IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 1, January 2021

DOI 10.17148/IJARCCE.2021.10104

Detection of Cookie Hijacking in Web Application

Asmita Jagtap[1], Pratibha Tambewagh[2]

Lecturer, Information Technology Department,BVIT,Kharghar,Navi Mumbai[1]

Lecturer, Information Technology Department,BVIT,Kharghar,Navi Mumbai[2]

Abstract: In computer science, session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system. The session established between the user and the server can be hijacked by an attacker by masquerading as an authorized user called Man-in-the-Middle (MITM).The target of the attacker is to have access to users' confidential records in the server for their own financial gain. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer (see HTTP cookie theft). Cookie hijacking is commonly used against client authentication on the internet The security of Web applications have been a great concern to many online services. The paper, therefore developed a web application for e-Commerce for the detection and prevention of cookie hijacking in order to protect individual records from unauthorized user.

Keywords: Cookie, Cookie Hijacking, Security, Vulnerability, Authentication, HTTP, Web Application, MITM.

I. INTRODUCTION

There are various security threats that are associated with web applications based on the transactions that takes place online daily. The dynamics of the content and functionalities of the web application have enable the users to communicate with the server effectively and displaying information through the browser platform [1]. Some of the web applications used the users for transaction purposes are e-commerce, online banking, shopping sites, online training etc. Web applications are increasing in features, programming and content [2]. The improvement in the web application is as a result of the users that interact on the web daily for one transaction or the other.Cybercriminals mostly attacks web applications in order to access user's data that are related to their financial records from the web browsers by inserting malicious program.

Cookie Hijacking or Session Hijacking is the most critical issues confronting the web application in the current trend of technology.As the number of internet users keeps increasing, the vulnerabilities of the web increases also and session hijacking becomes a great concern to every owner of the web application in securing the environment. The most common attack is called man-in-middle attack (MITM) which can sometime cause denial-of-service.[3] A man-in-the-middle (MitM) attack is when an attacker intercepts communications between two parties either to secretly eavesdrop or modify traffic traveling between the two. Attackers might use MitM attacks to steal login credentials or personal information, spy on the victim, or sabotage communications or corrupt data.

Session management in a web application ensures that user who logged in, is still the same person connected to the server and the integrity of the network is still intact.

In Section II of this paper, discussed about previous research and related work in this area. Section III presents the methodology, architecture of the system,. Section IV highlight precaution to take on system maintenance. Section V conclude on the paper.

II. LITERATURE REVIEW

A. Related Works

Several other studies have stressed the importance of privacy, security and usability of identity management, each focusing on specific issues or looking at the problem from a particular perspective. From the previous review work, it shows there are still vulnerabilities in an online transactions and these calls for an urgent need to put in place a high level of security in web applications in terms of privacy, confidentiality and integrity. Table 1 present some of the techniques that have been used in the previous study and the limitations of the research work.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 1, January 2021

DOI 10.17148/IJARCCE.2021.10104

Table 1: Related works based on the previous study.

S/N	Author	Title	Methodology	Limitation
1.	[4]	Sub-Session Hijacking on the Web: Root Causes and Prevention.	Improving protection against sub-session hijacking	There is a need to perform a large-scale analysis in securing the web application as a step ahead in improving the current system.
3.	[5]	An Effective Method for Preventing SQL Injection Attack and Session Hijacking	Hashing Technique	The technique proposed is used to prevent SQL injection and session hijacking but did not consider other Web application vulnerabilities
4.	[6]	Prevention of Session hijacking using OneTime Cookies	OneTime Cookies	Dependent on the Reverse proxy server and Only 1 session/user. This might cause a shake in the web services in creating session for web application and in establishing connection.
5.	[7]	An Analysis of Seven Concepts and Design Flaws in Identity Management Systems	Design of identity management.	It design system to identify defects in a network but focus was not on web applications
6.	[8]	A prevention model for session hijack attacks in wireless networks using Strong & encrypted session ID	Strong and Encrypted Session ID was used	This is restricted to some length of session ID to generate the encryption in Hijacking.
7.	[9]	An Analytical Study of Web Application Session Management Mechanisms & HTTP Session Hijacking Attacks	Performance evaluation of session management mechanisms & HTTP	Only consider the evaluation performance of the web management and HTTP attacks but detection of the attack of the web was not looked into.
8.	[10]	Prevention of Session Hijacking and I spoofing with Sensor nodes and Cryptographic Approach	Sensor Nodes and Cryptographic Approach	This focused on the fake access point and IP spoofing to detect session hijacking but didn't consider other aspect of hijacking.

Session hijacking is one of the safety threats utilized by varied attackers round the world on the web. Session Hijacking plays a serious role to steal user's record and vital information that are transferred through the web. It has the potentials to takes data from the server without the consent of the users. Identity attacks are of different kinds and these uses various mode of action to tackle the challenges.

B. Session Hijacking

Session Hijacking is the most common type of attack. It is often preferred by attacker because of the penetration in accessing the session. When a user is logged in or about to login into the system and has established connection with the server, then attacker takes over the session by masquerading as if it's still the real user that is logged in.Session Hijacking is the taking over of the user session id and having full control of system while the session is still in progress. The session hacking indicating the attack between the server and browser using packet sniffer were presented in figure 1 below.

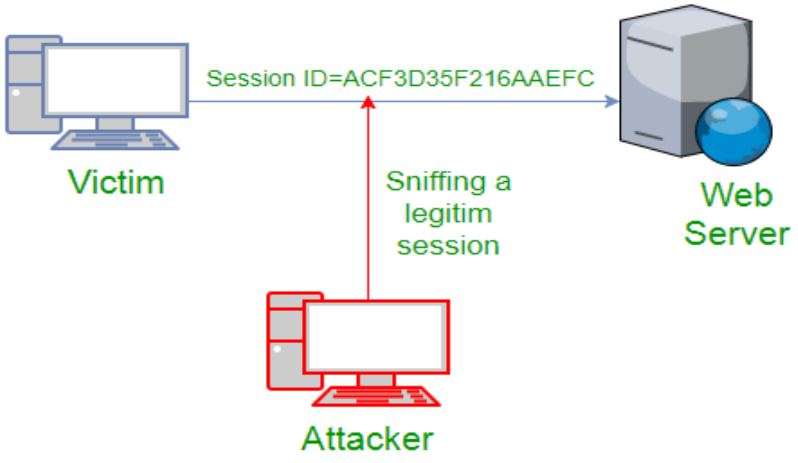

Figure 1: Session hijacking attack(Using Packet Sniffer)[11]

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 1, January 2021

DOI 10.17148/IJARCCE.2021.10104

In the above figure, it can be seen that attack captures the victim's session ID to gain access to the server by using some packet sniffers.

There are three types of session hijacking attacks:

i. Passive Session Hijacking: In a passive attack the focus is on monitoring the traffic or communication taking place between the client and the server. Sniffing software issued in this situation where the traffic monitored and captured while going across the wire.The attacker supervises the traffic between server and the digital computer. Within a passive connection the hacker follows the information of the user and safe it in a self-database to the purpose of attack. It is advisable for attacker to start with passion session hijacking [12]. The figure 2 display the e attack between the user and the server.

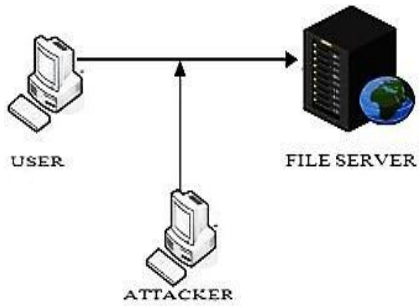

Figure 2: Passive Session Hijacking [13]

ii. Active Session Hijacking: This attack happens once the hacker takes over an active connection on a network. The hacker can mute one in all the devices, sometimes the shopper laptop, and overtake the clients' place within the communication exchange between the server and the digital computer and let go of the affiliation between the server and the user device [14]. There are different methods used to halt the connection with the server, one of the most common way is to send multiple quantity of traffic to attack the session which will cause a Denial of Service. This attack enable to have full control over the session id with the server. . Figure 3 shows the actual state of affairs of the active session hijacking.

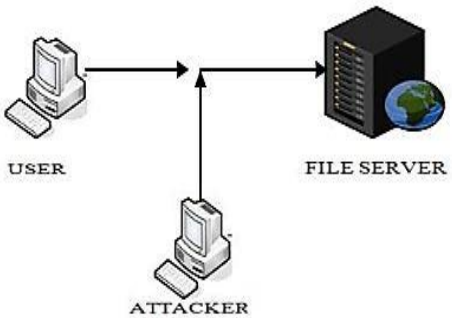

Figure 3: Active session hijacking [15]

iii. Hybrid Session Hijacking: This kind of attack is a combination of passive and active attacks that enables the assailant to concentrate to network traffic until one issue is found within it. The hacker can then make changes to the attack by taking the computer from the connection and assume their authentication.

C. Levels of Session Hijacking

There are two levels of session hijacking, this are the platform by which attacker use to gain access to the session id.They are network level and Application level.

i. **Network level:** It is the interruption of packets transmitted between the user and server through User Datagram protocol (UDP) session. The appliance level means gaining a session IDs to achieve UDP management as presented by the web application. The network session hijacking are classified as TCP Hijacking and UDP Hijacking.

ii. **Application level:** This level is concerned about hijacking established sessions but also try to create new session to take advantage. Application level of session hijacking focuses on gaining or obtaining an already established session ID by using some attack techniques, then uses the session ID to create an innovative session. It tries to work out identity in order to access the server from the application level.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 1, January 2021

DOI 10.17148/IJARCCE.2021.10104

D. Detection tools for Session Hijacking:

To protect against Session Hijacking there are various intrusion detection tools. The below are few commonly used tools:[16]

- **Arp-ON**: This tool is used to secure the Address resolution protocol,and avoid any MITM attacks.(Darknet,2000)
- **ARP-PING**:This is a Linux tool,and allows a user to ping a Media Access Control(MAC) directly.This can implemented to detect the attacker using a sniffer on the network
- **ANTI-SNIFF**:in this tool the user can detect any sniffer on the network used for packet capturing.(Storm-2011)
- **Cookie-Monster:** This tool was developed for analyzing the strength of the cookie by archiving and analyzing.(Pauli,Engebretson,Ham & Zautke,2011)

E. Prevention techniques used for Session Hijacking[18]

- **Encryption**: This is mostly used by e-commerce services to encode information in order to prevent from unauthorized user.
- **Use of a protracted random variety or string because the session key**: It is also been used to prevent application level breaches. It limit the opportunity of attacker guessing a session ID or way of trial and error or to suddenly hijack by using passphrases with the hope of guessing rightly
- **Regenerating the session id once a fortunate login**: This automatically create a session ID of the user once gained access to the server. This limit the attacker in hijacking a valid user session ID.
- **Making secondary checks:** This ensures a double check to validate the authentication of the user that logged in and the user currently using the session. The information request must matches with the right user and ensures delivery to the appropriate channel.
- **Changing the cookie value:** Some services can modify the worth of the cookie with users demand in the server. This will enable web services to spot if an attack has been launched but this can result to some technical problems.

F. Some Tools Used in Session Hijacking

Part of the tools used to carry out session Hijacking are:

- Wire shark
- Ethereal
- Juggernaut
- Hunt

III.METHODOLOGY

This session is centred on the system architecture to prevent session hijacking in a web application, the various component of the system and session hijacking module was explained The system architecture will therefore help to detect and prevent session hijacking in order to make user records more confidential, secure and reliable. Figure 4 shows the system architectural model for the detection and prevention of session hijacking in a web application.

A. System components

Web application are programs that runs on the web server. User of a web application uses web browser to access the server and then establish session. Hypertext Transfer Protocol (HTTP) enable the user to request for information from the server through the browser. User requests a web page from the server to fetch information and this respond to the HTTP which is identified by the session created. The session ID is uniquely identified on the web. Figure 4 maintain the database table and respond to cookies by the previous action of the user, the request consist of the session ID and also the cookies.

B. Session hijacking prevention module

i. **Session ID creation using rigid algorithm:** Fragile/Short session ID's can be expose to attacks. The application of cryptographic algorithm can enable us to detect the attack. The attacker can study the session ID generation to drawn knowledge in creating a new session.

ii. **Timing out Sessions:** If the system is left idle and user didn't perform any operation on it and did not log out. Attacker can steal the session ID and thereby hijack the session. It is therefore necessary for user to timeout after a constant period of time if idleness to prevent from attack.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 1, January 2021

DOI 10.17148/IJARCCE.2021.10104

iii. **Forcing Re-authentication:** This module enable user to access the system after a constant period of time to re- login. Here, the session ID is recreated and connection established. The previous session ID becomes outdated and it is therefore no longer useful for the attacker.

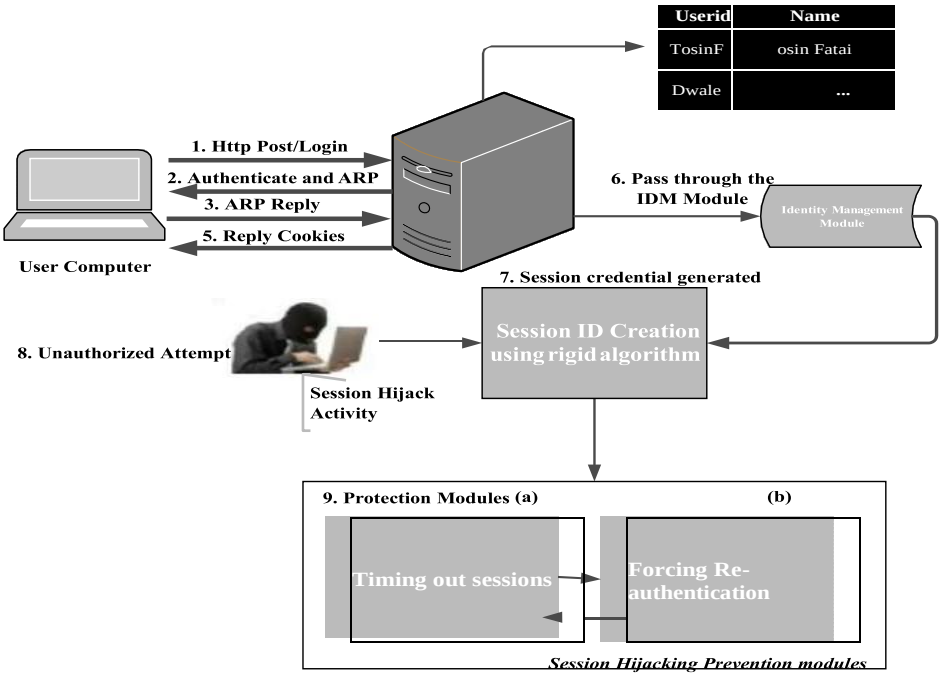

Figure 4: System architecture for session Hijacking Detection and Prevention

IV. SYSTEM MAINTENANCE

The following are ways that could be used to keep this information system maintened.

i. Ensure that every user uses a password that can be easily remembered but strong and must not be revealed to ensure maximum security.

ii. The system's administrator should publish data input deadlines for the processing period.

iii. Any deviation in the function of the system must be immediately reported to a system analyst for ratification.

iv. An up-to-date antivirus must be installed on every system that uses the application.

v. There must be stable power supply or UPS so as to be able to operate the information system as at any time required especially during result collation and checking.

V.CONCLUSION

Session hijacking is a serious issue that every web user and organization need to place priority on in securing their information on the web. This research paper provides the information on the vulnerabilities of using the web application and the attack that may be encountered by unauthorized user to cause damage to confidential information. The paper presented various types of session hijacking and how the attack is been done affect the operation on the web The techniques for preventing session hijacking and the tools used by attacker in carrying out destructive act on the web were discussed. Previous literature shows that, there are still vulnerabilities in an on transactions and these calls for an urgent need to put in place a high level of security in web applications in protecting individual records from attacks. The research also presented an architectural model that were used as a blueprint for the development of the e-commerce website to optimally detect and prevent session hijacking in a web application.

VI. FUTURE WORK

The network strategy can be implemented with different and more generic approach which can be applicable to multiple platforms.As of now critical parameter used to detect and make decision is the IP address,but for the future,to increase the security check and compare the User Agent String,Session ID,Session created time.

ACKNOWLEDGMENT

We want to thank the management of Bharati Vidyapeeth Institute of Technology for providing an enabling environment and other contributors in developing the web application.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 1, January 2021

DOI 10.17148/IJARCCE.2021.10104

REFERENCES

[1] A. Alzahrani, A. Alqazzaz, Y. Zhu, H. Fu, and N. Almashfi, "Web application security tools analysis," in 2017 ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids), 2017, pp. 237–242.
[2] V. S. Subrahmanian, M. Ovelgonne, T. Dumitras, and B. A. Prakash, "The Global Cyber-Vulnerability Report,"2015.
[3] N. Nikiforakis, W. Meert, Y. Younan, M. Johns, and W. Joosen, "SessionShield: Lightweight protection against session hijacking," in International Symposium on Engineering Secure Software and Systems, 2011, pp. 87–100.
[4] S. Calzavara, A. Rabitti, and M. Bugliesi, "Sub-session hijacking on the web: Root causes and prevention," J. Comput. Secur., vol. 27, no. 2, pp. 233–257, 2019.
[5] K. D'silva, J. Vanajakshi, K. N. Manjunath, and S. Prabhu, "An effective method for preventing SQL injection attack and session hijacking," in 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 2017, pp. 697–701.
[6] A. M. Sathiyaseelan, V. Joseph, and A. Srinivasaraghavan, "A proposed system for preventing session hijacking with modified one-time cookies," in 2017 International Conference on Big Data Analytics and Computational Intelligence (ICBDAC), 2017, pp. 451–454.
[7] J. J. Calixto and F. S. Ferraz, "An Analysis of Seven Concepts and Design Flaws in Identity Management Systems," 2015.
[8] S. S. Manivannan and E. Sathiyamoorthy, "A prevention model for session hijack attacks in wireless networks using strong and encrypted session ID," Cybern. Inf. Technol., vol. 14, no. 3, pp. 46–60, 2014.
[9] S. Wedman, A. Tetmeyer, and H. Saiedian, "An analytical study of web application session management mechanisms and HTTP session hijacking attacks," Inf. Secur. J. A Glob. Perspect., vol. 22, no. 2, pp. 55–67, 2013.
[10] A. K. Bharti and M. Chaudhary, "Prevention of Session Hijacking and Ipspoofing with Sensor Nodes and Cryptographic Approach," Int. J. Comput. Appl., vol. 76, no. 9, 2013.
[11] https://www.geeksforgeeks.org/session-hijacking/

[12] https://www.researchgate.net/publication/27478338_Passive_techniques_for_detecting_session_hijacking_attacks_in_IEEE_80211_wireless_networks
[13] https://www.researchgate.net/figure/Active-Session-Hijacking_fig1_325117343
[14] https://www.researchgate.net/figure/Active-Session-Hijacking_fig1_325117343
[15] S. Kamuni and S. ShreehaTejaswini, "Bhaskar," J, Dr. G. Manjunath "Wavelet Based Real Time Sess. Hijack Detect. Based Bluetooth Signal Anal. ISSN, pp. 1945–2249, 2012.
[16] https://uobrep.openrepository.com/bitstream/handle/10547/211810/louis2011.pdf?sequence=1
[17] https://en.wikipedia.org/wiki/Session_hijacking
[18] https://blog.eccouncil.org/what-is-session-hijacking-and-how-to-prevent-it/