture that incorporates features such as ongoing data monitoring, maintenance of thresholds, and reporting of alerts. The work presents a statistical methodology designed to identify hidden data leaks, with a particular focus on non-linear chaotic data. The algorithm's correctness was evaluated on a legitimate data stream, and it was determined that it had no occurrences of Type I and Type II mistakes when processing authentic ISNs. The dataset in the phase space was constructed using equations 2 and 7. The number of vectors in the dataset was determined according to the setup of the testbed. The threshold value utilised for discovering hidden data may vary depending on the hardware metrics accessible during calculation.

The research introduced a methodology for identifying hidden data leaks in TCP data streams, which demonstrated a low rate of false positives and surpassed several other methods in terms of both accuracy and performance. The statistical approach successfully identified hidden data leaks, particularly in complex, non-linear chaotic data, using significantly more efficient tolerance/threshold values.

The suggested method for preserving data transmission integrity in the TCP communication process entails integrating the key exchange into TCP headers to reduce transmission delay and guarantee safe message transport [13].

One of the protocols that is utilised for the transmission of personal and interactive data is known as Hypertext Transfer Protocol (HTTP). In the context of web browsing, the term "session" refers to a method that involves having individualised services and engaging in interactive sessions [14]. On the other hand, these sessions can be established between a secure element that is connected to a mobile device and an HTTP-OTA platform that is situated within a mobile network [15]. The procedure involves sending alerts from the platform to the mobile device, which then triggers the transmission of pre-determined events or commands from the mobile device to the secure element. If the alerts

https://doi.org/10.31436/ijpcc.v10i1.461

are successful, the process will be considered complete. This, in turn, causes an HTTP-OTA session to be initiated between the platform and the secure element [16]. In addition, the architecture that has been proposed has the objective of making it easier for personal services and web service providers to communicate among themselves. The personal services in question are referred to as "vanilla" HTTP services, and they are accessed using a browser. Service providers discover these services through the utilisation of a special agent known as a Broker [17]. This design uses an HTTP proxy in order to simplify the communication with individual services, such as personal authentication through the use of an electronic identification card [18].

The previous research studies reviewed emphasise the significance of dealing with privacy concerns in TCP streams of personal interactive transmission sessions. The insights provided include prospective solutions like as novel architectures, statistical methods for detecting leaks, and improvements to protocols. The combined efforts of these contributions are focused on improving network security, maintaining the integrity of data, and enabling smooth communication between users and service providers.

III. RESEARCH METHODOLOGY

The experimental methodology that is utilised in this study is centred on the establishment of transmission sessions. During these sessions, the complete set of session parameters is thoroughly recorded. Within the context of these transmission sessions, the ultimate goal is to conduct a thorough investigation of the possibility of eavesdropping. The experiment conducted at the Gombak Campus of the International Islamic University Malaysia (IIUM) aimed to examine the interaction between clients making requests for web page access and a remote server. The experiment involved clients situated at the Gombak Campus who launched requests to access web pages hosted on a server located at a different location.

A. Experimental Scenarios

The main objective of this experiment was to examine and comprehend the dynamics of this interaction process. This entails analysing different facets, such as investigating the communication protocols and techniques utilised in the transmission of HTTP requests and responses between clients and the remote server. This entails examining the arrangement and substance of the requests transmitted by clients and the matching responses returned from the server. This also entails confirming whether clients can effectively retrieve and exhibit the desired web pages without any mistakes or delays.

Initially, network access is established from the access point that is situated within the campus of IIUM Gombak. This access point may be identified by the Internet Protocol address 10.121.128.2.0 (See Figure 1). Each time the browser is opened on the research computer, a request is transmitted. This request is then transmitted through the router of the local area network, which is most likely located within the same building.

.

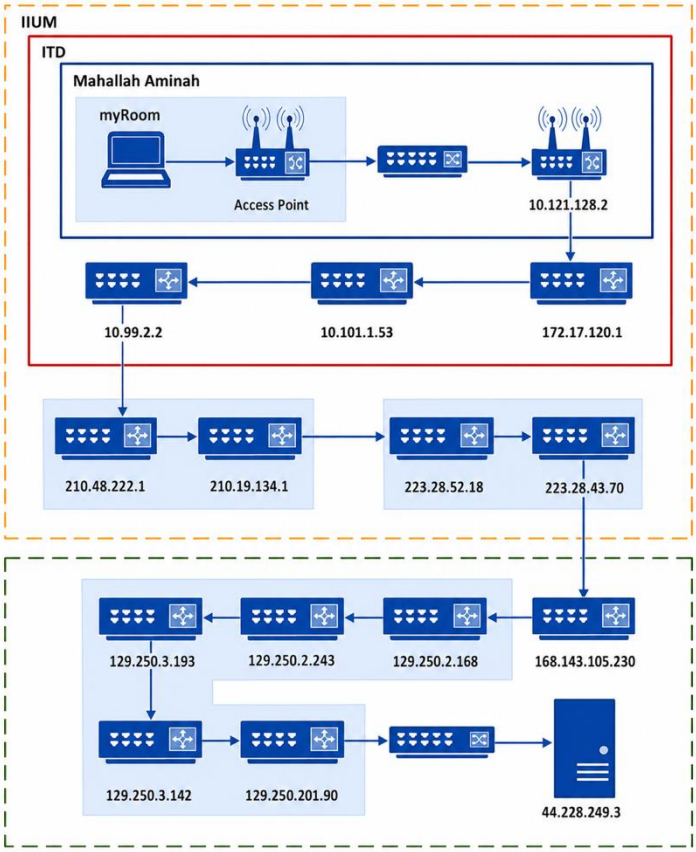

Fig. 1 The Personal Interactive Transmission Sessions

The next step is for the packets to travel through the local router, which can be identified by its IP address of 10.01.1.53, before being sent to an external or public router that has the IP address of 10.99.2.2. As can be seen in Figure 1, this process is carried out continuously through successive routers.

In comparison to the durations of succeeding hops, the time period beginning with hop 1 and ending with hop 11 is significantly shorter. For every increase in the number of hops, there is a corresponding rise in the amount of time it takes to respond. In addition to the distance that the packet must travel, this delay can be attributed to the processing pauses that are present at each router. The result is that the amount of time required to travel from hop 13 to hop 29 gradually increases.

The hops 9, 12, and from 18 to 23 are particularly noteworthy because they reflect situations in which

https://doi.org/10.31436/ijpcc.v10i1.461

particular routers were unable to receive packets within the allotted amount of time. Packets continue to be sent, successfully traversing the network until they reach following routers and ultimately arriving at their intended final destination. This occurs despite the fact that these delays continue to occur. Finally, once the server with the stated IP 44.228.249.3 is reached, the data is retrieved from the server and then transmitted back to the source.

B. Experimental Procedure

A personal interactive session between the client and the server, during which the client's personal data will be utilised, is initiated by the client in order to embark on the experiment. At this point, the information that pertains to "Personal Interaction" has been conveyed through the process of posting and giving a response. The research launched Wireshark and selected the Wi-Fi option to capture network traffic. Upon selecting the Wi-Fi interface, the research clicked on the "shark-fin" icon located in the top-left corner of the Wireshark interface to commence the packet capture process. Subsequently, launched another web browser and navigated to the URL, proceeded to click on the "signup" option located in the side panel of the homepage. Upon accessing the signup page, a login form pre-filled with default credentials, where the username was set to "test" and the password to "test". The research also inputted other personal information details accordingly and proceeded. This action redirected the research to a subsequent page prompting for additional information such as name, credit card number, email, phone number, and address. Once again, the research provided the requested information and clicked the update button to proceed.

Following the completion of these interactions on the website, the research returned to the Wireshark window and clicked on the stop button to halt the packet capture process, capturing all relevant transmission data. This comprehensive approach allowed for the thorough examination of network traffic generated during the session, providing insights into the communication patterns, data exchanges, and potential vulnerabilities within the network.

IV. PRESENTATION OF EXPERIMENTAL RESULT AND DISCUSSION

Following the completion of the Wireshark network traffic collection phase, the analysis phase begins with the application of filters to refine the data that was obtained. In this particular instance, I utilised a filter by entering the commands "tcp.port == 80 || udp.port == 80" into the Filter box located at the very top of the Wireshark control panel. This filter is designed to particularly target traffic on port 80, which is typically linked with communication using the Hypertext Transfer Protocol (HTTP).

It is just the packets that are pertinent to HTTP communication that are displayed by Wireshark once the filter has been applied (see Figure 2). In HTTP transactions, this filtering makes it possible to conduct a targeted study of the connections that exist between clients and servers. Following the completion of session establishment, the research then proceeded to investigate the HTTP traffic that was associated with the server. The findings of the research were seen in the filtered results.

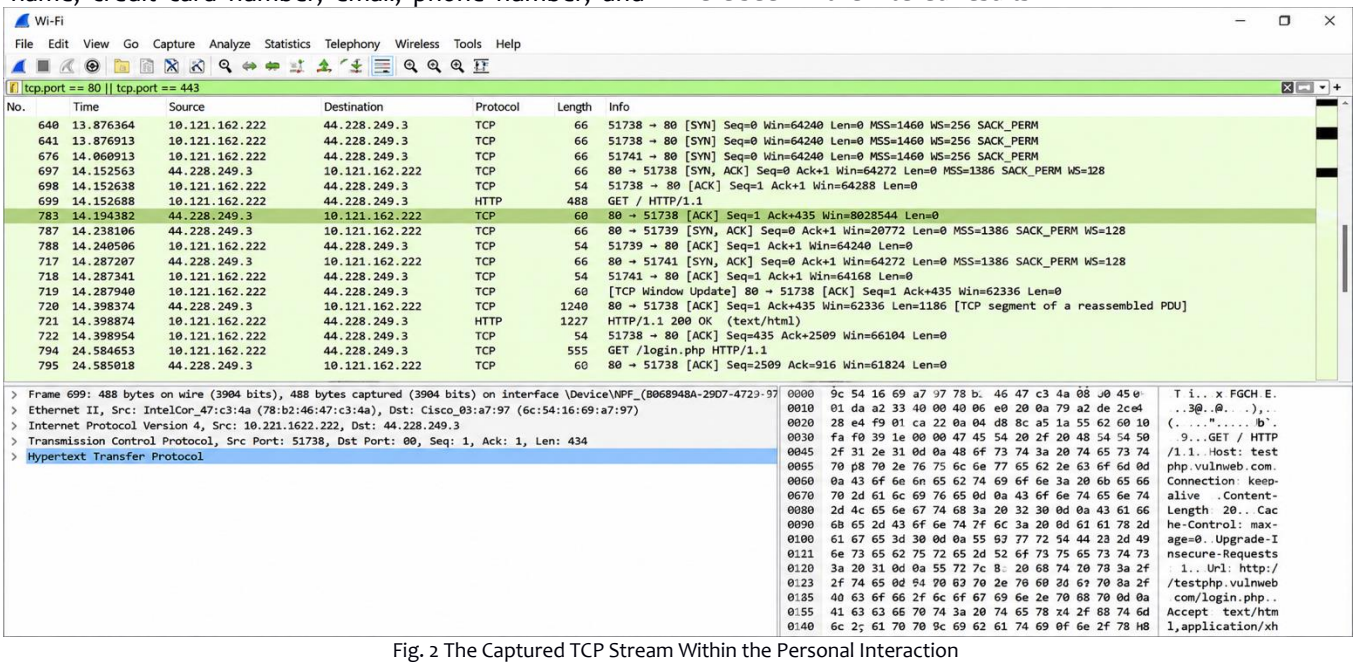

Fig. 2 The Captured TCP Stream Within the Personal Interaction

https://doi.org/10.31436/ijpcc.v10i1.461

The research was able to determine the connection to the HTTP server and obtain more insights into the nature of the communication that takes place between the client and the server by analysing the contents of the packets (see Figure 3). This analysis not only gives useful information about the behaviour of the network, but it also makes it easier to gain a deeper understanding of the mechanisms that regulate HTTP communication. Packet 794 of the intercepted network data contains a request to view a particular web page located at testphp.vulnweb.com/login.php. This request signifies the commencement of a transaction to retrieve the login page from the designated server. Consequently, the login page is displayed in the browser window, verifying the successful retrieval of the requested online material.

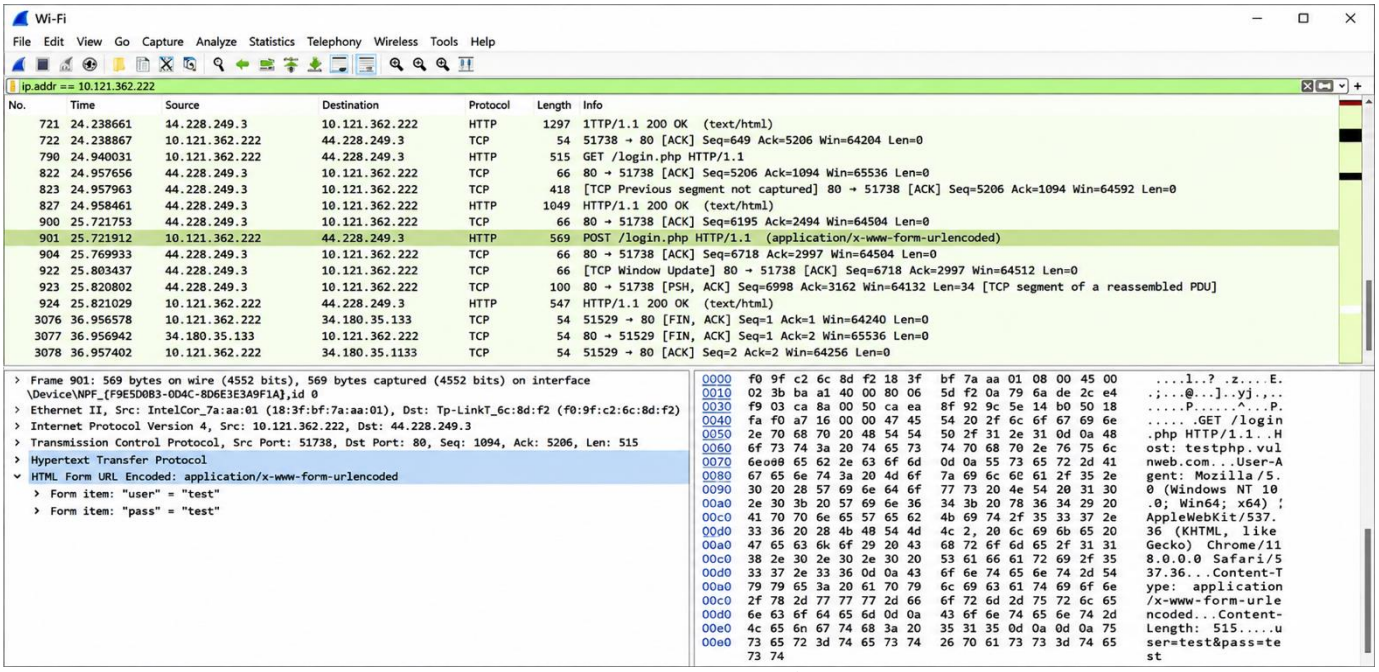

Fig. 3 The Selected Captured transmission session of the Personal Interaction

Following that, within packet 823, there is an occurrence of contact with the login page where the activity of signing up for an account is initiated by clicking a button or link. This action initiates supplementary requests and answers between the client and the server, resulting in the acquisition of additional information pertaining to the login page. Starting from packet 900, all the specific information related to the login page, such as form fields, buttons, and other components, is recorded in the network traffic data. This full capture allows for a meticulous analysis of the login page's structure, content, and operation, offering significant insights into the behaviour and potential weaknesses of the online service.

The packets 794, 823, and 900 provide a comprehensive view of the user's interaction with the web application hosted at testphp.vulnweb.com/login.php. This allows for a thorough investigation of the application's functionality and security status. The research findings indicate a weakness in the website testphp.vulnweb.com/login.php, namely related to how user-entered information is managed. This vulnerability was discovered through an examination that entailed capturing the transmission session using Wireshark, a network protocol analyzer.

During the analysis, it was noted that the login page of the website offered default login credentials, with the username pre-set as "test" and the password as "test" (see Figure 4). This configuration implies a possible security vulnerability, as the website can be retaining user data without employing sufficient security protocols. This vulnerability presents a substantial threat to user privacy and the integrity of data, as unauthorised parties could potentially access important information, leading to compromise. In addition, the research emphasises the robustness of the network architecture, even when faced with temporary interruptions or delays at certain router locations. The resilience of the network is demonstrated by the uninterrupted flow of packets, despite certain routers failing to receive them within the specified time limit. Notwithstanding these difficulties, the packets persevered in being transmitted, ultimately reaching their designated destinations. Finally, these findings emphasise the significance of having strong security measures to safeguard

https://doi.org/10.31436/ijpcc.v10i1.461

user data and address vulnerabilities in web applications. Furthermore, they stress the importance of ongoing surveillance and examination of network traffic to promptly detect and resolve possible security risks.

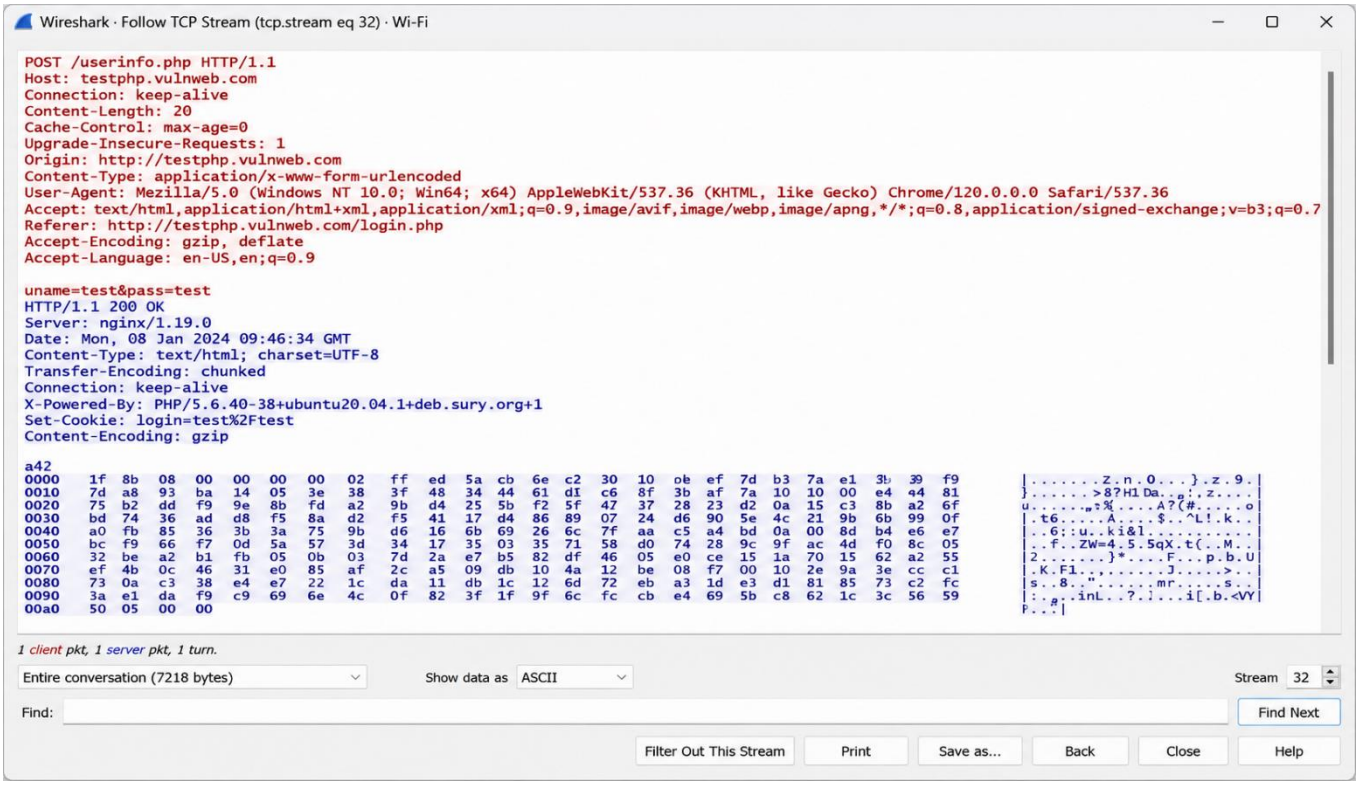

Fig. 4 The Explored Personal Details on the Transmission Session Captured

The findings emphasise the significance of having strong security rules and optimal procedures to reduce risks linked to unauthorised access and data breaches. Moreover, they emphasise the need of web developers and administrators giving top priority to security issues during the design, development, and deployment stages of web applications. Furthermore, the research has shown that network topologies are able to maintain uninterrupted packet progression, even when they experience temporary disturbances or delays at certain router sites. The resilience of modern network infrastructures highlights their reliability and efficiency in ensuring uninterrupted connection and data transmission. Ultimately, this study serves as a plea for stakeholders in many sectors to give priority to cybersecurity endeavours and establish strong security protocols to protect against ever-changing dangers in an interconnected digital environment. We can only guarantee the integrity, confidentiality, and availability of user data in the online environment by being watchful together and making coordinated attempts

V. CONCLUSION

Through rigorous analysis of network traffic using Wireshark, this research has identified serious vulnerabilities within the website testphp.vulnweb.com/login.php. The identification of a vulnerability in the processing of user-provided data, together with the existence of default login credentials on the login page, highlights the immediate necessity for enhanced security measures. These procedures are crucial for safeguarding user privacy and maintaining the integrity of sensitive data. Given these discoveries, it is crucial for organisations and developers to give priority to proactive security measures. This encompasses the performance of routine security audits, vulnerability assessments, and the implementation of strong encryption techniques. Organisations may effectively reduce risks, protect user data, and preserve user trust in the digital ecosystem by adopting a proactive approach to cybersecurity. To summarise, the discovery of weaknesses in testphp.vulnweb.com/login.php serves as a critical reminder of the significance of giving priority to cybersecurity endeavours. Organisations may enhance the security of their systems and users in a constantly changing

digital environment by adopting thorough security measures and adhering to best practices.

ACKNOWLEDGMENT

This research is made possible and supported by UMP-IIUM Sustainable Research Collaboration 2022 Research Grant (IUMP-SRCG22-014-0014).

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

REFERENCES

[1] J. Mehra. Web Personalization Using Web Session for Web Usage Mining. In2nd International Conference on Data, Engineering and Applications (IDEA) 2020, 28 (pp. 1-5).

[2] A. Følstad, C. Taylor. Investigating the user experience of customer service chatbot interaction: a framework for qualitative analysis of chatbot dialogues. Quality and User Experience. 2021 Dec;6(1):6.

[3] R. Shah, S. Correia S. Encryption of data over HTTP (hypertext transfer protocol)/HTTPS (hypertext transfer protocol secure) requests for secure data transfers over the internet. In2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT) 2021, 27 (pp. 587-590).

[4] A. Court, H. Alamleh . Multi-path Data Transmission to Protect Data in Transit. In2023 IEEE International Conference on Consumer Electronics (ICCE) 2023, 6 (pp. 1-6).

[5] A. Agrawal, A. Bhatia, A. Bahuguna, K. Tiwari, K. Haribabu, D. Vishwakarma, R. Kaushik. A survey on analyzing encrypted network traffic of mobile devices. International Journal of Information Security. 2022 Aug;21(4):873-915.

[6] D.I. Elewaily, H.A. Ali, A.I. Saleh, M.M. Abdelsalam. Delay/Disruption-Tolerant Networking-based the Integrated Deep-Space Relay Network: State-of-the-Art. Ad Hoc Networks. 2024 Jan 1;152:103307.

[7] F.F. Ashrif, E.A. Sundararajan, R. Ahmad, M.K. Hasan, E. Yadegaridehkordi. Survey on the authentication and key agreement of 6LoWPAN: Open issues and future direction. Journal of Network and Computer Applications. 2023 Oct 8:103759.

[8] J. Ruohonen. The Similarities of Software Vulnerabilities for Interpreted Programming Languages. In2021 IEEE International Conference on Progress in Informatics and Computing (PIC) 2021, 17 (pp. 304-307).

[9] W. Fraczek, W. Mazurczyk, K. Szczypiorski. Stream control transmission protocol steganography. In2010 International Conference on Multimedia Information Networking and Security 2010 Nov 4 (pp. 829-834)..

[10] S.K. Ghosh, A. Das, S.C. Ghosh, N. Das. Anti-eavesdropping Proportional Fairness Access Control for 5G Networks. InQuality, Reliability, Security and Robustness in Heterogeneous Systems: 17th EAI International Conference, QShine 2021, Virtual Event, November 29–30, 2021, Proceedings 17 2021 (pp. 144-158). Springer International Publishing.

[11] W. Frączek, W. Mazurczyk, and K. Szczypiorski, "Stream control transmission protocol steganography," in *Proc. 2010 Int. Conf. Multimedia Inf. Netw. Secur.*, Nanjing, China, Nov. 2010, pp. 829–834, doi: 10.1109/MINES.2010.177.

[12] S.A. Nor, R. Alubady, W.A. Kamil. Simulated performance of TCP, SCTP, DCCP and UDP protocols over 4G network. Procedia computer science. 2017 Jan 1;111:2-7.

[13] H. Nafea K. Kifayat Q. Shi, K.N. Qureshi, B. Askwith B. Efficient non-linear covert channel detection in TCP data streams. IEEE Access. 2019 Dec 25; 8:1680-90.

[14] V. Pevnev., Aleksandr, Frolov., Mikhail, Tsuranov., Heorhii, Zemlianko. Ensuring the Data Integrity in Infocommunication Systems. International Journal of Computing, 21(2) 2022, 228-233.

[15] C. Westlake C, inventor; Cardeasy Ltd, assignee. Accessing information from an internet user's web session. United States patent US 8,775,608. 2014 Jul 8.

[16] V, Tea, H. Huang. A method for establishing an http-ota session between a secure element and an http-ota platform. US Patent App. 16/327,427, 2019.

[17] A. Zúquete, F. Marques. An Architecture to Support the Invocation of Personal Services in Web Interactions. arXiv preprint arXiv:1904.01541. 2019 Apr 2.

[18] A. Avgetidis, O. Alrawi, K. Valakuzhy, C. Lever, P. Burbage, A. Keromytis, F. Monrose, M. Antonakakis. Beyond the gates: An empirical analysis of HTTP-managed password stealers and operators. In32nd USENIX security symposium (USENIX Security 23) 2023.

[19] M.A. Eltokhy, M. Abdel-Hady, A. Haggag, M.A. El-Bendary, H. Ali, T. Hosny. Audio SIMO system based on visible light communication using cavity LEDs. Multimedia Tools and Applications. 2023,10:1-5.