Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)

Title: **WEB SECURITY: VULNERABILITY, EXPLOITS AND PREVENTION**

Chairperson: Gp Capt **Ravinder Chhatwal**, Senior Fellow, CAPS

Speaker: Mr **Arjun Subramanian P,** Associate Fellow, CAPS

Discussant: Gp Capt **PA Patil,** Senior Fellow, CAPS

Rapporteur: Ms **Shaheli Das,** Research Associate, CAPS

Date: 10 February 2016

With the internet becoming an imperative aspect of our lives, the significance of the virtual world has grown to a point where the virtual world is increasingly getting connected to the real world. Whereas the influence of internet had initially started off as aiding the functioning of individual human life, yet today, it has started exerting considerable control on human behaviour. It is on these lines that a paper was presented by Arjun Subramanian P, Associate Fellow at the Centre in a weekly seminar conducted on February 10, 2016.

Over a period of time, there has been a visible surge in the number of websites created and launched. From just one website in August 1991, the figure has shot up close to one billion in a quarter of a century. Internet Live Stats had confirmed the number as one billion in September 2014. It is with the power of knowledge on an individual and his surroundings – which are collected and stored in the servers – that the virtual domain acts 'intelligently' today, to ease our daily activities. Such information is obtained through a threefold method: (a) the user voluntarily gives information about himself and his environment, (b) obtaining information about the user without his knowledge, (c) either or both the previous methods by way of comparative analysis and extrapolation.

Web Attacks

There are cases of hundreds and thousands of websites being hacked everyday across the world. Such attacks vary from minor and mischievous attacks to major data breaches which at times bring down entire websites. Most of the attackers mount attacks on web services for fun while some have financial and business motives. Apart from these, there have also been incidents of hackers attacking specific websites with ideological and sometimes religious motives. Websites are the preferred medium of launching different types of attacks due to the wide user base. There are frequent events of hackers defacing the website of other country's government sites. A case in point is the recent incident when some Pakistani hackers defaced as many as 24 Indian government websites.

Vulnerability of Websites

The major factor for web application vulnerability is bad coding. This mainly refers to the coding practice that does not take security into consideration while building the application. Looking from a web application building company's perspective, there are multiple factors that lead to insecure codes. First, software business seeking to meet the demands of its clients within a given timeframe. During this time period the company seeks to maximise user functionality and user friendly design. As a result, very less attention is given to security. Another point to note is, extensive sanitisation coding will sometimes slow down execution speed. It is interesting to note that, a secure code sometime affects performance in terms of processing speed. This is because an extensive sanitisation process takes up processing power. Next is the problem of division of application development into multiple modules by several compartmentalised teams.

It is due to these factors that there are numerous vulnerabilities. Earlier web security only focused on securing the server side operations and executions. However, at present, the improvements in front end web building technology have also opened up multiple vulnerabilities at the client side. Broadly, website attacks maybe classified into four methods, namely SQL Injection, Cross Site Scripting (XSS),File Inclusion which can be Local File Inclusion (LFI) or Remote File Inclusion (RFI) and Denial of Service (DoS) attacks. Further, the process of vulnerability detection is done via three broad blind categories which are Boolean HTTP injection, Error based HTTP injection and Time based HTTP injection.

Counter Measures

SQL Attacks

One way of ensuring protection against SQL injection attacks is to sanitise all the inputs given by the user via any means to the database server. A key step towards ensuring security against such attacks is to take care of proper error handling during developments. This is done to prevent the attacker getting information about the server.

Cross-Site Scripting Attacks (XSS)

Websites developed during most part of the nineties could be made dynamic only with server side coding. Modern web applications, due to the advancement of web technologies, can be made dynamic from the front end as well. However, these improvements in functionality have also led to discovery of methods that can exploit the applications. Some examples of XSS attacks are: Session Hijacking and Click Jacking.

Like counter SQL injection attack injection, here too every user input needs to be properly sanitised before it is processed by the database server. Above all the script tag should be sanitised as the most common scripting is done using javascript and to a lesser extent using other languages.

File Inclusion Attacks

In such attacks vulnerability is usually created due to improper file permission setting and un-validated file uploads. However, this can be prevented by (a) setting proper validation of any file uploads (b) setting proper permissions.

Safeguards to Practice Safe Browsing

Finally, having discussed the vulnerabilities that loom large in the sphere of web security, one must follow safe browsing practices. Examples to that end are : turning off cookies, avoid clicking on unknown links and pictures, usage of a good anti-virus software, updating browser security, ensuring that one's network is protected by a good firewall, maintaining an airgap between one's personal and professional systems and lastly avoiding the usage of pirated or third party software.
