Abstract

Attacks on web applications are growing rapidly with the opening of new technologies, HTML tags and JavaScript functions. Cross-Site Scripting (XSS) vulnerabilities are being exploited by the attackers to steal web browser’s resources (cookies, credentials etc.) by injecting the malicious JavaScript code on the victim’s web applications. The existing techniques like filtering of tags and special characters, maintaining a list of vulnerable sites etc. cannot eliminate the XSS vulnerabilities completely. In this paper, initially we have tried out the experiments on the exploitation of XSS vulnerabilities using local host server (i.e. XAMPP). After this, we have investigated for the XSS vulnerabilities on social networking sites (like Facebook, Orkut, Blogs, Twitter etc.) and tried to exploit the same on blogs. Finally, on the basis of some analysis and results, we have discussed a novel technique of mitigating this XSS vulnerability by introducing a Sandbox environment on the web browser.

References

- Open Web Application Security Project: https://www.owasp.org/index.php/Top_10
- Acunetix, Vulnerability Scanner &quot;http://www.acunetix.com/vulnerability_scanner&quot;.
- Zhushou Tang, Haojin Zhu, Zhenfu Cao, Shuai Zhao, L-WMxD: Lexical Based Webmail XSS Discoverer, IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2011, pp. 976-981.

Index Terms

Computer Science

Information Sciences
Keywords

Keywords are your own designated keywords which can be used for easy location of the manuscript using any search engines.