Towards Vulnerability Prevention Model for Web Browser using Interceptor Approach

Nayeem Khan, Johari Abdullah, Adnan Shahid Khan
Faculty of Computer Science & Information Technology
Universiti Malaysia Sarawak
94300 Kota Samarahan, Sarawak, Malaysia
Email: 15010049@siswa.unimas.my, {ajohari, skadnan}@fit.unimas.my

***Abstract*— Cross Site Scripting (XSS) is popular security vulnerability in modern web applications. XSS attacks are malicious scripts which are embedded by attackers into the source code of web page to be executed at client side by browsers. Researchers have proposed many techniques for detection and prevention of XSS, but eliminating XSS still remains a challenge. In this paper the authors propose a web security model for XSS vulnerability prevention for web browsers using interceptor approach. Several client and server side solution have been proposed but they degrade the browsing performance and increases configuration overheads. The proposed model is an effective solution with minimal performance overheads using both Client and Server side location in detection and prevention of XSS.**

Keywords*— Web Security; XSS; Attack; Prevention; Hybrid, Interceptor

I. INTRODUCTION

With the rapid expansion of the Internet and rich features of web application has led to many security flaws in web application. Some flaws are due to poor programming practices while some are intentionally scripted by the attackers behind the scene. Attackers are constantly working on techniques to get sensitive data through web applications. Applications which are vulnerable to malicious users can break the security and protection mechanism of the system by gaining access to personal information or taking control over system resources. The purpose of attack is to get access to personal information and system resource which may cause damage to assets of individuals and organizations. Any individual or organization which has its existence over web has some exposure of being attacked. Depending upon various factors the level of risk varies. Among the reported vulnerabilities, Open Web Application Security Project (OWASP) has ranked cross site scripting 2nd most dangerous vulnerability among top ten vulnerabilities. The first attack of XSS was reported in early 90's. Currently XSS hold a share of 43% among all the reported vulnerabilities. The target of XSS attack is Client side whereas SQL injections target server [1]. About 70% attacks are reported to occur at Application Layer Web browsers are the most susceptible application layer software for attacks. The purpose of web browser is to get the requested web resource from server and displayed in browser's windows. The format of supplied resource is not restricted to HTML but can also be PDF, image, etc. Attackers run malicious JavaScript in web browser to target users.

XSS attack is vulnerability at the application layer of network hierarchy by injecting malicious scripts to break security mechanism. XSS vulnerabilities reside at server side. Currently the solutions available either for protection against attacks for single user or for any organization is critically essential but cannot be successful in all types of web attack situations. They fail in one way or the other. The drawback with some existing approached is that they degrade the performance of the system with configuration overhead. Many researchers [2-4] have strongly backed an argument that there is no such server side approach available which can completely stop these types of attacks against users via web browsers.

Motivated with the above stated problem we are proposing a hybrid approach for detection and prevention of XSS attacks on web browsers using interceptor approach. In section II we introduce some technical background on XSS. In section III we discussed Impact of XSS attacks on Web browsers. In section IV we provide details about our proposed approach. In section V we presented some characteristics of using Interceptor. In section VI some targets to be achieved by this research are discussed. In section VII some existing approaches are discussed. Finally, section VIII concludes this paper and briefly discusses our future work

II. TECHNICAL BACKGROUND

XSS is a vulnerability that allows attackers to inject malicious code into the web page to be executed at victim's browser. If the malicious code gets successfully executed in the victims web browser then attacker takes the control of the victim's resource and sensitive data. Figure 1 depicts the principle of XSS attack. Three types of XSS are: Reflected, Stored and DOM based XSS.

A. Stored XSS (Persistent XSS)

Stored XSS occurs when malicious Java script is stored on the target server in database, guest book's message forum's etc. Figure 1 Shows Persistent XSS scenario. The malicious scripts gets executed when the user visits the malicious site thereby passing the privileges of the user to the attacker which then takes unauthorised actions without user permission.