Preventing Web Browser From Cyber Attack

Nor Fatimah Awang
Department of Computer Science
Faculty of Defence Science and Technology
Kuala Lumpur, Malaysia
norfatimah@upnm.edu.my

Arniyati Ahmad
Department of Computer Science
Faculty of Defence Science and Technology
Kuala Lumpur, Malaysia
arniyati@upnm.edu.my

Siti Rohaidah Ahmad
Department of Computer Science
Faculty of Defence Science and Technology
Kuala Lumpur, Malaysia
rohaidah@upnm.edu.my

Abstract—**Web browser has become a widely used platform for connecting and interacting people or organization with cyberspace. By using the web browser, we can share all the information, and now we can make transaction and pay our bills online. To users, they have to be careful when using internet and web browser to make all the transactions involved money as we know there are some vulnerabilities appear in web browser. This paper provides the discussion of the vulnerabilities appear in Firefox and Internet Explorer browser. It begins by providing an overview of web browser and describes what it is, how it is works, most popular web browser and common vulnerabilities found in web browser that can be used by hackers to attack the system. The paper then proposes some countermeasures to prevent the web browser from cyber attack.**

Keywords-component; web browser, vulnerabilities, countermeasures

I. INTRODUCTION

Wikipedia website defines web browser is a software application for accessing, retrieving and presenting recourses on the World Wide Web (1,2), and Hyper Text Markup Language (HTML) is a language used as a medium to deliver and display information into the web browser. In the early days of the internet, the WWW consisted only of web *sites* where containing static documents and web browsers were invented as a means of retrieving and displaying those documents. Most sites did not authenticate users, because of each user was treated in the same way and presented with the same information.

Nowadays, the World Wide Web is almost popular tools to communicate with two way communication between browser and server. Figure 1 shows how web browser works with web server using two way communication. The client requests a web page by using a web browser to the web server through HTTP and the server responds the request by content or sent an error message if unable to access. The best web server can also support server side scripting like Apache HTTP server, Java Script and PHP.

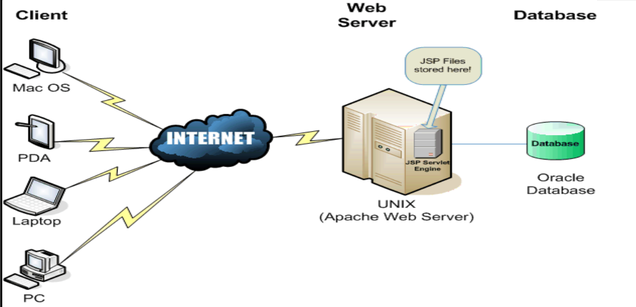


Fig. 1. Concepts of Web Browser Works

Some survey produced by Net Craff (4), the number of web sites at the end of 2010 is about 234 million and it shows that about 47 million website increase in 2010. Based on that survey, web browser has become more popular and widely used to access website and used all the features that offered by the websites. The majority of sites on the web offer registration and login, financial transactions, search, and etc. The content presented to users is generated dynamically on the fly, interacts with data repository and then presents information to the user through a web browser such as Internet Explorer (IE), Firefox, Netscape, Safari etc. Most of the information processed via web browser and web server is confidential and highly sensitive. Most of these critical systems are used on a daily basis, and there is an inherent sense of security in each of the web application (5). Therefore security is a big issue to ensure that all the information passed between web server and web browser is already secured.

II. THE MOST POPULAR WEB BROWSER

As you can see from the statistic below in Figure 2, Net Market Share has reported that Microsoft Internet Explorer and Firefox are the two most popular web browsers as of December 2010 where Internet Explorer is ahead of Firefox. In this statistics, Internet Explorer has had 57% from the usage of market share, Firefox has had 23%, Google Chrome 10% and Safari 6%.

DOI: 10.5176_2010-2283_2.1.145

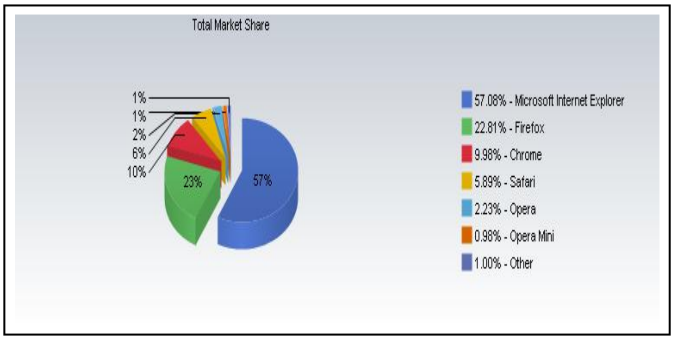


Fig. 2. Most popular Web Browser (7)

Some information related with popular web browser as stated below in Table1:

TABLE 1. MOST POPULAR WEB BROWSER

Web Browser	**Description**
Internet Explorer	Microsoft Internet Explorer or commonly known as Internet Explorer(IE) is a web browser developed by Microsoft and included as part of the Microsoft Windows line of operating systems starting in 1995 (1,2). It has been the most widely used web browser since 1999 and the latest stable version is Internet Explorer 8.
Firefox	Firefox is a popular browser for web designers because it is fairly standards compliant and even supports parts of HTML 5 and CSS 3(8). Firefox 3.6 is the most current version of this browser. Firefox is available for Linux, Macintosh, and Windows.
Safari	Safari is Apple's default web browser. Apple developed the browser for OX X and released it in 2003(3). Safari is also the default web browser on the iPhone and iPad. Safari is available for Macintosh and Windows.
Google Chrome	Chrome is a more recent browser on the scene. It is popular with designers because it has a lot of innovation as well as good support for HTML 5 and CSS 3.

III. WEB BROWSER VULNERABILITY

Web browser vulnerabilities are a serious security concern due to their role in online fraud and in the propagation of malicious code, spyware, and malware. Exploiting vulnerabilities in web browsers has become a popular way for attackers to compromise computer systems. They do that in order to take control over your computer, to steal your private information, use your computer to attack other computers, or to destroy your files and even your computer. Some of these attacks are performed by exploiting vulnerabilities in web browsers are described below :

- Third-party software may not receive security updates
- Many web sites require that users enable certain features or install more software, putting the computer at additional risk
- Many users do not know how to configure their web browsers securely
- Many users are unwilling to enable or disable functionality as required to secure their web browser
- Computer systems may be bundled with additional software that increases the number of vulnerabilities that may be attacked

As shown in Figure 3, Symantic Internet Security(9) has provided a report on total number of popular web browser vulnerabilities were found in year 2009 and 2008 where as of 2009, Firefox got highest total number of vulnerabilities compared to other popular web browsers. Firefox was affected by 169 new vulnerabilities in 2009 and this is more than the 99 vulnerabilities that were documented in 2008. In 2009, Safari was subject to 94 new vulnerabilities followed by Internet Explorer 45 vulnerabilities and Google Chrome 41 vulnerabilities.

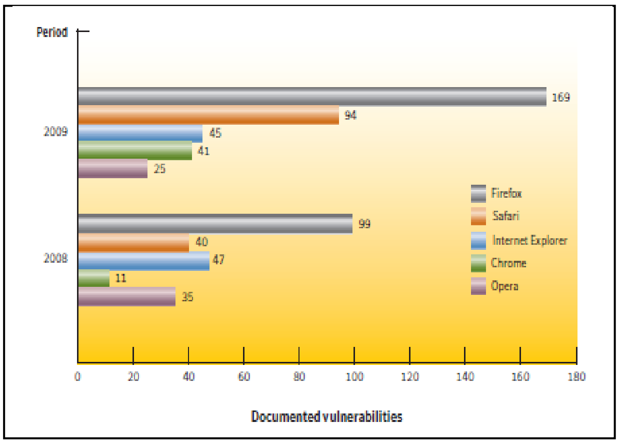


Fig. 3. Web Browser Vulnerabilities (9)

A. *Vulnerabilities Found in Firefox*

There are some vulnerabilities found in Firefox :

a) Proof of Concept Information Leak Vulnerability

This vulnerability was highlighted by researcher Gerry Eisenhaur on Jan. 19 2008 (10). This vulnerability can allow an attacker to load any JavaScript file on a machine or a server, where technically it is similar with directory traversal. The directory traversal allows the extensions directory to escape and files to be read in a predictable location on the disk. Attackers may use this method to detect the presence of files which may give an attacker information about which applications are installed.

b) Spoofing Vulnerability

A flaw has been discovered in Firefox where the URL in the address bar can be spoofed when a new window or tab is opened by a malicious web page. If a user visits a page hosting this malicious code, a new window or tab can be opened with a faked URL. There is no way of determining if the URL is authentic. This could result in the user disclosing confidential information to the malicious site, known as a phishing attack. This vulnerability is known to affect all current versions of Firefox.

c) Password Vulnerability

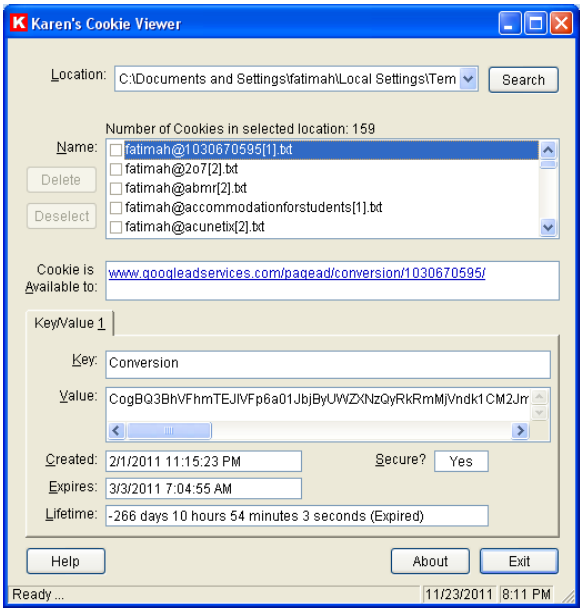
Firefox contains a password management vulnerability that can allow malicious web site to steal user password. A flaw has been identified in Firefox on July, 2010 (11), which is Javascript can be used to steal passwords from Firefox and also show how to grab other personal data from IE 6 and IE 7.

d) Add-on Security Vulnerability

An add-on called “Mozilla Sniffer” was uploaded on June 6th to addons.mozilla.org. It was discovered that this add-on contains code that intercepts login data submitted to any website, and sends this data to a remote location(12). If a user installs this add-on and submits a login form with a password field, all form data will be submitted to a remote location. Uninstalling the add-on stops this behavior. Anybody who has installed this add-on should change their passwords as soon as possible.

e) Cookies

Cookies are little pieces of information that are left on computer by web sites. Message boards use them so that a forum member does not have to log in every single time when they visit. Merchant sites use cookies to keep track of what is being added to shopping carts. Cookies also store database session or some other piece of information that allows the web site to know what transpired previously and has a Viewer as well. Refer to Figure 4, Viewer can discovers information that web sites store on user computer.



Location: C:\Documents and Settings\fatimah\Local Settings\Tem

Number of Cookies in selected location: 159

Name:
☐ fatimah@1030670595[1].txt
☐ fatimah@2o7[2].txt
☐ fatimah@abmr[2].txt
☐ fatimah@accommodationforstudents[1].txt
☐ fatimah@acunetix[2].txt

Cookie is Available to: www.googleadservices.com/pagead/conversion/1030670595/

Key: Conversion

Value: CogBQ3BhVFhmTEJlVFp6a01JbjByUWZXNzQyRkRmMjVndk1CM2Jr

Created: 2/1/2011 11:15:23 PM

Secure? Yes

Expires: 3/3/2011 7:04:55 AM

Lifetime: -266 days 10 hours 54 minutes 3 seconds (Expired)

Ready ... 11/23/2011 8:11 PM

Fig. 4. Cookie Viewer

B. *Vulnerabilities Found in Internet Explorer (IE)*

There are some vulnerabilities found in IE :

a) Redirection Information Disclosure Vulnerability

This vulnerability is caused due to an error in the handling of redirections for URLs with the “mhtml:” URI handler. This can be exploited to access documents served from another web site. Attacker can disclose potentially sensitive information using this vulnerability.

b) Allow Remote Code Execution

A flaw has been discovered in Microsoft in several Internet Explorer versions which have supposedly been used in the Chinese attack against Google and other companies. The vulnerability exists in Internet Explorer 6, Internet Explorer 7 and Internet Explorer 8(12) but the attacks seem to have been only targeting Internet Explorer 6 systems according to information posted in the vulnerability description at the Microsoft website. The vulnerability exists as an invalid pointer reference within Internet Explorer. It is possible under certain conditions for the invalid pointer to be accessed after an object is deleted. In a specially-crafted attack, in attempting to access a freed object, Internet Explorer can be caused to allow remote code execution.

c) Windows Injection Vulnerability

This vulnerability is that it allows for an attacker to inject the content of one window into the window of another site. This can be achieved if the specific target name of the window is actually known. In other words, the risks of this being exploited by malicious attackers in order to spoof the actual content of a pop-up window on a trusted site, are high(13).

IV. TESTING BROWSER VULNERABILITY

The testing was done by using BrowserCheck Online Tool(15) with involving ten computers. Each computer must have two browser installed, Internet Explorer and Firefox without knowing the browser's version.. Our results are shown in Table 2. The result shows that almost ten computers installed with insecure web browser. We identify the term 'insecure web browser with vulnerability' because of vulnerable of browsers increases significantly when the browser itself or the add-ons or plug-ins are not updated version. BrowserCheck Online Tools only check for up to date browsers as well as up to date plugins and add-ons. You may put your browser at risk or insecure if you have out-of-date versions.

Table 2: Insecure Items in Web Browser

Items	**Internet Explorer**	**Mozilla Firefox**
Adobe Flash Player	X	X
Adobe Reader 5.x and above	X	X
Adobe Shockwave Player	X	X
Apple Quicktime	X	X
Adobe Flash Player	X	X
Real Player	X	
Java Runtime	X	X

Note :X means browser at risk, outdated version

V. COUNTERMEASURES TO PREVENT

Some common countermeasures have been highlighted below to prevent web browser from cyber attacks.

A. Firefox

a) Blocking Cookies Option

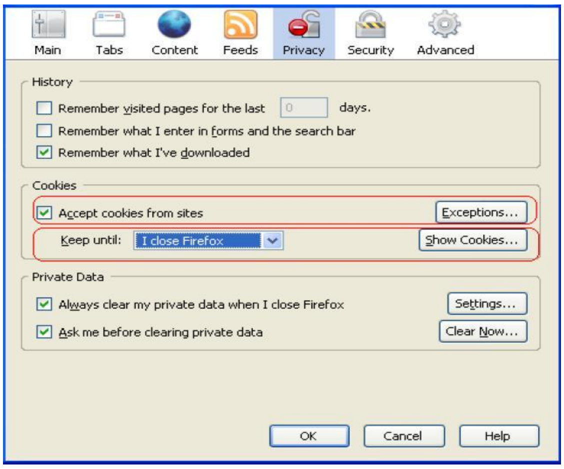
Firefox has option to block cookies whether block for single site, block cookies for all site or block third party cookies(14). Firefox can flush cookies every time the browser closes down, or users can set the date on which they want the cookies to expire. Cookies can disabled entirely but many sites require cookies to function properly.

b) Cleaning Unwanted Cookies

There is a built-in tool for cookie removal in Firefox. The sites for which the cookies are to be saved must be highlighted. There is a problem to clear out some cookies and save some others but built-in tool known as CookieCuller can be used to clean unwanted cookies.

c) Edit Privacy Setting, Security Setting and Content Setting

Under privacy section, there is an option for setting cookies. Cookies can be kept until they expire or browser is running, refer Figure 5. Under security setting, password setting can be changed as shown in Figure 6. Password can be remembered by browser with some exceptions.



History

☐ Remember visited pages for the last 0 days.

☐ Remember what I enter in forms and the search bar

☑ Remember what I've downloaded

Cookies

☑ Accept cookies from sites

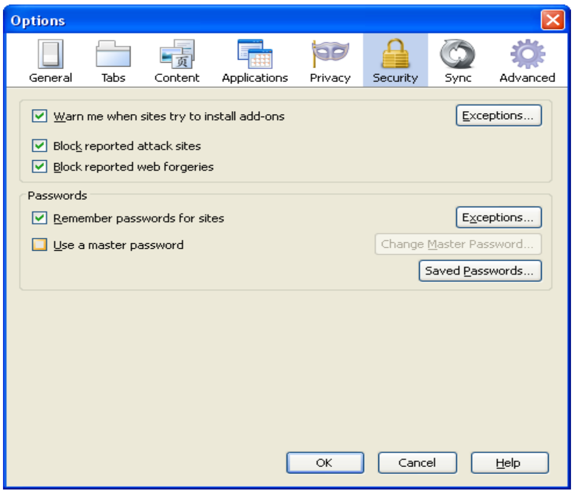
Keep until: I close Firefox

Private Data

☑ Always clear my private data when I close Firefox

☑ Ask me before clearing private data

Fig. 5. Setting Cookies



☑ Warn me when sites try to install add-ons

☑ Block reported attack sites

☑ Block reported web forgeries

Passwords

☑ Remember passwords for sites

☐ Use a master password

Fig. 6. Password Setting

d) Clear Private Data

Clear private data option is selected under tools tab in menu bar. Using this option, it will clear all the private data including browsing history, cookies, cache and passwords.

e) Prevent URL Spoofing

Users can mitigate this vulnerability by only sharing confidential information with websites that were opened from a bookmark, a trusted source, or by manually opening a new tab or window and entering a URL.

B. *Internet Explorer*

a) Security Zones

High security setting should be applied for internet zone. By selecting the High security setting, several features including ActiveX, Active scripting and Java will be disabled. With these features disabled, the browser will be more secure.

b) Trusted Sites Zone

Trusted sites are a security zone for web sites which are securely designed. It is recommended to set the security level for the Trusted sites zone to Medium when internet zone is set to high.

c) Privacy and Overwrite Automatic Cookie Handling

It is recommended to select the Advanced button and select Overwrite automatic cookie handling.

d) Specify Default Application

It is recommended to prevent the message that will display the default web browser

VI. CONCLUSION

Exploiting vulnerabilities in web browsers has become more popular way nowadays for attackers to compromise computer systems. Using web browser vulnerabilities, attacker can control over your computer, to steal your private information, use your computer to attack other computers, or to destroy your files and even your computer. Based on the statistic, Firefox is most unsecure web browser compared to Internet Explorer. To have a truly secure web browser, some recommendation for countermeasures should be followed and applied.

REFERENCES

[1] Wikipedia (2011). *Web Browser*. Retrieved from http://en.wikipedia.org/wiki/Web_browser/

[2] Wikipedia (2011). *Internet Explorer*. Retrieved from http://en.wikipedia.org/wiki/Internet_Explorer

[3] Whatis.com (2009). *Safari*. Retrieved from http://whatis.techtarget.com/definition/0,,sid9_gci1226179,00.html

[4] Net Craff. (2011). *January 2011 Web Server Survey*. Retrieved from http://news.netcraft.com/

[5] Teodoro, Serrao, *Web application Security Assessment in the Portuguese World Wide Web Panorama, 2010*

[6] Pete, (2009, November 11). *Web Browser Vulnerability Report - Firefox Leads the Pack at 44%*. Retrieved from http://prosecure.netgear.com/community/security-blog/2009/11/web-browser-vulnerability-report---firefox-leads-the-pack-at-44.php

[7] Net Market Share. (2010, December). *Browser Market Share*. Retrieved from http://www.netmarketshare.com/report.aspx?qprid=0&qptimeframe=M&qpsp=143

[8] Kyrnin, J. (2011), *Web Browser Resources*. Retrieved from http://webdesign.about.com/od/browsers/p/bl_browsers.htm

[9] Symantic Internet Security. (2010). *Symantic Internet Security Threat Report*. Retrieved from http://www.symantec.com/business/theme.jsp?themeid=threatreport

[10] Shanmuga. (2008). *Mozilla confirms Firefox proof of concept information leak vulnerability*. Retrieved from http://www.malwarehelp.org/mozilla-confirms-firefox-proof-of-concept-information-leak-vulnerability-2008.html

[11] Bort, J. (2010). *Firefox lets hackers grab your passwords*. Retrieved from http://www.networkworld.com/community/blog/firefox-lets-hackers-grab-your-passwords

[12] Martin. (2010). *Microsoft Confirms Internet Explorer Vulnerability*. Retrieved from http://www.ghacks.net/2010/01/16/microsoft-confirms-internet-explorer-vulnerability-security/

[13] Gerber, L.(2009). Don't like injections? Avoid the IE Window Injection Vulnerability. Retrieved from http://www.pc1news.com/news/0758/avoid-the-ie-window-injection-vulnerability.html

[14] Firefox Help. (2009). Blocking Cookies. Retrieved from http://support.mozilla.com/en-US/kb/Blocking%20cookies

[15] https://browsercheck.qualys.com/?scan_type=js