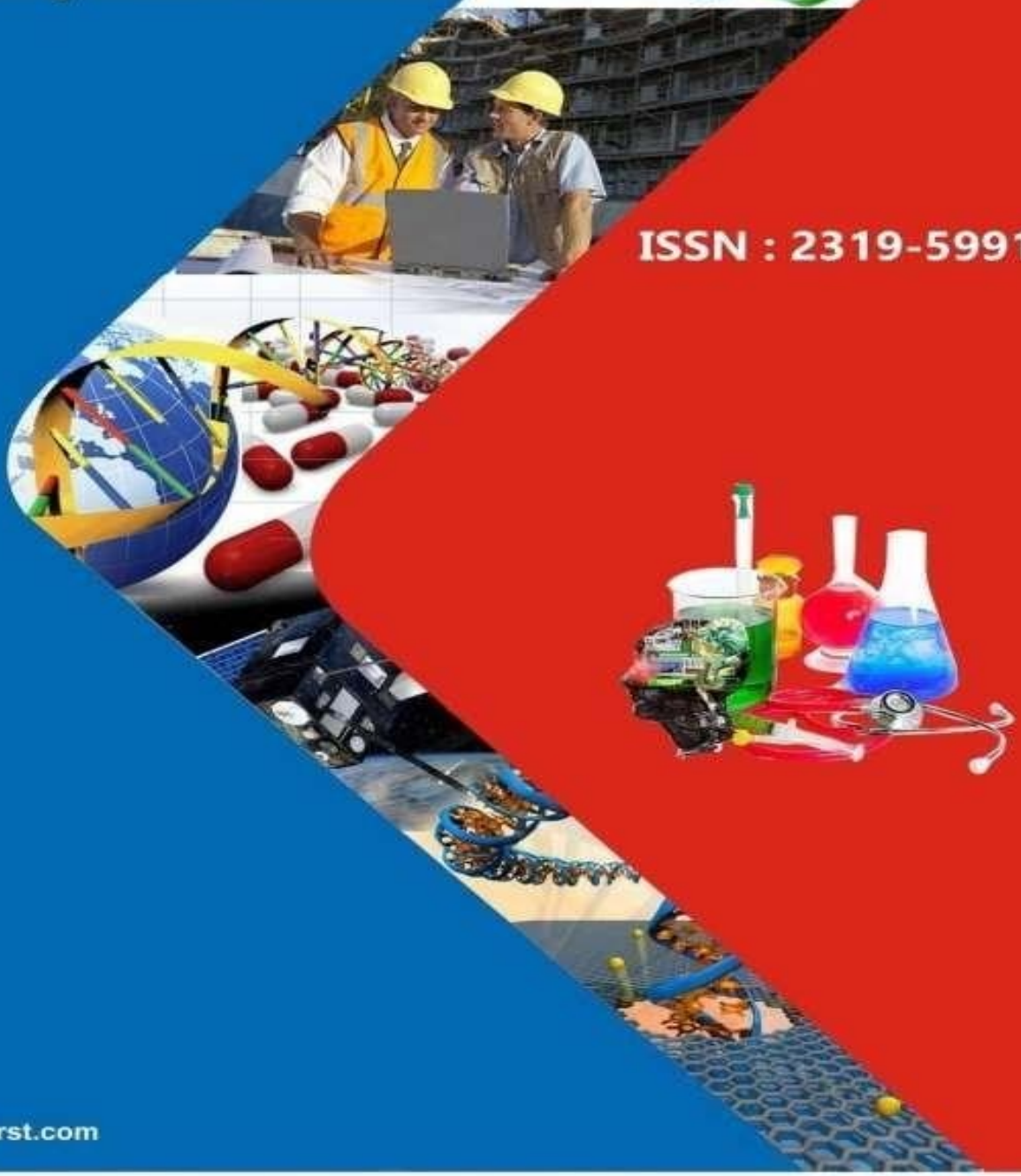
International Journal of Engineering Research and Science & Technology

IJERST

ISSN : 2319-5991



www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp747-755

Vol. 21, Issue 2, 2025

EXPOSING WEB VULNERABILITIES: A STUDY OF MAN-IN-THE-MIDDLE AND SESSION HIJACKING ATTACKS

[1]*Kummari Teja*, *MCA Student, Department of MCA*

[2] *Dr.K.Pavan Kumar, Ph.D, Associate Professor, Department of MCA*

[12]*Dr KV Subba Reddy Institute of Technology, Dupadu, Kurnool*

ABSTRACT

These days, data is king, thanks to the Internet. This data is very susceptible to attackers because of the seemingly open access Internet service. Attacks happening on the web may compromise users' data privacy. Attacks that occur on the Internet, including Man-In-The-Middle and session hijacking, are the subject of this SLR. Using an appropriate research selection approach, it examines around 30 studies spanning from 2016 to 2023. There are three research questions that make up this SLR. The first one gives an overview of recent tendencies in research on session hijacking and man-in-the-middle attacks. The trend indicates that there will be a decrease in the number of articles published from 7 in 2018 to 4 in 2021. India also ranks first in this field, with 73% of publications published in conference settings. As a publication, IEEE is the leading contributor, as this question highlighted. The second one discusses the methods that Man-In-The-Middle attacks and session hijacking apply to TCP/IP. The results show that whereas session hijacking attacks target just two levels—the application and the network—Man-In-The-Middle attacks target all layers. Thirdly, we want to know how various studies have dealt with session hijacking and man-in-the-middle assaults. Finally, by illuminating developing patterns, causes, and remedies in data privacy, this research emphasises the need of more robust cyber defences against Man-in-the-Middle and session hijacking attacks in the Internet age.

I. INTRODUCTION

There is a large user base for web-based apps due to the prevalence of the Internet [1]. It allows for server-client communication over web protocols [2]. Improving the quality of work is an integral aspect of everyday operations in many fields, including business, study, banking, shopping malls, etc. Users' personal information is securely stored on the web, which is a central repository for data [3]. Websites are very susceptible to attacks because of the increased use of the Internet. A vulnerability is any opening that might allow unauthorised access to sensitive information, compromise system security, or cause harm to the website, web application, or any of its components or activities. There are other common types of vulnerabilities, such as those involving networks or assets, but they are different. The need for online applications to connect with several users across different networks gives rise to these vulnerabilities, which hackers may easily exploit. By exploiting security holes in online applications, hackers may get unauthorised access to a company's data, processes, and vital assets.This kind of access gives attackers a lot of power, including the ability to hijack programs, plan attacks, use privilege escalation to steal data, disrupt essential services on a large scale, and much more besides. Approximately 42% of websites are compromised by cybercrimes [4]. Images of several web-based assaults are shown in Fig. 1. Sniffing out data packets in transit over a network is known as packet sniffing [5]. An attack known as SQL injection may compromise a network by gaining access to data packets in transit via the use of malicious backend

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp747-755
Vol. 21, Issue 2, 2025

programs [6]. In addition, vulnerable websites may have their data interaction compromised by cross-site scripting (XSS) [7]. Another kind of attack, known as path traversal, may access web servers by following a user's steps to get data [8]. Another way that bad actors might access data at the input and output devices—the places where data is created and sent—is via spooling [9]. In addition, all data from a web session may be stolen using Session Hijacking (SH) [10]. Finally, there's the Man-In-The-Middle (MITM) attack, when the hacker secretly listens in on the network [11].

It is essential to go beyond traditional vulnerability scanners when trying to identify security flaws in an organization's applications, since there are web application security solutions designed specifically for apps. A company's reputation and bottom line may be protected against data breaches and other security catastrophes with the aid of vulnerability management. Various security criteria and regulations may be more easily met with the aid of vulnerability management.

The three most common types of online attacks are man-in-the-middle attacks, phishing, and session hijacking. A Man-in-the-Middle assault in action (Figure 2). Internet assaults in their passive session hijacking condition (FIGURE 3). Attacks that aim to invade user privacy include Man-In-The-Middle (MITM) [11] and session hijacking [10]. When users communicate with the web app, their information is protected via Hypertext Transfer Protocol Secure (HTTPS) [12]. Transmission Control Protocol/Internet Protocol (TCP/IP) is essential for user-to-user communication [13]. Despite stringent security measures, the perpetrator nevertheless manages to get access to the user's private information.

In a man-in-the-middle (MITM) assault, the perpetrator even manages to disrupt the communication between users or between users and a website. This kind of attack happens when two legitimately connected hosts enable an intruder to illegally listen in on conversation [8]. The term "Man-In-The-Middle" describes an assault in which the perpetrator stands between the two parties involved in a communication. It breaks the user's initial connection to the website and establishes a new one in which the attacker may listen in on every word [15]. The man-in-the-middle assault is shown in Figure 2.

An intruder sits within the network and hijacks it passively. Subsequently, the hacker divulges the information to others posing as authorised network users. So, it takes over the system in this manner [10]. Displayed in Figure 3 is passive session hijacking. An active hijacking occurs when an attacker attempts to compromise a session that has already been created between users [10]. While launching a denial-of-service (DOS) attack, the malicious actor sniffs the session. This is an example of session sniffing, rather than an invasion of the user's connection to the web page. The hijacking of a session is shown in Figure 4. It is critical to address Blockchain technology in light of the present era's high attack rate. Unlike traditional databases, blockchains store data in interconnected blocks protected by encryption. It might be put to a lot of different applications. Reason being, it can enable secure, transparent, and global payments, which may radically alter the nature of financial transactions. Some well-known cryptocurrencies that provide this function are Bitcoin and Ethereum. Blockchain technology tracks the movement of assets and products, which enhances supply chain efficiency and transparency. By combining blockchain technology with self-executing contracts, we can automate agreements and

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp747-755
Vol. 21, Issue 2, 2025

transactions, cutting out intermediaries and saving money. By creating trustworthy digital identities, this technology streamlines operations like identity verification and document management. With blockchain technology, authorised parties may more easily share information and sensitive healthcare data is securely handled and stored, protecting patient privacy.

In conclusion, this technology has evolved into a game-changer, impacting future digital connections and reshaping several sectors. Its decentralised and secure nature gives it great promise for enhancing digital trust, streamlining processes, and increasing transparency. Its potential to boost confidence, openness, and safety is undeniable. As time goes on and more complicated problems are solved, blockchain is likely to have an even bigger impact on the digital world [14], [15], [16].

To avoid the risks of online assaults, it is essential to implement robust security measures. Various literature reviews have detailed a plethora of strategies. Businesses may significantly reduce their vulnerability to man-in-the-middle attacks, session hijacking, and other web-based hazards by implementing these strategies and staying updated on emerging threats. We want to collect this data in order to utilise it for two purposes: first, to guide the creation of new methods to fix these internet vulnerabilities; and second, to use these methods to guard against web assaults, particularly Man-in-the-Middle and session hijacking attacks.

There are three research questions in this article that will help find things like distribution by year, contribution by nation, publishing kind, article publishers, attack ratio, and a solution for man-in-the-middle and session hijacking.In order to alter data for our experiment, we examined several research papers' characteristics and factors related to Man-In-the-Middle (MITM), Session Hijacking (SH), Web Accessibility, and SH-MITM. Using relevant man-in-the-middle and session hijacking online attacks, this quantitative analysis is conducted in a systematic manner. Second, we gathered data from published articles and conference papers. Key information resources include IEEE, ACM, and Science Direct. Lastly, we took a look at the main security holes found in this study, which include things like fake server linkages, HTTPS application layers, unauthorised user access, and unexamined updated technology.

II. LITERATURE SURVEY

"Survey of web application vulnerability attacks," by O. B. Al-Khurafi and M. A. Al-Ahmad, published in December 2015 in the proceedings of the 4th International Conference on Advanced Computer Science and Applications (ACSAT), pages 154 to 158.

Online apps now play a crucial role in our everyday lives. Hackers seek for security flaws in online apps in order to steal data, impersonate users, or even destroy them altogether. This is because these programs hold sensitive information that is useful to the attackers. This article provides a detailed analysis of the three most common and dangerous vulnerabilities in online applications: SQL Injection, Broken Authentication and Session Management, and Cross-Site Scripting (XSS).

"Survey of the protection mechanisms to the SSL-based session hijacking attacks," published in Netw.Protocols Algorithms in April 2018, by M. S. Hossain, A. Paul, M. H. Islam, and M. Atiquzzaman, pages 83–108.

The use of web connections between servers and clients is widespread. Yet, for the majority of client-server connections, session hijacking has emerged as a key issue. Among several

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp747-755
Vol. 21, Issue 2, 2025

session hijacking attempts, SSL stripping poses the greatest threat. Several countermeasures have been suggested to stop session hijacking attempts that rely on SSL tripping. Unfortunately, previous surveys lacked a thorough summary of all the preventative strategies, since they lacked proper depiction and classification. This paper's goal is to examine and contrast current methods for protecting sessions against SSL stripping-based attacks. In this article, we have sorted all the current safeguards against SSL stripping-based session hijacking threats into two broad groups: those implemented on the client side and those implemented on the server side. We have included helpful graphics to thoroughly describe the solutions that have been suggested. Additionally, we have evaluated them using several performance metrics. By comparing and contrasting all solutions for SSL stripping based attacks, this article will aid web security experts in enhancing current solutions to better protect users against session hijacking attacks.

"Ethical dilemmas and privacy issues in emerging technologies:Areview," Sensors, vol. 23, no. 3, p. 1151, Jan. 2023, by L. L. Dhirani, N. Mukhtiar, B. S. Chowdhry, and T. Newe.

Cybersecurity threats specific to artificial intelligence (AI) have emerged as a result of the technology's fast adoption in mission-critical industries. There is a wide variety of cyber attacks that may damage or disable AI systems because to their complicated algorithms, large data dependencies, and other characteristics. Data poisoning, adversarial assaults, and systemic vulnerabilities resulting from the operational and infrastructure frameworks of the AI are all thoroughly examined in this article. Current defensive strategies that attempt to strengthen AI systems against such weaknesses are examined critically in this work. These mechanisms include adversarial training and threat modelling. This study delves into a thorough framework for the development and execution of strong AI systems as a reaction to the shortcomings of existing methods. The focus of this approach is on strengthening AI systems' resilience via the creation of dynamic and adaptive security mechanisms that may change in reaction to new cyber threats. In addition to discussing the technical aspects of AI cybersecurity, the article delves into the moral implications, stressing the need of measures to safeguard user data while also promoting equity in all dealings. This article delves into future avenues in AI cybersecurity while also examining present tactics and ethical problems.

In the proceedings of the annual international conference on theory and applications of cryptography, held in Trondheim, Norway in 2022 and published by Springer, the authors "Single-server private information retrieval with sublinear amortised time" (pp. 3-33).

In the context of a single server, we provide novel techniques for retrieving confidential information. With our techniques, a client may access a series of database entries anonymously, and the server can respond to each query in an average time that is sublinear to the size of the database. To be more precise, we provide the first single-server private information retrieval techniques that permit adaptive client queries, have sublinear amortised server time, and need sublinear extra storage. Simple cryptographic assumptions (e.g., choice Diffie-Hellman, quadratic residuosity, learning with mistakes) are all that our protocols depend on. In order for them to function, the client must first request a little "hint" on the database's contents from the server. It takes server time that is proportional to the size of the database to generate this hint. Subsequently, the client may use the hint to send a limited number of adaptive queries to the server, which will provide sub-linear amortised

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp747-755
Vol. 21, Issue 2, 2025

cost replies in sub-linear time. Last but not least, we prove, via lower bounds, that our best strategy optimises the trade-off between server up time and client storage.

III. SYSTEM ANALYSIS AND DESIGN

EXISTING SYSTEM

As an example, a survey on the prevention of session hijacking [2] on Secure Socket Layer / Transport Layer Protocol (SSL/TLP) is only one of several separate surveys carried out in the area of Man-in-the-middle attacks and session hijacking. It can only handle SSL/TLP. In addition, session hijacking's cutting-edge approach is covered in another study [10]. Session hijacking in financial systems is the only topic covered here. Classification of attacks and solutions to cope with attackers are shown in a survey linked to MITM assaults [11]. Using MITM in computer and wireless networks is the subject of yet another review paper [17]. It classifies MITM attacks and provides ways to avoid them.

The topic of security is not addressed in another poll [18], which is concerned with accessibility for those with impairments on the Web. Topics like as man-in-the-middle attacks and session hijacking are not addressed in this work [19]. In addition, while one article addresses web accessibility, another skips over the security concerns of session hijacking and man-in-the-middle attacks. No research has concentrated on session hijacking and MITM at the same platform, according to the analysis of references [2, 10, 11, 17, 18, 19]. According to Table 1, there is a lack of study on MITM and Session Hijacking (MITM-SH), which necessitates SLR. The overarching goal of this SLR is to examine and contrast SH with MITM.

Disadvantages

1) An attacker may create a hostile environment in which users are unable to interact or transfer data in a TCP hijacking. This is an example of how an attacker might record an entire network session by duplicating data flowing from both ends [40].

Attempting to get unauthorised access, IP spoofing disguises the actual user's IP address and communicates via a network [24], [26], [31], [34], [35], “46”.

A packet sniffer allows an attacker to see the data exchanged between users via an interface that is shared by all of them [47].

4) Before the server answers, the attacker in UDP hijacking replies as a valid user [48].

PROPOSED SYSTEM

Three research questions make up the suggested system; they will aid in determining the following: distribution by year, contribution by nation, publishing kind, article publishers, assault ratio, and the suggested solution for man-in-the-middle and session hijacking. In order to alter data for our experiment, we examined several research papers' characteristics and factors related to Man-In-the-Middle (MITM), Session Hijacking (SH), Web Accessibility, and SH-MITM. Using relevant man-in-the-middle and session hijacking online attacks, this quantitative analysis is conducted in a systematic manner. Second, we gathered data from published articles and conference papers. Science Direct, IEEE, and ACM are the main places to get this information. Lastly, we took a look at the main security holes found in this study, which include things like fake server linkages, HTTPS application layers, unauthorised user access, and unexamined updated technology.

Advantages

• There is great potential in the suggested approach to integrate behavioural analytics with cybersecurity measures. It is possible to detect compromised sessions or unauthorised access by analysing patterns of user behaviour in real time. Extensive research is being conducted to

International Journal of Engineering Research and Science & Technology

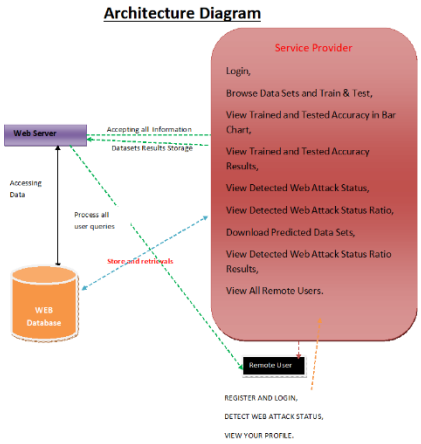
ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp747-755

Vol. 21, Issue 2, 2025

enhance and personalise behavioural analytics models in order to provide a versatile defence against threats such as Man-in-the-Middle attacks and session hijacking.

SYSTEM ARCHITECTURE



IV. IMPLEMENTATION

Service Provider

The Service Provider must provide their username and password in order to access this module. Once he has successfully logged in, he will be able to do actions like browsing data sets and running tests. Look at the Bar Chart for Trained and Tested Accuracy, Check Out the Results for Trained and Tested Accuracy, Check the Current Status of Detected Web Attacks, See the Current Status Ratio of Detected Web Attacks, Download Data Sets with Predictions, Check the Results of the Web Attack Status Ratio, See Who Is Accessible From Another Location.

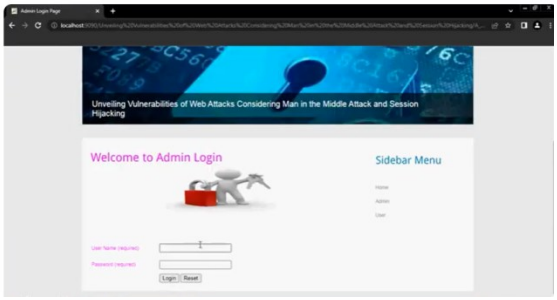
View and Authorize Users

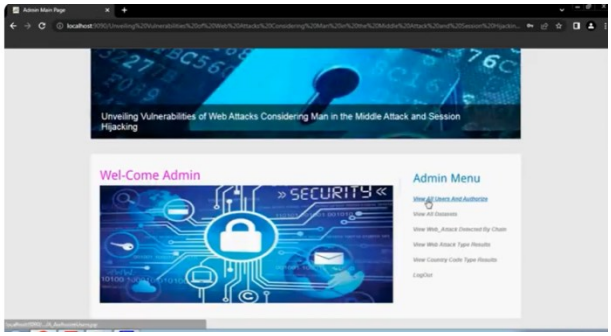
The administrator has access to a comprehensive list of registered users in this section. Here, the administrator may see the user's information (name, email, and address) and grant them access.

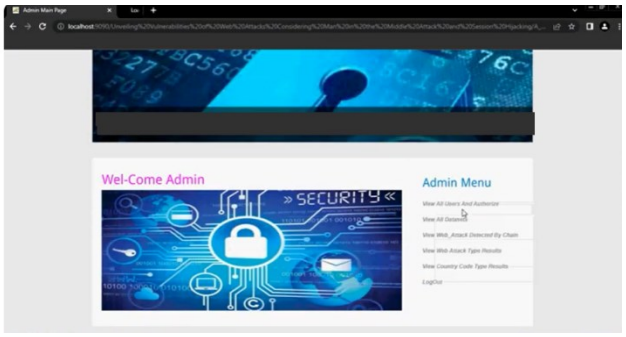
Remote User

There are n users in this module at the moment. Do not proceed with any activities until the user has registered. The user's information will be entered into the database after they register. He will need to log in using the authorised username and password when registration is completed. The user will be able to do actions such as seeing their profile, detecting web attack status, and logging in when the login process is successful.

V. SCREEN SHOTS





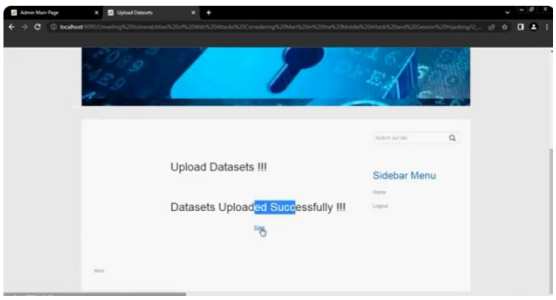


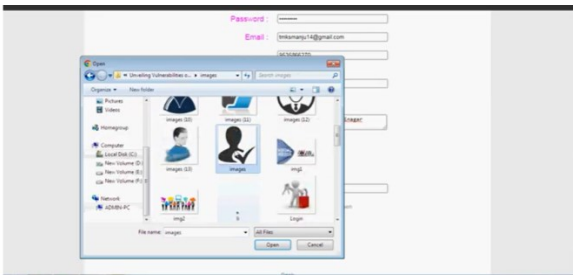
International Journal of Engineering Research and Science & Technology

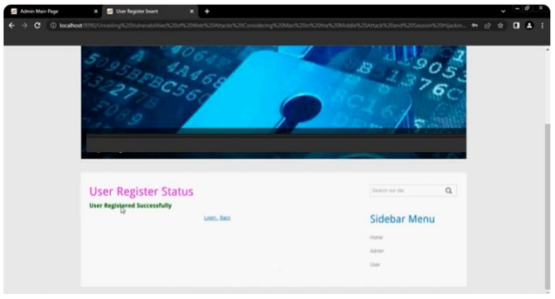
ISSN 2319-5991 www.ijerst.com

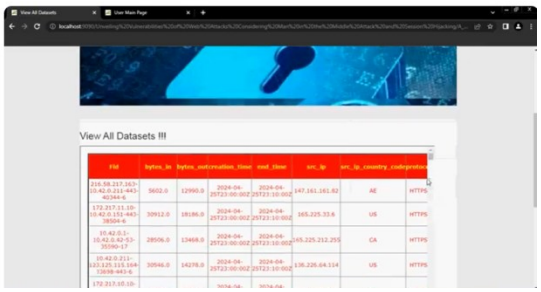
https://doi.org/10.62643/ijerst.2025.v21.i2.pp747-755

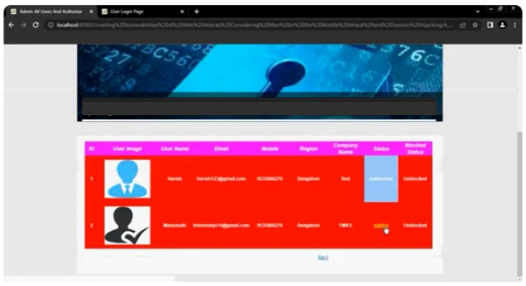
Vol. 21, Issue 2, 2025

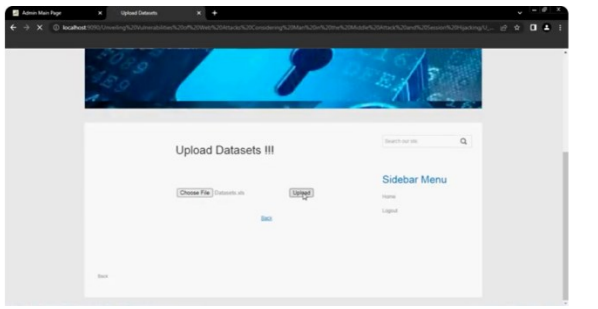


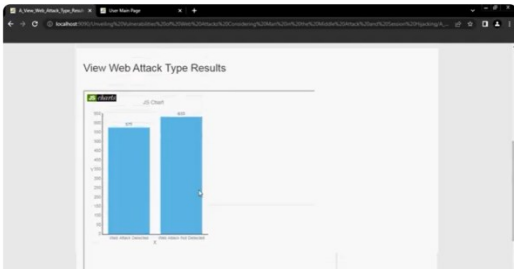










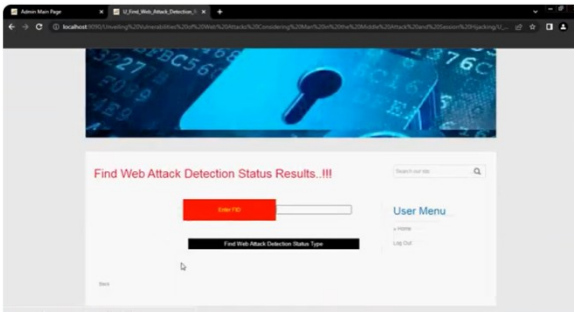


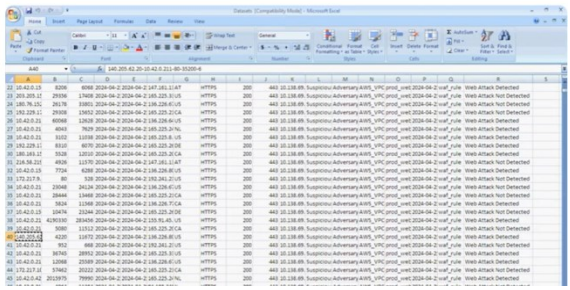
International Journal of Engineering Research and Science & Technology

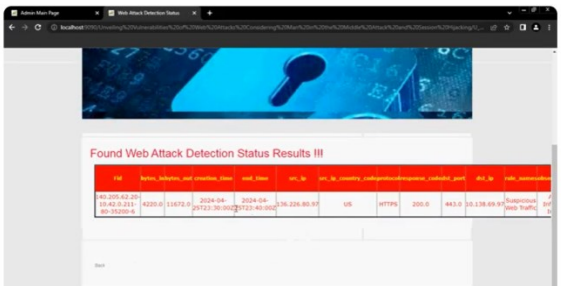
ISSN 2319-5991 www.ijerst.com

https://doi.org/10.62643/ijerst.2025.v21.i2.pp747-755

Vol. 21, Issue 2, 2025







VI. CONCLUSION

Web-based apps are often used online and are vulnerable to many threats. There are two distinct kinds of online attacks: session hijacking and MITM. According to evaluations, the research trend peaked in 2018 with seven publications; also, India is the country that contributes the most to the field of MITM-SH, with eight out of thirty papers. 73% of the chosen publications are conference pieces, which make up the majority of the articles. Additionally, research indicates that whereas session hijacking only happens on the application and network levels of the TCP/IP protocol, MITM attacks may occur on all five layers. Furthermore, whereas session hijacking just involves the attacker taking control of the system and saving a copy of it, MITM involves the attacker sitting between the user and the Web site. Finally, MITM-SH methods are offered to identify, stop, and lessen the assaults.

REFERENCES

[1] O. B. Al-Khurafi and M. A. Al-Ahmad, ‘‘Survey of web application vulnerability attacks,’’ in Proc. 4th Int. Conf. Adv. Comput. Sci. Appl. Technol. (ACSAT), Dec. 2015, pp. 154–158.

[2] M. S. Hossain, A. Paul, M. H. Islam, and M. Atiquzzaman, ‘‘Survey of the protection mechanisms to the SSL-based session hijacking attacks,’’ Netw. Protocols Algorithms, vol. 10, no. 1, pp. 83–108, Apr. 2018.

[3] L. L. Dhirani, N. Mukhtiar, B. S. Chowdhry, and T. Newe, ‘‘Ethical dilemmas and privacy issues in emerging technologies:Areview,’’ Sensors, vol. 23, no. 3, p. 1151, Jan. 2023.

[4] H. Corrigan-Gibbs, A. Henzinger, and D. Kogan, ‘‘Single-server private information retrieval with sublinear amortized time,’’ in Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn. Trondheim, Norway: Springer, 2022, pp. 3–33.

[5] D. Glăvan, C. Răcuciu, R. Moinescu, and S. Eftimie, ‘‘Sniffing attacks on computer networks,’’ Sci. Bull. Mircea cel Batran Naval Academy, vol. 23, no. 1, pp. 202–207, 2020.

[6] M. Nasereddin, A. ALKhamaiseh, M. Qasaimeh, and R. Al-Qassas, ‘‘A systematic review of detection and prevention techniques of SQL injection attacks,’’ Inf. Secur. J., Global Perspective, vol. 32, no. 4, pp. 252–265, Jul. 2023. [7] V. Nithya, S. L. Pandian, and C. Malarvizhi, ‘‘A survey on detection and prevention of cross-site scripting attack,’’ Int. J. Secur. Appl., vol. 9, no. 3,
pp. 139–152, Mar. 2015.

[8] A. Bernal, O. Parra, and R. Díaz, ‘‘Man in the middle attack: Prevention in wireless LAN,’’

International Journal of Engineering Research and Science & Technology
ISSN 2319-5991 www.ijerst.com
https://doi.org/10.62643/ijerst.2025.v21.i2.pp747-755
Vol. 21, Issue 2, 2025

Int. J. Appl. Eng. Res., vol. 13, no. 7, pp. 4671–4672, 2018.
[9] H. Fadhil and A. R. Hakim, ‘‘Classification model of web application attacks,’’ in Proc. 6th Int. Workshop Big Data Inf. Secur. (IWBIS), Oct. 2021, pp. 87–90.
[10] P. Kamal, ‘‘State of the art survey on session hijacking,’’ Global J. Comput. Sci. Technol., vol. 16, no. 1, pp. 39–49, Mar. 2016.
[11] M. Conti, N. Dragoni, and V. Lesyk, ‘‘A survey of man in the middle attacks,’’ IEEE Commun. Surveys Tuts., vol. 18, no. 3, pp. 2027–2051, 3rd Quart., 2016.
[12] D. Glăvan, C. Răcuciu, R. Moinescu, and S. Eftimie, ‘‘Man in the middle attack on HTTPS protocol,’’ Sci. Bull. Mircea cel Batran Naval Academy, vol. 23, no. 1, pp. 199–201, 2020.
[13] A. A. Mohammadi, R. Hussain, A. Oracevic, S. M. A. R. Kazmi, F. Hussain, M. Aloqaily, and J. Son, ‘‘A novel TCP/IP header hijacking attack on SDN,’’ in Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), May 2022, pp. 1–2.
[14] N. S. Alghamdi and M. A. Khan, ‘‘Energy-efficient and blockchainenabled model for Internet of Things (IoT) in smart cities,’’ Comput., Mater. Continua, vol. 66, no. 3, pp. 2509–2524, 2021.
[15] F. Algarni, M. A. Khan, W. Alawad, and N. B. Halima, ‘‘P3S: Pertinent privacy-preserving scheme for remotely sensed environmental data in smart cities,’’ IEEE J. Sel. Topics Appl. Earth Observ. Remote Sens., vol. 16, pp. 5905–5918, 2023.
[16] M. A. Khan, ‘‘A formal method for privacy-preservation in cognitive smart cities,’’ Expert Syst., vol. 39, no. 5, p. e12855, Jun. 2022.
[17] B. Bhushan, G. Sahoo, and A. K. Rai, ‘‘Man-in-the-middle attack in wireless and computer networking—A review,’’ in Proc. 3rd Int. Conf. Adv. Comput., Commun. Autom. (ICACCA), Sep. 2017, pp. 1–6.
[18] T. C. P. B. Pichiliani and E. B. Pizzolato, ‘‘Cognitive disabilities and web accessibility: A survey into the Brazilian web development community,’’ J. Interact. Syst., vol. 12, no. 1, pp. 308–327, Dec. 2021.
[19] P. Teixeira, C. Eusébio, and L. Teixeira, ‘‘Diversity of web accessibility in tourism: Evidence based on a literature review,’’ Technol. Disability, vol. 33, no. 4, pp. 253–272, Nov. 2021.
[20] B. Kitchenham, L. Madeyski, and D. Budgen, ‘‘How should software engineering secondary studies include grey material?’’ IEEE Trans. Softw. Eng., vol. 49, no. 2, pp. 872–882, Feb. 2023.
[21] S. Ajmal and M. B. Muzammil, ‘‘PVRS: Publication venue recommendation system a systematic literature review,’’ in Proc. 5th Int. Conf. Comput. Eng. Design (ICCED), Apr. 2019, pp. 1–6.
[22] A. R. Chordiya, S. Majumder, and A. Y. Javaid, ‘‘Man-in-the-middle (MITM) attack based hijacking of HTTP traffic using open source tools,’’ in Proc. IEEE Int. Conf. Electro/Inf. Technol. (EIT), May 2018, pp. 0438–0443.
[23] D. R. Rupal, D. Satasiya, H. Kumar, and A. Agrawal, ‘‘Detection and prevention of ARP poisoning in dynamic IP configuration,’’ in Proc. IEEE Int. Conf. Recent Trends Electron., Inf. Commun. Technol. (RTEICT), May 2016, pp. 1240–1244.
[24] S. Al-Sharif, F. Iqbal, T. Baker, and A. Khattack, ‘‘White-hat hacking framework for promoting security awareness,’’ in Proc. 8th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS), Nov. 2016, pp. 1–6.
[25] S. Sivakorn, A. D. Keromytis, and J. Polakis, ‘‘That’s the way the cookie crumbles: Evaluating HTTPS enforcing mechanisms,’’ in Proc. ACM Workshop Privacy Electron. Soc., Oct. 2016, pp. 71–81.