Abstract

Web applications are useful for various online services. These web applications are becoming ubiquitous in our daily lives. They are used for multiple purposes such as e-commerce, financial services, emails, healthcare services and many other captious services. But the presence of vulnerabilities in the web application may become a serious cause for the security of the web application. A web application may contain different types of vulnerabilities. According to OWASP TOP 10 vulnerability report, Cross-site Scripting (XSS) is among top 5 vulnerabilities. So this research work aims to implement an effective solution for the prevention of cross-site scripting vulnerabilities. In this paper, we implemented a novel client-side XSS sanitizer that prevents web applications from XSS attacks. Our sanitizer is able to detect cross-site scripting vulnerabilities at the client-side. It strengthens web browser, because modern web browser do not provide any specific notification, alert or indication of security holes or vulnerabilities and their presence in the web application.

References

- Dromaeo javascript performance testing. Available at http://dromaeo.com/, JavaScript
Performance Testing.
- New international project on web vulnerabilities. Available at https://www.owasp.org/index.php, OWASP.
- Prevent xss with jsoup jsoup sanitizer. Available at http://jsoup.org/cookbook/cleaning-html/ whitelist-sanitizer, JSOUP.
Client-side Automated Sanitizer for Cross-Site Scripting Vulnerabilities

Web, WWW’06, pages 247–256, New York, NY, USA, 2006. ACM.


Index Terms

Computer Science

Information Sciences
Keywords
Web application  Cross-site scripting  Vulnerability  Sanitizer