International Journal of Interdisciplinary Innovative Research &Development (IJIIRD)
ISSN: 2456-236X
Vol. 05 Issue 01 | 2020

The Relationship Between Cookies and Cybersecurity

[1]Vinay Singh Dhapola
, [1]Master student, Department of MCA, Jain Deemed-to-be University, Bengaluru, Karnataka, India

ABSTRACT

One of the primary dangers to arrange is meeting commandeering which can be done with the assistance of cookie misuse. A HTTP cookie is a little bit of information or content record which is sent from a site or server and it is put away in the customer side internet browser while the client is perusing it. Cookies are made when a client visits a site and that site utilizes cookies to keep track the developments of the client. Primary dangers which are identified with cookie are a) Sniffing system traffic for cookies b) XSS assault c) Cross-site demand falsification (CSRF) Attack d) Session Fixation Attack. By utilizing any of these techniques an aggressor can discover the treat and can utilize it to complete meeting seizing.

Keywords: Cookie, XSS, CSRF, Session Fixation

1. INTRODUCTION

Remote systems have become exceptionally mainstream and significant these days. Principle points of interest of remote systems are that give versatility and adaptability to the clients or customers. The present PC systems are helpless against different kinds of assaults. One of the principle dangers to organize is meeting seizing which can be completed with the assistance of cookie abuse. A HTTP cookie is a little bit of information or content document which is sent from a site or server and it is put away in the customer side internet browser while the client is perusing it. Cookies are made when a client visits a site and that site utilizes cookies to keep track the developments of the client. Each time client visits the site, program sends the treat an incentive to the server to inform the past movement of the client to server. Cookies are plain content and don't contain any executable code. Cookies are utilized to store the different exercises of the clients on a site, for example, clicking specific catches, signing in, or recording pages' history of a site. Server trains customer side program to store this treat data and afterward send its incentive back with each solicitation. With this data server can recognize the individual clients.

For the most part treat store following data: name of the cookie, estimation of cookie, lapse date of the cookie, and substantial space name of the cookie, legitimate treat way, and security data for the cookie.

2. TYPES OF COOKIES

Various sorts of cookies which are utilized to keep up the condition of a site are given underneath:
a) Session cookie: It is likewise called a transient cookie and it contains data about a client. It is erased when the client closes the internet browser. It is put away in brief memory of the client's PC.

b) Persistent cookie: Persistent cookie isn't erased when the client closes the internet browser. It is erased at a specific date or after a specific time. With the assistance of this cookies web server recalls client's setting and data when client visit that site later. Principle data put away in this cookie is validation data, language, menu inclinations and bookmarks or top picks of visiting site.

c) Secure cookie: This cookie is scrambled when they are moved.

d) Http Only cookie: HttpOnly cookie must be utilized when transmitted by means of HTTP convention or by HTTPS convention. It is put away in client's hard drive. Fundamental favorable position of utilizing this cookie is that they can't be prepared through XSS vulnerabilities.

e) Third-party cookie: Outsider cookies are those cookies which are composed on a customer by a site that isn't really visited by the client. These kinds of cookies are made by a page that heaps the substance from another site page. Fundamental utilization of utilizing such sort of treats is following the conduct of the clients. At that point they share this data to the promoting companies.

f) Super cookie: It is a kind of program cookie that is for all time put away on a client's PC. These are utilized for following advancements that don't depend on HTTP cookie. Fundamental distinction between standard cookie and super cookie is that they can't be erased in comparative way as ordinary cookie. Super cookies additionally do a similar capacity as ordinary cookies. They are utilized to store data like perusing history, confirmation information and promotion related information.

g) Zombie cookie: These cookies are consequently reproduced in the wake of being erased by a customer side content.

1)A cookie stores the present condition of a site page of a site in the client's PC. This data assists client with exploring between the pages of site proficiently.
2) With the assistance of cookie a web server can likewise recognize the quantity of guests visiting the website.
3) Cookies can likewise store client inclinations and settings with the goal that the client visits the website again then same inclinations can be stacked again by the web server.
4) Cookies can likewise use to follow the time client spends on the site.
5) Cookies likewise permit clients to redo site to their advantage.

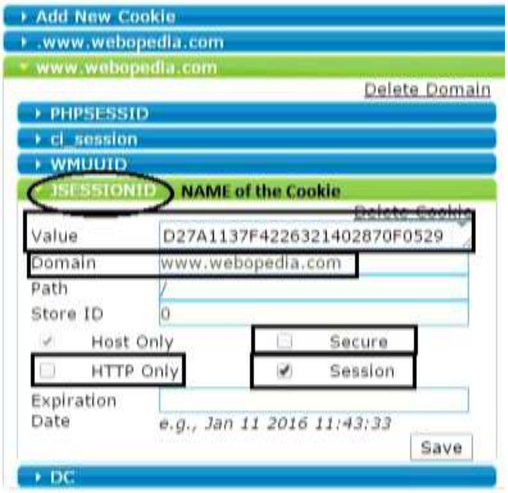
2.1 Structure of Cookie

Fundamental segments of cookie are Name and Values. Different properties of the cookies are
a) Secure: Cookie can be taken by sniffing. So to conquer this issue treat information is encoded before it sends over the system. Encoding cookie information implies if in the event that an aggressor sniffs information he/she won't have the option to understand information, accordingly guaranteeing security of cookie information. Yet at the same time these days' numerous applications scramble just login page of site and just other touchy page of site. Other solicitation for the information, for example, picture documents or little clasp records are sent without the server without utilizing encryption. In any case, cookies are likewise sent over the system with these solicitations, and an aggressor is as yet ready to sniff the information and can take meeting data from these cookies. Also a few destinations permit both kind of correspondence utilizing HTTP just as HTTPS. So in these cases it is imperative to send cookie just over HTTPS associations and not at HTTP. What's more, this is finished with the assistance of secure quality of a cookie.

b) Domain: This characteristic decides area for which this cookie is substantial or not. Path: This characteristic decides the way or URL for which the cookie is substantial. The default way for this quality is '/'. Both the above said credits are utilized to decide the extent of the cookie.

c) HTTP Only: Estimation of this credit is utilized to check whether the customer side contents are permitted to get to the cookie or not.
d) Expires: This credit is utilized to decide the time and date when the program will erase the cookie.

Picture given underneath shows the different properties of cookie.



Value D27A1137F4226321402870F0529
Domain www.webopedia.com
Path /
Store ID 0
✓ Host Only
□ Secure
□ HTTP Only
☑ Session
Expiration Date e.g., Jan 11 2016 11:43:33

Fig -1: Various Attribute of Cookies

3. WORKING OF COOKIES

At the point when a client types a url in the internet browser then the program sends a solicitation to the web server. Presently when web server gets a solicitation from the program, it first searches for the treats. On the off chance that cookie isn't there, at that point it makes a cookie with a novel id for the given solicitation and afterward passes it to the client. The cookie is put away on the client's hard plate. At that point different settings just as inclinations are additionally put away in the site database with a connect to the treat. Presently on the off chance that the client visits a similar website once more, at that point cookie is additionally sent and web server from the put away database pulls similar inclinations and provides for client.

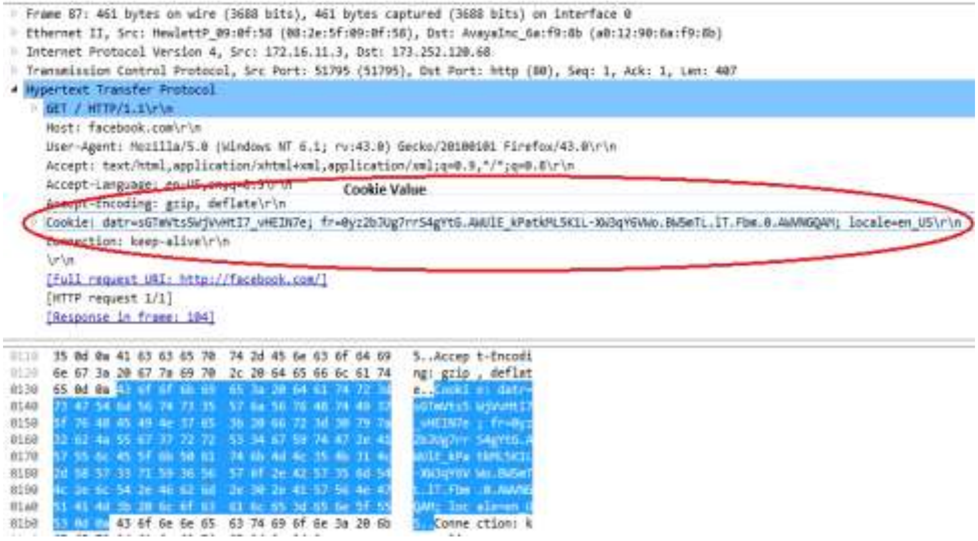
4. MAIN THREATS RELATED TO COOKIES ARE

4.1 Sniffing network traffic for cookies is: Principle virtual products which can be utilized to sniff the cookies are recorded beneath:

- Wireshark,
- kismet,
- Microsoft organize screen
- Cain and capable
- CommView

Prior all the sites were utilizing http convention and not https convention. So around then Main bundle analyzer which was utilized to sniff the cookies was wireshark. It is as yet utilized for sniffing purposes. Still there are sites which can't utilize https in appropriate manners. So wireshark can be utilized to sniff the cookies

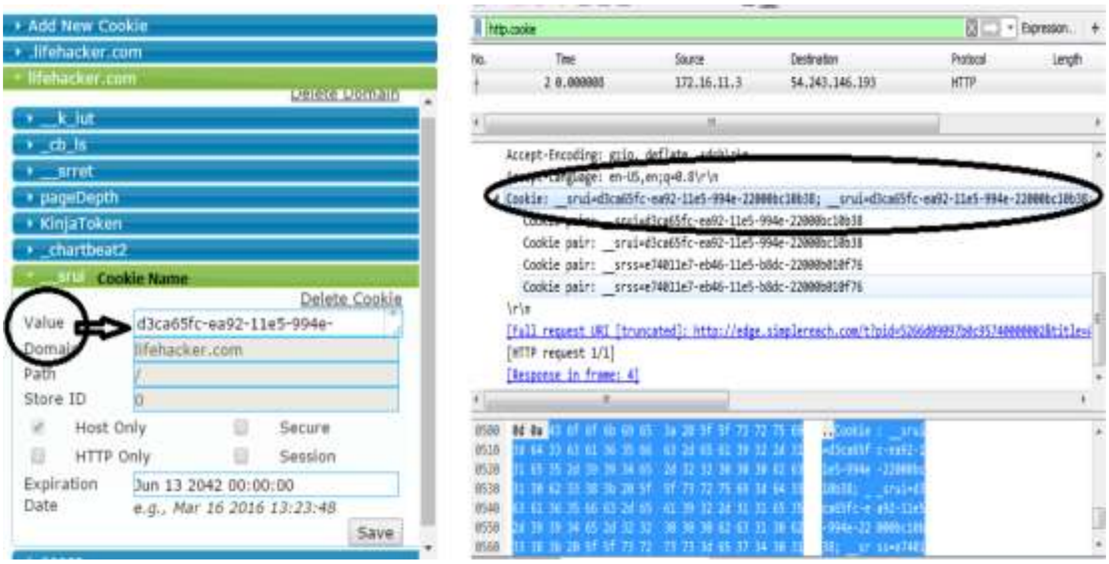
Pictures given underneath show treat sniffed by wireshark and chrome expansion.



```
Frame 87: 461 bytes on wire (3688 bits), 461 bytes captured (3688 bits) on interface 0
Ethernet II, Src: HewlettP_09:0f:58 (08:2e:5f:09:0f:58), Dst: AvayaInc_6a:f9:8b (a0:12:90:6a:f9:8b)
Internet Protocol Version 4, Src: 172.16.11.3, Dst: 173.252.120.68
Transmission Control Protocol, Src Port: 51795 (51795), Dst Port: http (80), Seq: 1, Ack: 1, Len: 407
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  Host: facebook.com\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:43.0) Gecko/20100101 Firefox/43.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Cookie: datr=sGTmVtsSwjVvHtI7_vHEIN7e; fr=0yz2bJUg7rrS4gYtG.AWUIE_kPatkML5K1L-XW3qY6VWo.BW5mTL.IT.Fbm.0.AWVNGQAM; locale=en_US\r\n
  Connection: keep-alive\r\n
  \r\n
  [Full request URI: http://facebook.com/]
  [HTTP request 1/1]
  [Response in frame: 104]

0110  35 0d 0a 41 63 63 65 70  74 2d 45 6e 63 6f 64 69   5..Accep t-Encodi
0120  6e 67 3a 20 67 7a 69 70  2c 20 64 65 66 6c 61 74   ng: gzip , deflat
0130  65 0d 0a [illegible]                               e..Cooki e: datr=
0140  [illegible]                                        sGTmVtsS wjVvHtI7
0150  [illegible]                                        _vHEIN7e ; fr=0yz
0160  [illegible]                                        2bJUg7rr S4gYtG.A
0170  [illegible]                                        WUIE_kPa tkML5K1L
0180  [illegible]                                        -XW3qY6V Wo.BW5mT
0190  [illegible]                                        L.IT.Fbm .0.AWVNG
01a0  [illegible]                                        QAM; loc ale=en_U
01b0  [illegible] 43 6f 6e 6e 65  63 74 69 6f 6e 3a 20 6b   S..Conne ction: k
```

Fig -2: Finding cookie by wireshark



Value d3ca65fc-ea92-11e5-994e-
Domain lifehacker.com
Path /
Store ID 0
☑ Host Only □ Secure
□ HTTP Only □ Session
Expiration Date Jun 13 2042 00:00:00
e.g., Mar 16 2016 13:23:48

```
http.cookie                                            Expression...  +
No.   Time        Source       Destination      Protocol   Length
2     0.000000    172.16.11.3  54.243.146.193   HTTP

Accept-Encoding: gzip, deflate, sdch\r\n
Accept-Language: en-US,en;q=0.8\r\n
Cookie: __srui=d3ca65fc-ea92-11e5-994e-22000bc10b38; __srui=d3ca65fc-ea92-11e5-994e-22000bc10b38;
  Cookie pair: __srui=d3ca65fc-ea92-11e5-994e-22000bc10b38
  Cookie pair: __srui=d3ca65fc-ea92-11e5-994e-22000bc10b38
  Cookie pair: __srss=e74011e7-eb46-11e5-b8dc-22000b010f76
  Cookie pair: __srss=e74011e7-eb46-11e5-b8dc-22000b010f76
\r\n
[Full request URI [truncated]: http://edge.simplereach.com/t?pid=5266d09997b8c95740000002&title=
[HTTP request 1/1]
[Response in frame: 4]

0500  0d 0a [illegible]     ..Cookie : __srui
0510  [illegible]           =d3ca65f c-ea92-1
0520  [illegible]           1e5-994e -22000bc
0530  [illegible]           10b38; __srui=d3
0540  [illegible]           ca65fc-e a92-11e5
0550  [illegible]           -994e-22 000bc10b
0560  [illegible]           38; __sr ss=e7401
```

Fig -3 Cookie Value by Chrome Extension and Wireshark

4.1.1 Cure

A few strategies to abstain from sniffing of cookies are given beneath:

- Encrypting information. Attempt to utilize SSL/HTTPS encryption for the whole site.
- Using a long number or string rather than modest number or string as the meeting key. So an aggressor can't animal power the meeting id.
- Changing program settings for confining cookies.
- Clearing the history and treats from the program. It very well may be finished with the assistance of program or from outsider programming like C Cleaner.

4.2 Cross-Site Scripting Attack

This strategy is likewise exceptionally regular for taking the cookies. In this sort of assault an assailant takes cookie data by making client tapping on a connection that contains a malevolent content. This content code peruses cookie data and sends this data to the assailant via mail.
There are three sorts of XSS.

a) Stored XSS
b) Reflected XSS
c) DOM-based XSS.

- Stored XSS:

For this situation an aggressor stores the malignant code for all time on the objective servers for example in a database, log record or in a remark field and so on. The casualty when explore the influenced website page then he gets the pernicious code from the server. It implies that casualties will wind up executing the pernicious code once the page is opened in the program.
The vindictive code can be in JavaScript, HTML, and Flash or in some other sort of code that the program can execute it.

- Reflected XSS:

In a reflected XSS assault, the aggressor's malignant code is a piece of the casualty's solicitation which is sent to web server. The site at that point sends this vindictive code to the casualty as a reaction. The casualty's program executes this vindictive content and sends cookies to the assailant's server.

- DOM-based XSS

DOM-based XSS is a customer side assault. DOM implies report object model and it is utilized by HTML for working with the items. At the point when a content is executed customer side program, it gives the code the DOM of the HTML page so as to get to different properties and estimations of that page. For this situation aggressor infuses the malevolent code as a major aspect of DOM and it is executed when the information is perused once again from the DOM

4.2.1 Cure

A few strategies for evacuating XSS assaults are:

- Filtering methods going outside information through a channel which will evacuate the risky catchphrases.
- Escaping methods by getting away from perilous character with the assistance of getting away from characters.

4.3 Cross-site demand imitation (CSRF) Attack

In this sort of assault an assailant powers a signed in client to play out a significant activity without his assent or information. This assault can likewise be utilized to change firewall settings, posting unapproved information or even to lead fake monetary exchanges.

4.3.1 Cure

A few techniques which are utilized or proposed for forestalling CSRF assaults are given beneath:
Using a Synchronizer token example Main Characteristics of a CSRF Token are

- It ought to be Unique for per client and per client meeting
- It ought to have enormous irregular worth
- It ought to be produced by a cryptographically secure calculation

- By checking the referrer header
- By Checking the Origin Header
- By utilizing Challenge-Response method, for example, CAPTCHA or Re-Authentication (secret phrase)

4.4 Session Fixation Attack

Meeting obsession assaults misuse the powerlessness of a framework which permits one individual to discover someone else's meeting identifier.

4.4.1 Cure

A few strategies which are utilized or proposed for forestalling Session Fixation assault are given underneath:

- Main protection is coding web applications accurately
- Regenerating another meeting identifier (SID) for each solicitation

5. CONCLUSIONS

There are many sites which are defenseless against treat robbery. In this paper different strategies which are utilized by the aggressor to take the cookies are talked about. Conceivable anticipation measures for shielding the cookies are likewise talked about.

6. REFERENCES

[1] http://www.paladion.net/cross-site-scripting-attacks/
[2] https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
[3] http://www.acunetix.com/websitesecurity/xss/
[4] http://excess-xss.com/
[5] http://www.acunetix.com/blog/articles/preventing-xss-attacks/
[6] http://resources.infosecinstitute.com/how-to-prevent-cross-site-scripting-attacks/
[7] https://www.tinfoilsecurity.com/blog/what-is-cross-site-request-forgery-csrf
[8] http://searchsoftwarequality.techtarget.com/definition/cross-site-request-forgery
[9] https://en.wikipedia.org/wiki/Cross-site_request_forgery
[10] https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet
[11] http://www.computerweekly.com/answer/Session-fixation-protection-How-to-stop-session-fixation-attacks
[12] https://en.wikipedia.org/wiki/Session_fixation
[13] https://coffeeonthekeyboard.com/best-basic-security-practices-especially-with-django-697/