SCHOLARS INDIAN SCHOOL

Secure your Web Browser

The Web browser is used to gain access to information and also resources on the World Wide Web. It is a software application used to trace and display the web pages .The main purpose of a web browser is to bring the information resources to the user. The process begins with uniform resource identifier (URI) or uniform resource locator.

Uniform Resource Locator (URL)

- Consider an example of the URL :
- Each URL is divided into different sections as shown below
- **http:// -** In short, http means the hypertext transfer protocol and the file is a web page and every time you don't need to type the http, it is automatically inserted by the browser.
- **www** –World Wide Web
- **infosecawareness** – site name
- **.in** –It is one of the domains name, which is basically a country name.
- Other domain names are .com (commercial organization), .net (network domain) etc.
- (The organization address and location of the organization address are known as the domain name).
- **co.in** –suffix or global domain name shows the type of organization address and the origin of the country like the suffix co.in indicates a company in India.
- Generally a web browser connects to the web server and retrieves the information.Each web server contains the IP address, and once you are connected to the web server by using http, it reads the hyper text mark-up language (HTML) which is a language used to create document on World Wide Web in which the same document is displayed in the web browser .
- In short, a browser is an application that provides a way to look at and interact with all the information on the World Wide Web.

Understanding usage of Web Browsers

A Web browser is a software application that runs on the internet and allows viewing the web pages, as well as content, technologies, videos, music, graphics, animations and many more. In other words, a browser is an application that offers a method to look at and interact with the entire information on the World Wide Web.

Types of Web Browser

There are different types of web browsers available with different features. A web browser is a tool used not only on the personal computers, but is also used on mobile phones to access the information. There are different technologies that support web browsers like Java, frames, XHTML and many more. Web browsers are also available in different languages like English, German, Chinese, Arabic and many more .By knowing all the web browsers and their uses, it will become easier to improve the internet usage.

Risks towards Web Browser

There are increased threats from software attacks taking advantage of vulnerable web browsers. The vulnerabilities are exploited and directed at web browsers with the help of compromised or malicious websites.Exploiting vulnerabilities in web browsers have become a popular way for attackers to compromise computer systems, as many users do not know how to configure their web browser securely or are unwilling to enable or disable functionality as required to secure their web browsers.

Secure web browser

By default, a Web browser comes with an operating system, and it is set up with default configuration, which does'nt have all secure features enabled in it. There are many web browsers installed in computers like Internet explorer, Mozilla, Google Chrome, etc. that are used frequently. Not securing a web browser leads to problems caused by anything like spyware, malware, viruses, worms, etc. Being installed into a computer this may cause intruders to take control over your computer.
There is an increased fear of threat from software attacks which may take advantage of vulnerable web browsers. Some softwares of a web browser like Javascript, Active X, etc may also cause vulnerabilities to the computer system. So it is important to enable security features in the web browser you use which will minimize the risk to the computer. Web browsers are frequently updated. Depending upon the software, features and options may change.It is therefore recommended to use the updated web browser.

How to secure your web browser?

Features and Security Setting of Mozila Firefox v3.6 Browser

It is a free, open source web browser developed by Mozilla corporation .The browser can be used in different operating systems like windows, MAC, Linux, etc.

- **Anti-Phishing**

  Shop and do business safely on the Internet. Firefox gets a fresh update of web forgery sites 48 times in a day, so if you try to visit a fraudulent site that's pretending to be a site you trust (like your bank), a browser message—big as life—will stop you.

- **Anti-Malware**

  Firefox protects you from viruses, worms, trojan horses and spyware delivered over the Web. If you accidentally access an attack site, it will warn you away from the site and tell you why it isn't safe to use.

- **Anti-Virus Software**

  Firefox integrates elegantly with your Windows antivirus software. When you download a file, your computer's antivirus program automatically checks it to protect you against viruses and other malware, which could otherwise attack your computer.

- **Instant Web Site ID**

Want to be extra sure about a site's legitimacy before you make a purchase? Click on a site favicon for an instant identity overview. Another click digs deeper: how many times have you visited? Are your passwords saved? Check up on suspicious sites, avoid Web forgeries and make sure a site is what it claims to be.

- **Private Browsing**

Sometimes it's nice to go undercover, so turn this feature on and protect your browsing history. You can slip in and out of private browsing mode quickly, so it's easy to go back to what you were doing before as if nothing ever happened. It's great if you're doing your online banking on a shared computer or checking email from an Internet café.

- **customized Security Settings**

Control the level of scrutiny you'd like Firefox to give a site and enter exceptions—sites that don't need the third degree. Customize settings for passwords, cookies, loading images and installing add-ons for a fully empowered Web experience.

Enable security options

Firefox checks every part of a Web page before loading it to make sure nothing harmful is sneaking through the back door.

Security settings in a firebox control the level of examination you'd like Firefox to give a site and enter exceptions—sites that don't need the third degree. Customize settings for passwords, cookies, loading images and installing to add-ons for a fully empowered Web experience as shown below .

From the tool's menu of the firebox browser select the options and then click on the security tab.

- Under security tab enable the options like warn me when sites try to install the add-ons in and to add or remove the sites click on the exceptions tab and add or remove the sites you want.
- Enable the option tell me if the site I'm visiting is a suspected attack site.
- Enable the option tell me if the site I am using is a suspected forgery Firefox gets a fresh update of web forgery sites 48 times in a day, so if you try to visit a fraudulent site that's pretending to be a site you trust a browser prompts you a message and will stop you.
- Disable the option remember passwords for sites Firefox integrated the feature into your surfing experience. Choose to "remember" site passwords without intrusive pop-ups. Now you'll see the "remember password" notification integrated into your view at the top of the site page, and if you choose the never remember passwords for sites it will not show any notification.
- Select the advanced tab and enable the encryption tab in order to have a secure data transfer and use SSL 3.0.
- The other features are automated updates. This lets us to find the security issues and fix updates and make the safe surfing and receive automatic notification or wait until you are ready.
- Privacy settings in a Firefox control the level of examination you'd like Firefox to give a site and enter exceptions—sites that don't need the third degree. Customize settings for, cookies, Remembering passwords, downloads and History storage.
- The other features are automated updates. This lets us to find the security issues and fix updates and make the safe surfing and receive automatic notification or wait until you are ready.
- Privacy settings in a Firefox control the level of examination you'd like Firefox to give a site and enter exceptions—sites that don't need the third degree. Customize settings for, cookies, Remembering passwords, downloads and History storage.

Features and Security Setting of Internet Explorer (IE Version 8)

It is known as Microsoft Internet Explorer in short IE. It is one of the most popular web browsers and latest edition of IE is available with some of the Windows operating system like Windows XP, Windows 2003, Windows Vista and Windows 2007 .

- From the menu select tools and choose the smart screen filter and click on the turn on smart screen filter and enable the smart screen filter which is recommended, this option is used to "Avoid phishing scams and malware" .It alerts you if a site you are trying to open has been reported as unsafe.
- In the internet explorer, there is an option called "Identify fake Web addresses", this helps you to avoid false Web sites that are designed to trap you with misleading addresses. The domain name in the address bar is highlighted in black and the rest of the address is in grey to make it easy to identify a Web site's true identity.
- From the tools menu select the option, In private filtering settings, this option is used for "Browse privately". If you want to protect yourself from fraud when you use a public computer, it's a good idea to erase your tracks. In Private Browsing it is told to the Internet Explorer not to record or save your browsing history, temporary Internet files, from data, cookies, and user names and passwords?
- There is one feature in internet explorer that is "Detect malicious code". The new Cross Site Scripting (XXS) Filter helps detect malicious code that's running on compromised Web sites. This type of code is used in identity theft.
- From the tool's menu of internet explorer select the internet options and then click on the security tab and check the current security settings and change the settings of the security zone as per the necessisity.
- To change the security setting under security level move the slider up to increase the security level from a medium to high level.
- Enable the protected mode using this option, all the websites are opened in protected mode.
- To add or remove trusted or restricted websites, click on the sites option and then click on the add or remove button and enter your list of site's for the selected zone.
- Select the advanced tab and select the options as you want like enable "Use SSL 3.0, Use TLS 1.0".
- For more settings and controls click on the custom level and then select the options you want.
- In the browser settings from the menu bar click tools--> select Pop-up blocker
- Turn-on pop-up blockers. Alternatively In Internet Explorer click --> Internet Options-->Select Privacy
- Mark Turn on Pop-up Blocker as shown below

Features and Security Settings of Safari v 4.0

It is a web browser developed by Apple Corporation. It is a default web browser of MAC OS X .This browser also works on Windows XP Windows Vista and Windows 7

The following are the features of safari secure web browser

- **Phishing Protection**

Safari protects you from fraudulent Internet sites. When you visit a suspicious site, Safari warns you about its suspect nature and prevents the page from loading.

- **Malware Protection**

Safari recognizes websites that harbour malware before you visit them. If Safari identifies a dangerous page, it warns you about the suspect nature of the site.

- **Antivirus Integration**

  Thanks to support for Windows Attachment Monitor, Safari notifies your antivirus software whenever you download a file, image, application, or other item. This allows the antivirus software to scan each download for viruses and malware.

- **Secure Encryption**

  To prevent eavesdropping, forgery, and digital tampering, Safari uses encryption technology to secure your web communications. Safari supports the very latest security standards, including SSL versions 2 and 3, Transport Layer Security (TLS), 40- and 128-bit SSL encryption, and signed Java applications.

- **Automatic Updates**

  Get quick, easy access to the latest security updates. Safari takes advantage of Apple Software Update, which checks for the latest versions of Safari when you're on the Internet.

- **Pop-Up Blocking**

  By default, Safari intelligently blocks all unprompted pop-up and pop-under windows, so you can avoid distracting advertisements while you browse.

- **Cookie Blocking**

  Some companies track the cookies generated by the website you visit, so they can gather and sell information about your web activity. Safari is the first browser that blocks these tracking cookies by default, better protecting your privacy. Safari accepts cookies only from your current domain.

Features and Security Settings of Google Chrome

It is a web browser designed for a Windows operating system. This browser works on windows XP, Windows Vista, MAC OS and Linux.

The following are the features and security settings of Google chrome web browser

- From the setting menu select the Incognito window a new window appears. Pages you view from this window won't appear in your web browser history or search history. They won't leave any traces like cookies after you close the incognito window any files you download or bookmarks will be preserved.
- Chrome there is a new feature that has an own Task Manager that shows you how much memory and CPU usage each tab and plug-in is using. You can open it by clicking Shift-Esc from within Chrome or place the cursor on a window and right click and select the Task Manager. You can get more details by clicking the "Stats for nerds" link, which is on the Task Manager, and it will open a page with full details of memory and CPU usage for each process within the browser. It is used to close a bad process in one tab and won't kill your whole browser session.
- One of the features of chrome is dynamic tabs . Here you can drag tabs out of the browser to create new windows, gather multiple tabs into one window or arrange your tabs. However, you wish and it becomes quick and easy to login into the desired sites i.e. reopen the closed sites.
- The safe browsing feature in the Google Chrome displays a warning if the web address listed in the certificate doesn't match the address of the website .The following are the steps for safe browsing setting in Google Chrome.

- From the settings tab select the options and select under the hood under privacy enable the option show suggestions for navigation error.

- Enable the option use a suggestion service to help complete searches and URLS typed in the address bar.
- Enable DNS pre-fetching to improve page load performance.
- Enable the phishing and malware protection.
- Under minor tweaks enable the never save passwords.
- Under computer wide SSL settings enable the option use SSL 2.0.
- From the page menu select the create application shortcuts, this is used if you want some websites to be viewed regularly, and you may want to create application shortcuts for the desired websites that can be placed on your desktop, Start menu or quick launch menu so you can choose any one of these options .After creating, if you double-click on the shortcut icon on the desktop or start menu, the websites open in a special window that don't display tabs, buttons, address bar or menus.
- Many of the browser functions are available instead in the drop-down menu that appears when you click the page logo in the upper-right corner of the window. If you click a link that takes you to a different website, the link opens in a standard Google Chrome window so you won't lose track of your website.