International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 06 | June - 2022 Impact Factor: 7.185 ISSN: 2582-3930

IMPORTANCE OF BROWSER SECURITY

[1]SATABDI DEY, [2]CHANDRIKA M
[1]PG SCHOLAR, [2]ASSISTANT PROFESSOR
DEPARTMENT OF MCA
DAYANANDA SAGAR COLLEGE OF ENGINEERING
AFFILIATED TO VTU, BENGALURU, INDIA

Abstract

In this paper we will discuss the security issues in functionality and mechanisms supported by web browsers. A web browser is a software that allows you to access the websites which acts as a portal to the internet. Example of web browsers are Google Chrome, Internet Explorer, Mozilla Firefox, Microsoft Edge and Apple Safari. Vulnerabilities in the browser cache memory, UI of the web page, plug-in, extensions leads to possibility of variety of attacks on web browsers. The web browser which serves as a doorway to the internet is one of the most frequently used applications on mobile device or computer today. Web browser is used worldwide for variety of tasks, making it an extremely popular target for various types of attack. With increased attacks and threat, it is observed that such attacks can be halted at the setting of web browser. Thus the security aspect of web browser is an essential benchmark to safeguard user's data which could be easily accessible by the attackers.

Introduction

The web browser, most widely used application on any device connected to internet network is changing into an important platform and progressively capable for immeasurable of today's computer users. The web browser is a user's window to the world which provides an interface to perform a wide range of activity like email correspondence, social networking, shopping, professional business.

There are a number of web browsers available and different web browsers have different security settings options. These customized settings in web browser are useful and it ensures that the user's information is not vulnerable to the attackers. Browsers are an appealing target to the attacker because browsers have a huge and complex trusted computing base. Historically, every browser has contained a bug at some point which malicious website operator overcome the browser's security policy and compromise the computer of users. Having one platform to handle several functions and media types is useful for users but however it comes at the expense of security. The complexity of browser uncovers numerous points of weakness that an attacker can utilize. Few commonly exploited weaknesses of the web browser are weak antivirus, malicious redirects, DNS attacks, unsafe plugins, unblocked popups, unsafe use of save passwords from data.

Types Of Security Issues in Web Browser

- **Weak Antivirus Software and other protections:**

  Antivirus should be able to detect the possible number of malicious programs exists in the system. And weak antivirus does not provide the complete protection, they offer only basic level of protection. Threat actors are convincing increasingly in sophisticated ways to violate antivirus software, firewalls and other measures of protection.

How to prevent?

Antivirus software has been invented to prevent, remove and detect malware infections. It is necessary to install the standard antivirus on the device. User should make sure that the antivirus software updates automatically. To prevent attackers before they reach the user's browser user can implement email scanners, browser proxies and content filtering. To detect unknown threats users can provide extra layer of protection by deploying endpoint protection platform (EPP).

- **Redirects and Popups Ads:**

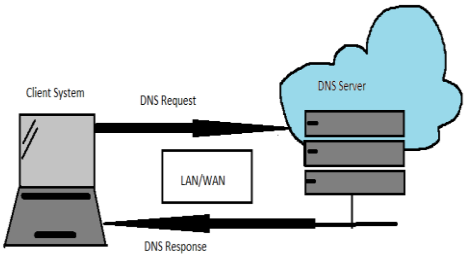
The redirects and pop-ups were used for payment and merchant gateways websites. Because of huge number of phishing websites and spammers, redirects and pop-ups were being misused a lot to hack or spam the data of the users. Threat actors commonly uses Popup *windows* to infect computers with malicious code. The popup might try and force users for accessing unsafe sites, or downloading malware. Another *common* technique is malicious redirects which takes the user from a safe web page to a malicious page.

How to prevent?

It is dangerous to keep enable the features like redirects and pop-ups for the websites. Redirects and pop-ups are helpful but suspicious and disturbing at the same time. To halt the attackers, users can use content filtering solutions to prevent malicious content for displaying to the first place of user. Web filtering can be installed at the enterprise level or on the user's device. For example, secure web gateway (SWG) can be used.

- **Communication With DNS Servers:**

DNS was created for people for connecting to services on the internet. Anyone can access and connects to a public DNS server without any authentication. When users type an address into a web browser, browser connects to DNS server to find the IP address which matches that address. The DNS server is the one which is accountable to redirect the browser to appropriate website, however attackers can disrupt the connection by directing the browser to a malicious website.



How to prevent?

Organization can use the private DNS resolver to protect against DNS attacks and should ensure it is secure. Using secure hosted DNS service is additionally an alternative choice. User ought to keep the DNS servers updated. User must use two-factor authentication if they are using a third-party DNS server

- **Saved Password and Form Info:**

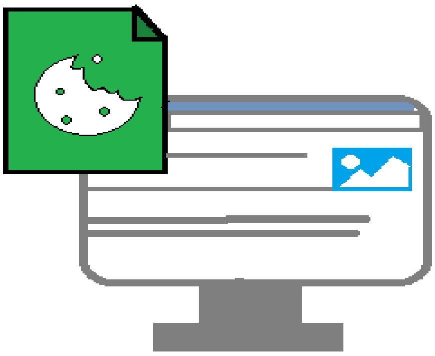
Saving the password within the web browser is a quite common mistake made by users. And if the attackers would be able to decrypt and get access to the user's computer, hackers might extract the data from the database and get access to all private logins of the user. Password protects access to systems and networks and valuable information, but many users create same weak password for many accounts and saves the password in unprotected way. If attacker manages to decrypt passwords, they can utilize these credentials to acquire unauthorized access to the entire network or, certain systems and databases.

How to prevent?

Users should not use the save password feature in the browser. Multifactor authentication (MFA) is more effective and stronger measure. User should use multifactor authentication (MFA) for everyday authentication. Multifactor authentication (MFA) uses a combination of various types of authentication techniques like OTP, SMS, emails, phone calls, hardware and software system tokens, passwords, security question, PIN etc.

- **Analysing Cookies:**

HTTP cookies are part of the modern internet but it is vulnerable to user's privacy. Cookies let the website to remember the user. Cookies stores files locally which identifies users and link them to sites. They are another potential attack vector. Cookies can reveal where user go and what user's account name is like browser history.

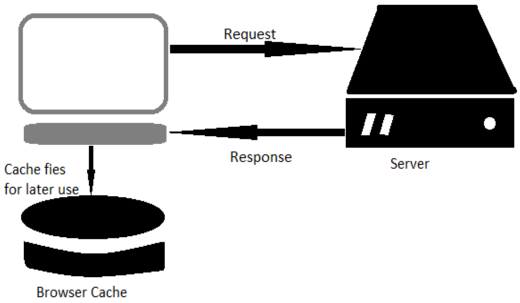


How to prevent?

A basic knowledge of cookies can help the users to keep malicious eyes off from their internet activity. A potential solution is to disable the cookies. Since many sites depends on cookies so this can be problematic if these are turned off. Instead, removing cookies systematically can help to protect user but user have to enter the information again and again as prompted by websites.

- **Exploring The Browser Cache:**

The Browser cache involves to store sections of web pages for easier access, which can figure where the user has been and what the user have seen.



How to prevent:

User should clear the cache manually as needed or incognito mode also can help user. Clearing the Browser cache is one of the best ways to flush damaging information. User should use the incognito mode i.e. the private browsing.

Handling The Issues with Browser Security

- **Secure Web Gateway:**

A secure web gateway i.e .SWG might be a cybersecurity solution that defend the system and information and helps to use security policies in a company. To achieve two main goals: to implement corporate policies for web traffic and to protect against web-based threats, Secure Web gateway (SWG) can help organizations. These solution combines few technologies such as malware scanners, URL filters, and Application controls.

- **Use HTTPS:**

Hypertext Transfer protocol Secure i.e. HTTPS that is web communication protocol and it protects the sensitive and integrity of data between the website and user's system. When user visits a website, they should check that the site uses HTTPS, which is encrypted, secure communication protocol. User should avoid using the website if the green padlock in the URL bar does not appears, or else attackers can interrupt the communication and steal user's data.

- **Keep Browsers Up-To-date:**

  User should make sure that the web browser used by them are updated because new versions of web browsers consist of built-in security features. The necessary part of browser security which should never be overlooked is keeping browser software updated.

- **Block Pop-ups and Ads:**

  Chrome is the web browser that displays pop-ups or ads on user's screen automatically. But if user doesn't want any website to redirect them, then the most effective and easiest way to disable the redirect feature. Users ought to enable built-in ability to block pop-ups in the modern browsers. To block pop-ups and ads it is better for the users to install the browser from a secure, known software system supplier.

- **Disable Auto Complete for Forms:**

  Attackers can easily detect if the user has enabled auto complete for forms. If the user remains logged into the website, attackers can hijack user's browsing session and steal user's data. So, users should disable the auto complete feature on the browser and clear the stored passwords.

Conclusion

In this paper we have discussed about the web browser security issues faced by the user and how to deal with the respective issues. The web browser is the heart of the internet. The privacy of user is incredibly necessary within the internet, however the attacker is awaiting for any possibility to steal information from users. As the usage of internet which contains sensitive data has increased so users as well as the web developers should be more concerns about the fraud, attacks and security. To give an excellently secure browser there is no silver bullet. But there are numerous techniques that browser developers can use to protect users. Users must use the right software to protect themselves. For everyday use, user must have a secure browser. User should make sure that the browser used by them values both privacy and security.

References

[1] K.M. Kren and E. Phetteplace, "Handling the Browser", Reference & User Service Quaterly, vol. 51, no. 3, pp. 210-214, 2012.

[2] cache poisoning attack, Veracode, 2018. [Online].

[3] M. Dargin, How to protect your infrastructure from DNS cache poisoning, Network World 2018. [Online]

[4] Google's Malaysian Domains Hit with DNS Cache Poisoning Attack, Oct 11, 2013.

[5] John C. Mitchell Browser security Model from the original on 20 June 2015.

[6] "Google Safe Browsing" from the original on 14 September 2014.

[7] The Browser Security: Lessons from Google Chrome. [Online]

[8] "Securing Your Web Browser" from the original on 20 April 2013.

[9] Information from:
http://en.wikipedia.org/wiki/Mozilla_Firefox

[10] The Information from:
http://addons.mozilla.org