# Study & Analysis of different security vulnerability issues in popular web browsers

Harish Singh Baghel, Dr. Bharat Mishra, Pramod Singh
M.G.C.G.V, Physical science Deptt. Chitrakoot Satna(M.P)

## Abstract

*In the designing of the web browsers, security plays a vital role in accessing of data from the unauthorised users in the network. The security threats can be performed by the external and the internal users. An external security threats occurs when someone from the outside can access the network. An internal security threats occurs when someone from the inside can access the network in an unauthorised manner. Today many new browsers has launched in the market and hence the chances of attackers and hackers has increased, so the idea is to secure these web browsers from different types of attackers and hackers such the security issues in the web browsers has been increased to make these browsers popular. Here in this paper we study and analyse the various security vulnerabilities possible in web browsers and how these vulnerabilities can be reduced in the popular web browsers.*

## 1. Introduction

From the cellular phone to the desktop, the web browser has become a ubiquitous piece of software in modern computing devices. These same browsers have become increasingly complex over the years, not only parsing plaintext and HTML, but images, videos and other complex protocols and file formats. Modern complexities have brought along security vulnerabilities, which in turn attracted malware authors and criminals to exploit the vulnerabilities and compromise end-user systems. This paper attempts to show and contrast the current protocol posture of various major web browsers.

These browsers are the popular web browser because of following parameters:

- Operating system support
- Accessibility features
- Acid score
- HTML support
- Mobile web technology support
- Plugins and syndicated content support
- JavaScript support
- Protocol support
- Image format support
- Security and vulnerability

### Mozilla Firefox

Firefox is an open-source project that is managed by the Mozilla Foundation. Each component is divided into submodules. Each of these modules is owned by a specific individual that is in charge of managing the development of that that module. It descended from Mozilla Corporation suite and is managed by Mozilla Corporation. Firefox includes tabbed browsing, a spell checker, incremental find, live bookmarking, a download manager, and an integrated search system that uses the user's desired search engine .Functions can be added through add-ons created by third party developers, which include the No Script JavaScript disabling utility, Tab Mix Plus customizer, Foxy Tunes media player control toolbar, Adblock Plus ad blocking utility, Stumble Upon (website discovery), Foxmarks Bookmark Synchronizer (bookmark synchronizer), WOT: Web of Trust security site advisor, download enhancer, and Web Developer toolbar. With a market share of 45.5% in 2009 it is the most popular browser.

### Internet Explorer

Windows Internet Explorer (formerly Microsoft Internet Explorer; abbreviated MSIE), commonly abbreviated to IE, is a series of graphical web browser developed by Microsoft and included as part of the Microsoft Windows line of operating system starting in 1995. It has been the most widely used web browser since 1999, attaining a peak of about 95%usage during 2002 and 2003 with IE 5 and IE6 and that percentage share has declined since in the face of renewed competition from other web browser developers. Internet Explorer uses DOCTYPE sniffing to choose between "quirks mode" (renders similarly to older versions of MSIE) and standard mode (renders closer to

W3C's specifications) for HTML and CSS rendering on screen (Internet Explorer always uses standards mode for printing). It also provides its own dialect of ECMA Script called Jscript.Internet Explorer has been subjected to criticism over its limited support for open web standards.

### Google Chrome

Chrome the latest browser released in 2008 already had a market share of 3.9% in Jan 2009. Chromium is the open source project behind Google chrome. Salient Features include:

1. Task Manager for Websites

2. Visual Browser History

3. Super Clean Contextual Menus

4. Search option from the Address Bar

5. Check Memory Usage by Different Browsers

6. Reopen Website tabs that you closed by mistake

7. Launch Websites from the Start Menu / Quick Launch Bar

8. Developers claim faster speed (Sunspider and v8 benchmarks), better stability and performance and high security. Architecture of chrome provides insight into its security features. Chromium has two modules in separate protection domain: browser kernel and rendering engine. This architecture helps mitigate high severity attack without compromising the compatibility.

### Opera

Opera has market share of 2.3%. But the features of this browser get it a place in our comparison chart. Claimed to be a fast and secured browser it, has the following new features in its latest version:

- Content blocking

- Bit Torrent support

- Widgets

- Search engine editor

- Site preferences

- New installer. One package—30 languages

- Integrated source viewer

- Opera: config for advanced settings configuration

- Tab use: Thumbnails when you hover the cursor over a tab

- Widgets in Opera are more like small standalone applications that can interact with the internet and live outside the browser, rather than interface elements that can change the basic behavior of the browser, as Firefox's extensions are.

### Innovative Features in Opera

Opera was the first browser with tabs, RSS support, and built-in BitTorrent client and tab thumbnails. It allows for duplication of tabs, Goto URL feature for web address that is not hyperlinked, periodic reloading, fitting to window size (ERA), rewinding, crash recovery, page zoom, instant back, tab closing. Along with this it does the best on the Acid2 web standards test. Though the safari browser is been used more as per the statistics given above we have taken chrome and opera because chrome is the latest browser by Google which is popular and wanted to know the details of the new browser.

### Safari

Safari is a web browser developed by Apple Computer for its Mac OS X operating system. The first version was released in January 2003. The main design goals for Safari are usability, speed, standards compliance, and integration with OS X. Safari reuses the KHTML rendering engine and the KJS JavaScript interpreter from the KDE project. The modified versions are called WebCore and JavaScriptCore, and are released under the GNU Lesser General Public License (LGPL). However, the rest of Safari’s code is proprietary, including the user interface.

### Lynx

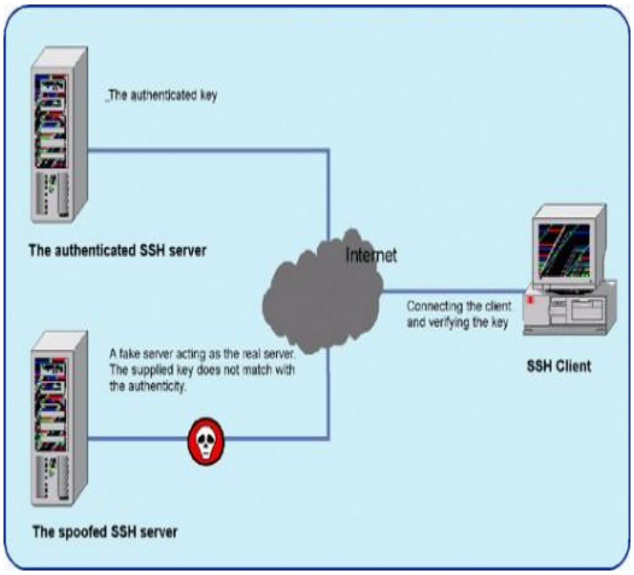
Lynx is a one of the most popular text-only browsers in use today. It predates the WWW, first serving as an interface for an “organization-wide information system.” Custom hypertext capabilities were then added, followed by support for the Gopher protocol. Finally, support for WWW protocols was grafted on, making Lynx into a true web browser. This incremental development process has resulted in a system composed of small fragments of code with no coherent overall structure. Furthermore, much of the code is low-level and platform specific, increasing its complexity.

### Netscape

Netscape Browser is the name of a proprietary Windows web browser published by AOL, but developed by Mercurial Communications. It is the eighth major release in name of the Netscape series of browsers, originally produced by the defunct Netscape Communications Corporation.

While Netscape Browser's version numbers start at 8, it is based on Mozilla Firefox, whereas Netscape 6 and 7 were based on Mozilla Application Suite, itself a complete rewrite of the codebase developed in versions 1 through 4 - Netscape Navigator and Netscape Communicator. As with other recent versions, it incorporates support for AOL Instant Messenger, and other AOL-related features.

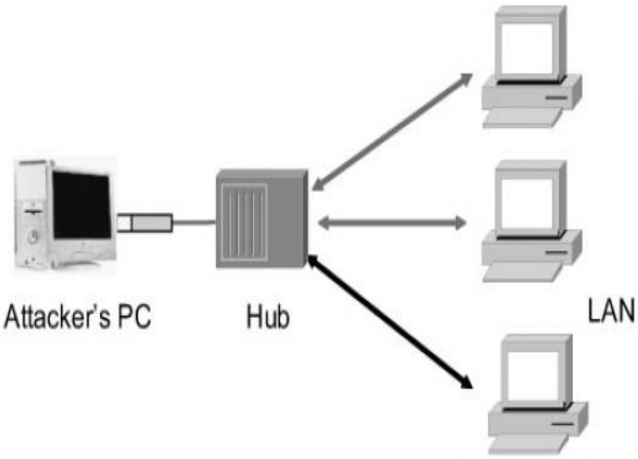
### 1. Spoofing (Identity spoofing or IP Address Spoofing)


The authenticated key
The authenticated SSH server
Internet
Connecting the client and verifying the key
SSH Client
A fake server acting as the real server. The supplied key does not match with the authenticity.
The spoofed SSH server

Any internet connected device necessarily sends IP datagram's into the network. Such internet data packets carry the sender's IP address as well as application-layer data. If the attacker obtains control over the software software running on a network device, they can then easily modify the device's protocols to place an arbitrary IP address into the data packet's source address field. This is known as IP spoofing, which makes any payload appear to come from any source. With a spoofed source IP address on a datagram, it is difficult to find the host that actually sent the datagram.

The countermeasure for spoofing is ingress filtering. Routers usually perform this. Routers that perform ingress filtering check the IP address of incoming datagrams and determine whether the source addresses that are known to be reachable via that interface. If the source addresses that are known to be reachable via that interface. If the source address is not in the valid range, then such packets will be discarded.

### 2. Sniffing



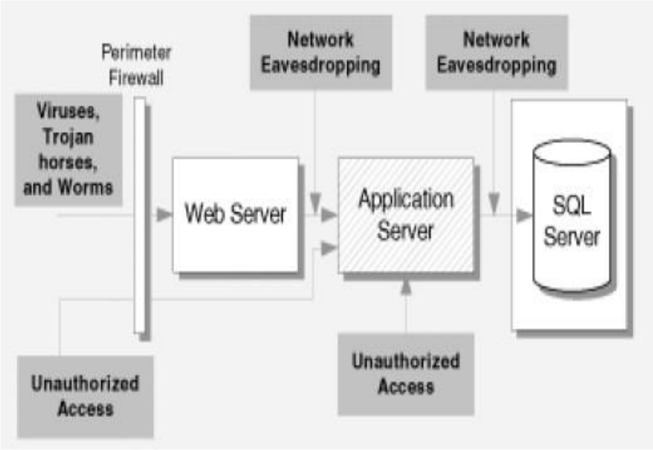
Packet sniffing is the interception of data packets traversing a network. A sniffer program works at the Ethernet layer in combination with network interface cards (NIC) to capture all traffic traveling to and from internet host site. Further, if any of the Ethernet NIC cards are in promiscuous mode, the sniffer program will pick up all communication packets floating by anywhere near the internet host site. A sniffer placed on any backbone device, inter-network link or network aggregation point will therefore be able to monitor a whole lot of traffic. Most of packet sniffers are passive and they listen all data link layer frames passing by the device's network interface. There are dozens of freely available packet sniffer programs on the internet. The more sophisticated ones allow more active intrusion.

The key to detecting packet sniffing is to detect network interfaces that are running in promiscuous mode. Sniffing can be detected two ways:

1. ***Host-based* :** Software commands exist that can be run on individual host machines to tell if the NIC is running in promiscuous mode.
2. ***Network-based* :** Solutions tend to check for the presence of running processes and log files, which sniffer programs consume a lot of. However, sophisticated intruders almost always hide their tracks by disguising the process and cleaning up the log files.

The best countermeasure against sniffing is end-to-end or user-to-user encryption.

### 3. Mapping (Eavesdropping)

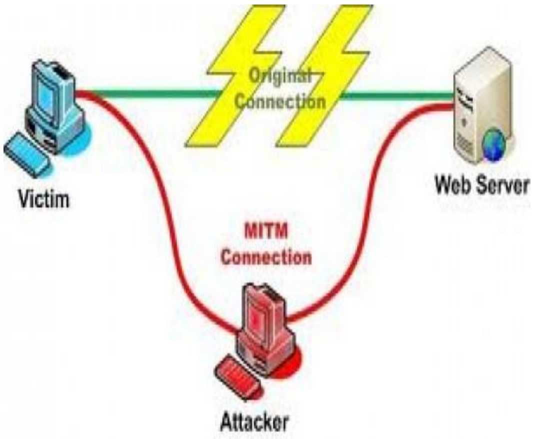


Before attacking a network, attackers would like to know the IP address of machines on the network, the operating systems they use, and the services that they offer. With this information, their attacks can be more focused and are less likely to cause alarm. The process of gathering this information is known as mapping.

In general, the majority of network communications occur in an unsecured or "clear text" format, which allows an attacker who has gained access to data paths in your network to "listen in" or interpret the traffic. When an attacker is eavesdropping on your communications, it is referred to as *sniffing* or *snooping*. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise.

Counter measures are strong encryption services that are based on cryptography only. Otherwise your data can be read by others as it traverses the network.

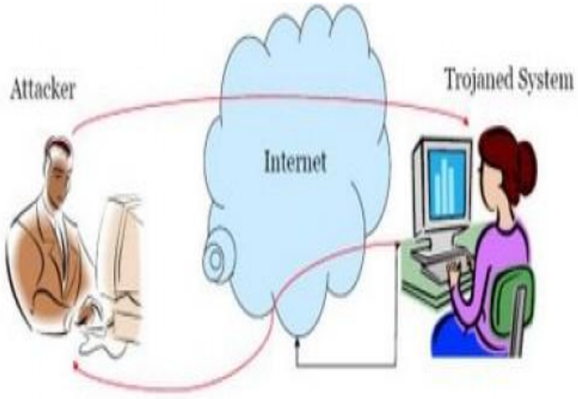
### 4. Hijacking (man-in-the-middle attack)



This is a technique that takes advantage of a weakness in the TCP/IP protocol stack, and the way headers are constructed. Hijacking occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data.

Man-in-middle attacks are like someone assuming your identity in order to read your message. The person on the other end might believe it is you, because the attacker might be actively replying as you, to keep the exchange going and gain more information.

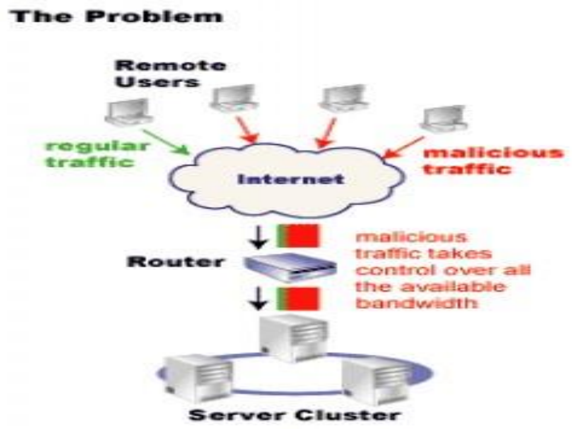
### 5. Trojans



These are programs that look like ordinary software, but actually perform unintended or malicious actions behind the scenes when launched. Most remote control spyware programs are of this type. The number of trojan techniques are only limited by the attacker's imagination. A torjanizes file will look, operate, and appear to be the same size as the compromised system file.

The only protection is early use of a *cryptographic checksum* or *binary digital signature* procedure.

### 6. Denial-of-Service attack (DoS) and Distributed-Denial-of-Service (DDoS)



A denial of service attack is a special kind of Internet attack aimed at large websites. It is a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Denial of Service can result when a system, such as a Web server, has been flooded with illegitimate requests, thus making it impossible to respond to real requests or taks. Yahoo! and e-bay were both victims of such attacks in February 2000.

A Dos attack can be perpetrated in a number of ways. There are three basic types of attack.

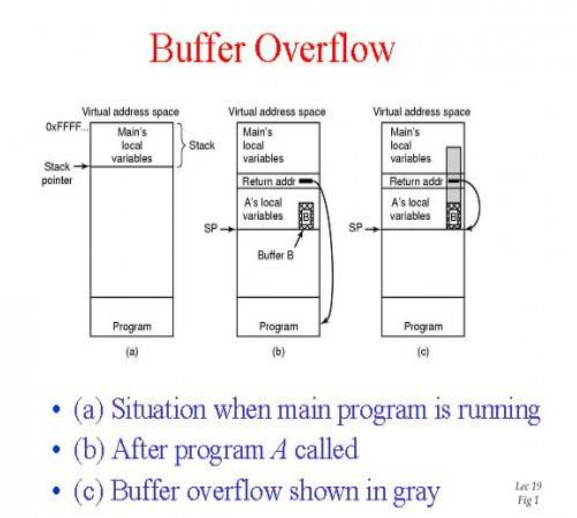
- Consumption of computational resources, such as band width, disk space or CPU time.
- Disruption of configuration information, such as routing information.
- Disruption of physical network components.

The consequences of a DoS attack are the following:

- Unusually slow network performance.
- Unavailability of a particular web site.
- Inability to access any web site.
- Dramatic increase in the amount of spam you receive in your account.

**Common forms of denial of service attacks are,**

**a) Buffer Overflow Attacks**

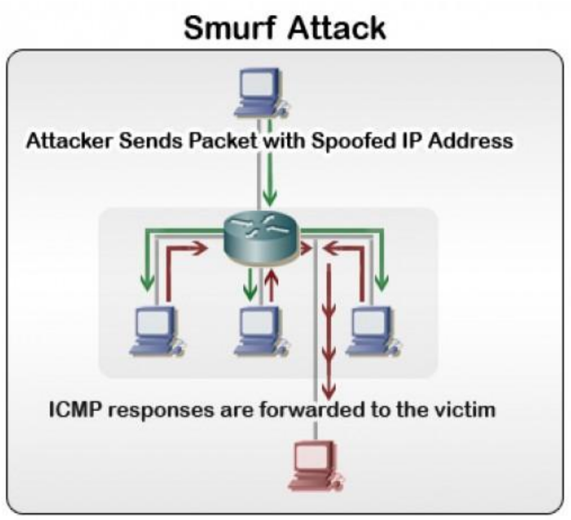

Buffer Overflow

- (a) Situation when main program is running
- (b) After program *A* called
- (c) Buffer overflow shown in gray

The most common kind of DoS attack is simply to send more traffic to a network address than the programmer's expectation on size of buffers. A few of the better known attacks based on the buffer characteristics of a program or system include:

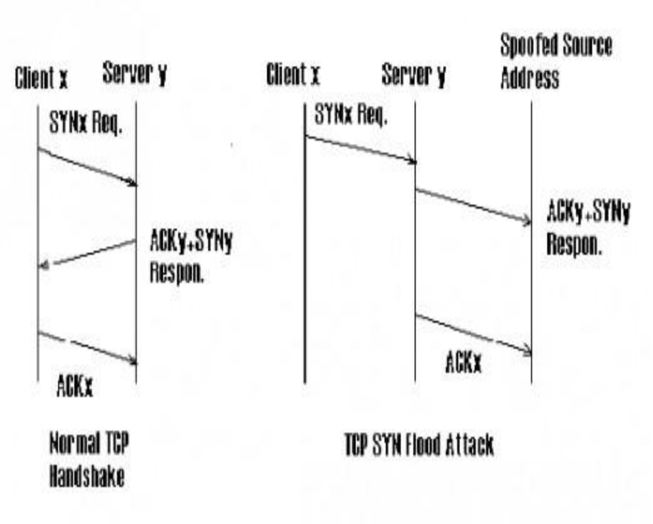
- Sending e-mail messages that have attachments with 256 character file names to Netscape and Microsoft mail programs.
- Sending over sized Internet Control Message Protocol (ICMP) packets.
- Ending to a user of an e-mail program a message with a "From" address longer than 256 characters.

**b) Smurf Attack**


Smurf Attack
Attacker Sends Packet with Spoofed IP Address
ICMP responses are forwarded to the victim

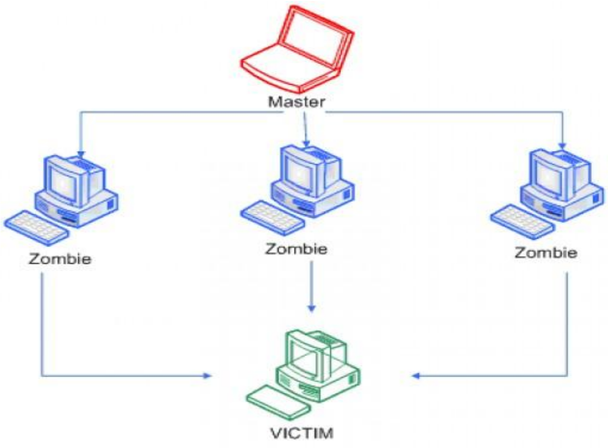
In this attack, the perpetrator sends an IP ping request to a receiving site. The ping packet specifies that, it is broadcast to a number of hosts within the receiving site's local network. The packet also indicates that the request is from another site, which is the target site that is to receive the denial of service attack. The result will be lots of ping replies flooding back to the innocent, spoofed host. If the flood is great enough, the spoofed host will no longer be able to receive or distinguish real traffic.

**c) SYN floods**



When a computer wants to make a TCP/IP connection to another computer, usually a server, an exchange of TCP/SYN and TCP/ACK packets of information occur. The computer requesting the connection, usually the client's or user's computer, sends a TCP/SYN packet which asks the server if it can connect. If the server is ready, it sends a TCP/SYN-ACK packet back to the client to say "Yes, you may connect" and reserves a space for the connection, waiting for the client to respond with a TCP/ACK packet. In a SYN flood, the address of the client is often forged so that when the server sends a TCP/SYN-ACK packet back to the client, the message is never received from client because the client either doesn't exist or wasn't expecting the packet and subsequently ignores it. This leaves the server with a dead connection, reserved for a client that will never respond. Usually this is done to one server many times in order to reserve all the connections for unresolved clients, which keeps legitimate clients from making connections.

**Distributed Denial-of-Service attacks (DDoS)**



A distributed denial of service attack (DDoS) occurs when multiple compromised sysrems or multiple attackers flood the band width or resources of a targeted system with useless traffic. These systems are compromised by attackers using a variety of methods.

In DDoS attacks, the attacker first gains access to user accounts on numerous hosts across the Internet. The attacker then installs and runs a slave program at each compromised site that quietly waits for commands from a master programs running, the master program then contacts the slave programs, instructing each of them to launch a denial-of-service attack directed at the same target host. The resulting coordinated attack is particularly devastating, since it comes from so many attacking hosts at the same time.

Here also ingress filtering only can control DoS attack and that too to a small extent.

## 2. EXISTING WORK

Internet Attack Methods and Internet Security Technology [1] in 2008 proposed the major challenging issues in the web based attacks.
Survey some attacks on client side, browser & cloud [2] in 2012 proposed on the cloud the different types of attacks and proposed that security of cloud computing become more strong if system is secure from client side attacks and web browsers attacks. When both of them is able to persist these attacks then most of security related issues of cloud have not mean.

Secure web browsing with the OP web browser [3] in 2008 proposed that the OP web browser and the different elements that make the browser secure.

## 3. Result Analysis

**Percentage usage of browsers by users**

| Year | Internet Explorer | Firefox | Chrome | Safari | Opera |
|---|---|---|---|---|---|
| 2012 | 18.5 % | 35.6 % | 39.7 % | 4.2 % | 2.2 % |
| 2011 | 23.6 % | 41.4 % | 31.3 % | 4.3 % | 2.2 % |
| 2010 | 32.3 % | 45.8 % | 17.4 % | 3.5 % | 2.1 % |
| 2009 | 40.9 % | 47.3 % | 8.4 % | 3.4 % | 2.1 % |
| 2008 | 48.5 % | 43.6 % | 3.6 % | 2.5 % | 2.0 % |

**Table 1**

As shown in the table above is the percentage usage of the popular web browsers of last five years.

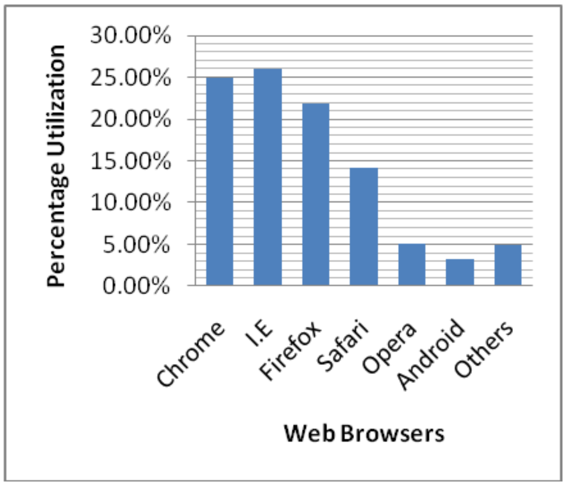


**Fig. 1**

As shown in the graph above is the percentage utilization of the modern web browsers. According to the above graph and the statically survey it was found that the Internet Explorer web browser has the highest utilization in terms of their performance and the features. The Internet Explorer contains most of the protocols integrated which increase its market share and is getting more efficient.

| Browsers | Extremely critical (number / oldest) | Highly critical (number / oldest) | Moderately critical (number / oldest) | Less critical (number / oldest) | Not critical (number / oldest) |
|---|---|---|---|---|---|
| Google Chrome 17 | 0 | 0 | 0 | 0 | 0 |
| Internet Explorer 6 | 0 | 0 | 4<br>17 November 2004;<br>7 years ago | 8<br>27 February 2004;<br>8 years ago | 12<br>5 June 2003;<br>8 years ago |
| Internet Explorer 7 | 0 | 0 | 1<br>30 October 2006;<br>5 years ago | 4<br>6 June 2006;<br>5 years ago | 9<br>5 June 2003;<br>8 years ago |
| Internet Explorer 8 | 0 | 0 | 0 | 1<br>26 February 2007;<br>5 years ago | 7<br>5 June 2003;<br>8 years ago |
| Internet Explorer 9 | 0 | 0 | 0 | 0 | 1<br>6 December 2011;<br>5 months ago |
| Firefox 12 | 0 | 0 | 0 | 0 | 0 |
| SeaMonkey 2 | 0 | 0 | 0 | 0 | 0 |

| | | | | | |
|---|---|---|---|---|---|
| Opera 11 | 0 | 0 | 0 | 0 | 1<br>6 December 2011; 5 months ago |
| Safari 5 | 0 | 0 | 1<br>7 March 2012; 2 months ago | 0 | 1<br>20 December 2011; 4 months ago |

**Table 2.**

As shown in the table 2  is the various security vulnerability issues in the web browsers.

## 4. CONCLUSION

The security in the web browsers is an important factor and during the implementation of the web browsers these can be extent to a level so that chances of effective of the web browsers has been reduced and the web browsers when used in the internet the chances of different types of attacks in the internet has been reduced.

## REFERENCES

[1] Olalekan Adeyinka School of Computing and Technology, University of East London," Internet Attack Methods and Internet Security Technology", IEEE 2008.

[2] pragya singh baghel department of computer science university of utter Pradesh lucknow,utter pradesh (india)," survey some attacks on client side, browser & cloud",2012.

[3] Chris Grier, Shuo Tang, and Samuel T. King Department of Computer Science University of Illinois at Urbana-Champaign," Secure web browsing with the OP web browser", 2008.

[4] Polsson, Ken (2011). "Chronology of PersonalComputers".http://www.islandnet.com/~kpolsson/comphist/comp1996.htm. Retrieved  in 2011.

[5] "Windows History". Microsoft. 2003. http://www.microsoft.com/windows/WinHistoryIE.mspx. Retrieved 2011.

[6] "Opera 4.0 for Windows Released" (Press release). OperaSoftware.2000.http://www.opera.com/press/releases/2000/06/27/. Retrieved 2008.
[7] Hardmeier, Sandi (2005). "The History of Internet Explorer". Microsoft. Archived from the original on [26]2009.http://web.archive.org/web/20090418194454/http://www.microsoft.com/windows/IE/community/columns/historyofie.mspx. Retrieved  2011.
[8] Berners-Lee, Tim. "Frequently asked questions - What were the first WWW browsers?". World Wide Web Consortium. http://www.w3.org/People/BernersLee/FAQ.html#browser. Retrieved  2010.
[9] Rijk (2006). "Rendering engines and code names". Tweak.OperaSoftware. http://my.opera.com/Rijk/blog/2006/rendering-engines-and-code-names. Retrieved 2008.
[10] "Microsoft Internet Explorer Web Browser Available on All Major Platforms, Offers Broadest International Support" (Press release). Microsoft. 1996. http://www.microsoft.com/presspass/press/1996/apr96/iemompr.mspx. Retrieved 2011.
[11] Håkon Wium Lie; Bert Boss. "Chapter 20 - The CSS saga".WorldWideWebConsortium. http://www.w3.org/Style/LieBos2e/history/.  Retrieved 2010.
[12] Petrie, Charles; Cailliau, Robert in 1997 "Interview Robert Cailliau on the WWW Proposal: "How It Really Happened."". Institute of Electrical and Electronics Engineers.http://www.computer.org/portal/web/computingnow/ic cailliau. Retrieved  2010.
[13] Paciello, Michael G. (2000). "Accessible Web Site Sesign.
[14] "Firefox 3.6 due this month; next comes 'Lorentz'". CNET. 2010. http://news.cnet.com/8301-30685_3-10433844-264.html. Retrieved 2010.
[15] Sink, Eric (2003). "Memoirs From the Browser Wars". Eric Weblog. http://www.ericsink.com/Browser_Wars.html. Retrieved  in 2011.

## 7. Main text

Type your main text in 10-point Times, single-spaced. Do **not** use double-spacing. All paragraphs should be indented 1/4 inch (approximately 0.5 cm). Be sure your text is fully justified—that is, flush left and flush right. Please do not place any additional blank lines between paragraphs.

**Figure and table captions** should be 10-point boldface Helvetica (or a similar sans-serif font). Callouts should be 9-point non-boldface Helvetica. Initially capitalize only the first word of each figure caption and table title. Figures and tables must be numbered separately. For example: “Figure 1. Database contexts”, “Table 1. Input data”. Figure captions are to be centered *below* the figures. Table titles are to be centered *above* the tables.

## 8. First-order headings

For example, “1. Introduction”, should be Times 12-point boldface, initially capitalized, flush left, with one blank line before, and one blank line after. Use a period (“.”) after the heading number, not a colon.

### 8.1. Second-order headings

As in this heading, they should be Times 11-point boldface, initially capitalized, flush left, with one blank line before, and one after.

**8.1.1. Third-order headings.** Third-order headings, as in this paragraph, are discouraged. However, if you must use them, use 10-point Times, boldface, initially capitalized, flush left, preceded by one blank line, followed by a period and your text on the same line.

## 9. Footnotes

Use footnotes sparingly (or not at all) and place them at the bottom of the column on the page on which they are referenced. Use Times 8-point type, single-spaced. To help your readers, avoid using footnotes altogether and include necessary peripheral observations in the text (within parentheses, if you prefer, as in this sentence).

## 10. References

List and number all bibliographical references in 9-point Times, single-spaced, at the end of your paper. When referenced in the text, enclose the citation number in square brackets, for example [1]. Where appropriate, include the name(s) of editors of referenced books.

[1] A.B. Smith, C.D. Jones, and E.F. Roberts, “Article Title”, *Journal*, Publisher, Location, Date, pp. 1-10.

[2] Jones, C.D., A.B. Smith, and E.F. Roberts, *Book Title*, Publisher, Location, Date.

## 11. Copyright forms and reprint orders

You must include your fully-completed, signed IJERT copyright release form when you submit your paper. We **must** have this form before your paper can be published in the proceedings. The copyright form is available as a Word file in author download section, <IJERT-Copyright-Agreement-Form.doc>.