Automatic generation of content security policy to mitigate cross site scripting

ABSTRACT

Content Security Policy (CSP) is powerful client-side security layer that helps in mitigating and detecting wide ranges of web attacks including cross-site scripting (XSS). However, utilizing CSP by site administrators is a fallible process and may require significant changes in web application code. In this paper, we propose an approach to help site administers to overcome these limitations in order to utilize the full benefits of CSP mechanism which leads to more immune sites from XSS. The algorithm is implemented as a plugin. It does not interfere with the web application original code. The plugin can be 'installed' on any other web application with minimum efforts. The algorithm can be implemented as part of Web Server layer, not as part of the business logic layer. It can be extended to support generating CSP for contents that are modified by JavaScript after loading. Current approach inspects the static contents of URLs.

Keyword: CSP; Security; XSS