Journal of Online Engineering Education
ISSN: 2158-9658 Volume: 14 Issue: 1s
Article Received: 24 January 2023 **Revised**: 26 March 2023 **Accepted**: 25 April 2023

The Interrelation between Cookies and Cybersecurity

[1]Neville Benny, [2]Pratik Devendra Pandey
[1]Thakur Institute of Management Studies, Career Development & Research (TIMSCDR)
Mumbai, India
Nevillebenny92@gmail.com
[2]Thakur Institute of Management Studies, Career
Development & Research (TIMSCDR)
Mumbai, India
Pandeypratik400@gmail.com

Abstract— People nowadays, according to the 21st century, are said to live in the "digital era." It's the era of technological advancement. Because there are numerous items that were not around a few decades ago but are now. Third parties may access any description of any information that pertains to a secure and individual person. Information and data from the past, present, and future are more damaging than ever. This study sheds light on some crucial issues regarding cookies, privacy, and cyber security.

The websites you visit produce cookies, which are files. They facilitate your internet experience by preserving browsing data. Cookies enable websites to keep you logged in, remember your choices, and deliver information that is appropriate for your location. Two varieties of cookies exist: The website you visit places first-party cookies on your device. In the address bar, the website is shown. Cookies from third parties are produced by other websites. Some of the pictures or advertisements you see on websites you visit are the property of these sites. Rejecting third-party cookies is a wise decision. Your browsing history might be sold to outside parties if you don't object. It may also leave you vulnerable if your personal information is shared with third parties without your consent.

Keywords — Cookies, First party cookies, Third-party cookies

I. INTRODUCTION

Many people utilise cookies, a highly significant and current piece of technology, on the Internet nowadays. Cookies are essential to the Internet experience. It was a wonderful fill-in for a minor quantity procedure that was lacking. With that, a client is able to recall the schedule for when a user may access his or her website. Online purchasing experiences, personalised user content, and truthful advertising are also preferable. However, cookies do not necessarily have security built into their architecture and may be used to understand their history and functionality.

Security is not intended for the cookie. The information's security, reliability, or integrity are not guaranteed. Two cookie characteristics, however, deserve special attention: Safe and HTTP only. When a client connects to a cookie and the request exceeds the TLS limit, Secure Load restricts cookies for secure channels only (Transport Layer Security). While doing so safeguards the cookie's privacy, it does not guarantee that an attacker will not succeed in submitting a request to a secure website. The only other attribute is for HTTP.

Hackers get access to systems and networks in order to steal sensitive and private information. These specifics might relate to the medical, financial, or another industry. Since the parties to whom the information belongs have contracts in place, maintaining the confidentiality of such information is crucial. The most challenging part is with create cyber defense system. Mainly two issues arise when creating a cyber-defense system.

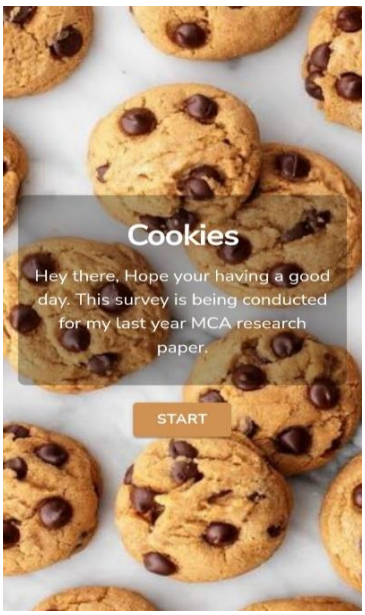
To replace "centrally-controlled policies" and enable organisations or nodes to "make informed judgements," co-ordination security exchanges cyber security knowledge from organisations or nodes. This alliance has the

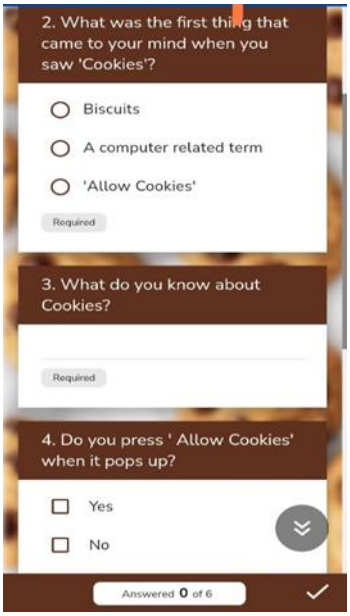
Journal of Online Engineering Education
ISSN: 2158-9658 Volume: 14 Issue: 1s
Article Received: 24 January 2023 **Revised**: 26 March 2023 **Accepted**: 25 April 2023

goal of helping you make better informed decisions. The proper choice may be made by using the information. As a result, "Collaborative Safety" refers to a collaborative effort that involves exchanging various safety data in order to give the most effective options among different safety systems. [2] Collaboration security systems have been utilised for spam, harmful malware, illegal identifications, and high security connections. Desktop and mobile contexts give rise to collaborative protection. [3].

There is a lot of information available, and the number of cybercrimes is rising daily. A robust cyber security system must be built, and unusual behaviour or anomalies should be used to predict whether it will protect the user from any offence before harming the system. This is because different computer-based learning technologies-based learning techniques attempt to gain unauthorised access to data. This may be accomplished by learning from the current dataset that contains details about different incursions or assaults and the reactions to them. The system can determine if a new incursion happens once it has finished learning from the created dataset.

II. SURVEY





III. COOKIES

The theft of sessions with the use of cookie exploitation is one of the biggest hazards to the network. When a user is searching, an HTTP cookie is a short text or data file that is delivered from a website or server and kept in the client's web browser. When a user visits a website, cookies are established, and the website utilises them to monitor the user's movements [6].

In current digital age, wireless networks are both a vital fact and a very popular technology. The main benefits of wireless networks for clients are their mobility and flexibility. The wireless networks of today are vulnerable to a number of threats. The primary risk is that cookies may take advantage of the snapshot.

When a user accesses a website, the web browser notifies the server about the user's prior behaviour and transmits a cookie value. Cookies don't have any executable code; they are just plain text. Cookies are used for a variety of website operations [7]. When a cookie is stored, the server directs the browser and returns its value with every request, making it possible to identify specific users of the information server.

A cookie is primarily used to store the data listed below, including cookie name, cookie value, cookie expiration, domain name, cookie route, and cookie security information [6]. Additionally, there are a huge variety of cookies.

Journal of Online Engineering Education
ISSN: 2158-9658 Volume: 14 Issue: 1s
Article Received: 24 January 2023 **Revised**: 26 March 2023 **Accepted**: 25 April 2023

Transient cookies, also known as session cookies, save information about the user. User session cookies are also deleted after exiting the web browser. This kind is a transient

Persistent cookies are cookies that do not disappear even after quitting the browser. Cookies that are persistent have a set expiration date and time. The user can remember their preferences and information when they visit a website by using this cookie web server [6]. This sort of cookie stores important information such login details, language, menu choices, bookmarks, and website accessibility.

Secure cookies vary primarily in that they send data after being encrypted.

Cookies only sent through HTTP Through the HTTPS protocol, only cookies are sent. This is kept on a hard disc or other user storage. Cookies that are sent through HTTP can't be protected against XSS.

Third-party cookies - These cookies are written on the relevant server but are not always visited by the user. A website that loads the page content of another website creates third-party cookies. These cookies are mostly used to track user behaviour. These cookies exchange information with advertising organisations after evaluating user activity.

Super cookie: Super cookies are stored on users' computers forever. These cookies use more modern technology independent of http cookies. The main distinction of t is that it cannot be deleted from the storage like other cookies. Super Cookies keep track of data such browser history, verification information, and advertising data.

Zombie cookie: After being deleted from a client-side script, zombie cookies are automatically created again. The user's hard disc or an internet server immediately stores the zombie cookies. Because of this, these cookies violate the browser's security and are difficult to remove .

IV. HOW COOKIES WORK

How a cookie functions is seen in the diagram above. Figure 1 demonstrates how to use a website without cookies. A web server looks for cookies when it gets a URL request from a browser. If cookies aren't available, the system produces a cookie with a special identifier for the user, embeds the website's header in the cookie, and delivers the cookie to the user. The cookie will then be stored on the user's hard disc after that. The cookie's id value is linked to the user's preferences and settings in the website database. Every time a user accesses the same website, a cookie is provided along with the URL, and the web server uses the cookie's unique id to get the user's customised preferences.

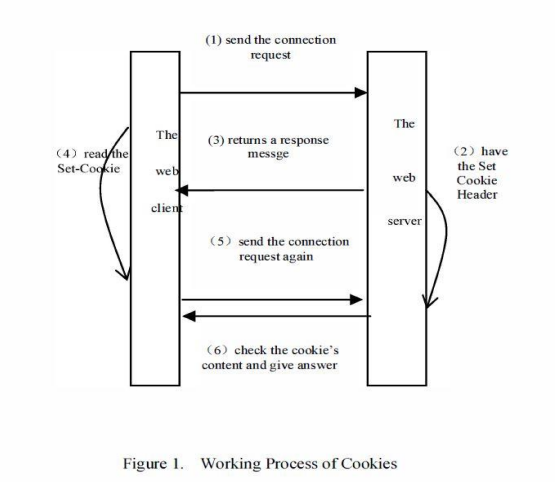


Figure 1. Working Process of Cookies

V. RISK ASSOCIATED WITH COOKIES

Attack using Cross-Site Request Forgery Since cookies are always sent along with requests, they are weak points that allow attackers to perform CSRF and send erroneous requests. The victim's privilege and the Cookie

Journal of Online Engineering Education
ISSN: 2158-9658 Volume: 14 Issue: 1s
Article Received: 24 January 2023 **Revised**: 26 March 2023 **Accepted**: 25 April 2023

that is sent in response to the attacker's request both have an influence on the CSRF vulnerability. Although the main objective of a CSRF attack isn't data extraction, state changes will almost likely have a detrimental effect on the web application being attacked. As a result, it is advised that you forego using preventative measures to safeguard your website from CSRF. Session Fixation, B The application level determines how attacks on session fixation work. In this form of assault, the attacker compels the victim to use their own or another's session ID.

By taking advantage of the cookie's browser directive route, which enables user impersonation, this is done. This tactic may be used by an attacker to trick a user into logging in as themselves on several application levels. Cybersecurity and Cookies: A Case Study Ramesh Chaudhary, Ankit Kumar Tiwari, and Naman Kumawat Cookies and Cybersecurity: A Case Study 9 www.wjrr.org Cross-site Scripting, or C. To execute a cross-site scripting attack, an attacker must save the vulnerability in a cookie. The payload will subsequently be retrieved from the cookie by the exploit vector, which will then execute the exploitation. When the cookie has already been placed, this type of attack is more challenging.

Attack by Throwing Cookies One of the most frequent types of cookie attacks is cookie throwing, which operates as follows: Let's take the case of a user that visits www.example.com and receives a domain cookie. The web server receives the cookie the following time a user accesses the same website. The cookie's absence of a route or website name is the current problem. As a result, the web server will accept both cookies if an attacker produces a subdomain cookie and sends it along with a genuine cookie. The browser can choose to send the subdomain cookie first because there is no rule mandating it to do so. if the web server receives its first cookie from the malicious subdomain.

VI. CYBER SECURITY

Cybersecurity encompasses a wide range of topics, including the use of security analytics to identify threats, the definition of organisational anti-threats requirements, the development of IT security strategies, the creation of cloud-based IT security, the migration of data to cloud-based strategies, and the maintenance of IT security platforms.

The concepts of privacy and national security are significantly impacted by the field of cyber security. At all levels, cyber dangers have been fought, and user data has been employed to safeguard users' assets. Cyber-attacks are conducted with the express purpose of being exploited [12]. These are the stages that a cyberattack goes through.

• Phase 1: As spyware, online attackers observe how the system functions across numerous programmes to identify potential targets.

Phase 2 involves infiltrating the system. The attacker may not be able to access certain services or disable the system for others as long as it can't get inside.

Phase 3: Investigating the system's resources and rights of access to the data it holds.

Phase 4: The assailant retrieves that data and snatches it along with critical data or damage.

VII. COOKIES AND PRIVACY

For a long time, the topics of cookies and privacy have dominated a variety of debates, with many people contending that cookies do not provide a privacy risk when used in certain ways. The same objection is heard from those who assert that cookies have nothing to do with system and privacy risks. In actuality, cookies do not in any way harm computer systems. They are all text files that you may disable at any time. Both of their apps and they are not plug-ins. Cookies cannot be used to propagate malware or access the hard drive of your machine. Not that cookies aren't essential for a user's online anonymity and privacy.

Journal of Online Engineering Education
ISSN: 2158-9658 Volume: 14 Issue: 1s
Article Received: 24 January 2023 **Revised**: 26 March 2023 **Accepted**: 25 April 2023

VIII. HOW COOKIES INVADE PRIVACY

Online users have described and confirmed that cookies have breached their privacy in a variety of ways. To illustrate this, it is important to utilise a real-world scenario that anyone using the Internet may encounter, such as walking into a restaurant or a hotel. The security guards at the entry halt one and request that they do a thorough search. They make a list of everything they find with you and make notes on what they find. As if that weren't enough, there are covert cameras that capture every motion and activity a person makes. The operation of cookies is comparable to this illustration. Cookies collect data about browsing actions.

Regarding the implicated parties' privacy, this is seen as a serious matter of concern. Cookies provide unending adverts that, aside from ending frustrating surfing sessions, may entice one to look at the products being presented in addition to tracking one's browser activity. These advertisements have problems since they frequently come from the same source and there is a strong probability that something identical will be displayed. It made it impossible for anybody to examine brand-new themes or items from competing companies. Many individuals find the constant adverts that come as a result of cookies to be unsettling since they obstruct the surfing experience with pointless pop-ups.

IX. SECURITY CONCERNS

Although cookies don't directly pose security problems, there have been certain instances when cookies have indirectly raised security concerns for IT users. Numerous users often set cookies, login information, and, in some cases, session details for websites that typically utilise cookies to offer access control systems. The system is susceptible to different vulnerabilities introduced by outside parties when improper implementation occurs. When cookies are exchanged between the server and the browser, packed sniffer applications may frequently access them, gaining access to the website in issue that permits cookies.

It is fairly feasible to cheat and play ahead with a browse in sending cookies to the server through temporary subversion of the Domain name server (DNS), which is used to determine the cookies used with a certain served. Because of this vulnerability brought about by cookies, it becomes possible for someone's login credentials to be compromised.

X. HOW IMPROVING CYBERSECURITY WILL HELP.

Invasion of personal privacy and cyberattacks have grown recently. Data loss and identity theft have caused costs for both businesses and people. Despite some quick advancements in technology, there have never been any effective security enhancement techniques that answer the present security worries individuals have. However, there are several strategies that may be used to lessen risks and vulnerabilities. Reducing reliance on technology excessively is one of the greatest ways to ensure that security and privacy are improved.

This makes sure that important information doesn't get spread online. Utilizing modern technologies to manage incidents is a crucial method to improve privacy and security. This calls for utilising the most recent technologies and tackling security issues. Antimalware software can assist in identifying cookies that are designed to steal personal data.

XI. CONCLUSION

Computer cookies can only store data in a few distinct ways, despite the fact that they are virtually safe. They are unable to independently access computers to get personal information or divulge data. Order forms, login pages, payment pages, and other internet pages are where users upload their information to websites, not cookies. The data is then encrypted and secured against assaults using security tools such reliable socket layers (SSL). However, cookies have received harsh criticism in the past for being seen to pose a risk to user privacy. This is due to the fact that they track user activities and log browser history.

Web users are susceptible to harmful advertisements, and their information may be traced online, which presents a big problem for cybersecurity. In conclusion, one of the main issues for internet users is security. Access to a

Journal of Online Engineering Education
ISSN: 2158-9658 Volume: 14 Issue: 1s
Article Received: 24 January 2023 **Revised**: 26 March 2023 **Accepted**: 25 April 2023

patient's medical history is one area of life where privacy is relevant. While security ensures the safety of the information saved from being accessible by violating security rules, personal bio and other important information, such as credit and social security number, are also stored. On the other hand, cookies are largely used to improve how users interact with a website. They have frequently been linked to the violation of online users' privacy rights. Therefore, it's crucial to comprehend how cookies work as well.

REFERNCES

[1] "Cookies and Sessions: A Study of What They Are, How They Work, and How They Can Be Stolen," Proceedings - 2017 International Conference on Software Security and Assurance, ICSSA 2017, pp. 20-24, 2018. K. Lacroix, Y. L. Loo, and Y. B. Choi.
[2] "Privacy principles for sharing cyber security data," Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015, pp. 193–197, 2015. G. Fisk, C. Ardi, N. Pickett, J. Heidemann, M. Fisk, and C. Papadopoulos.
[3] "Privacy protecting cyber threat information sharing and learning for cyber security," S. Badsha, I. Vakilinia, and S. Sengupta, pp. 708–714, 2019.
[4] "Securing cookies with a MAC address encrypted key ring," 2nd International Conference on Networks Security, Wireless Communications, NSWCTC 2010, H. Wu, W. Chen, and Z. Ren.