PROTECTING TECHNIQUES AGAINST CROSS-SITE SCRIPTING ATTACKS

D. VOLODKO

Nowadays, many web sites make extensive use of client side scripts to enhance user experience. Unfortunately, this trend has also increased the popularity and frequency of cross-site scripting (CSS for short, but more often abbreviated as XSS) attacks. Cross-site scripting is an attack against web application in which scripting code is injected in to the output of an application, sent to a user browser, executed with the browser permissions and used to transfer sensitive data to a third party (i.e the attacker).

XSS protecting techniques could be divided in to client side or server side by deployment methods and dynamic or static by the type of analysis used. Dynamic server side protection example is Perl's taint mode when the flow of tainted values is tracked within the Perl interpreter [1]. Static analysis proposes to use flow-sensitive, inter-procedural and context-sensitive dataflow analysis to discover vulnerable points in a program. In addition, alias and literal analysis were employed to improve the correctness and precision of the results [2].

Client-side protection introduces an application level firewall that analyzes browsed HTML pages for hyperlinks that might lead to the leakage of sensitive data. Suspicious requests are blocked based on the analysis and generated on-the-fly rules [3]. Client-side methods of performing an in-depth and precise analysis of how sensitive values are propagated inside the user's browser. Using a combination of dynamic and static analyses, they can efficiently identify implicit information flows that purely dynamic approaches cannot identify.

XSS vulnerabilities are being discovered and disclosed at an alarming rate. XSS attacks are generally simple, but difficult to prevent because of the high flexibility that HTML encoding schemes provide to the attacker to pass through server-side/client-side input filters and there is a growing need for automated vulnerability detection in Web application development.