International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 5, Issue 1, Feb 2015, 91-98

HYBRID APPROACH FOR WEB MASHUP SECURITY FRAMEWORK

VINOD SAPKAL[1] & RAVI RANDALE[2]

[1]Department of Computer Engineering, Pillai HOC College of Engineering and Technology, Maharastra, India

[2]Department of Information Technology, Pillai HOC College of Engineering and Technology, Maharastra, India

ABSTRACT

There are several innovative ways for developing software applications on the web. One of the ways is "Web Mashup". It allows users to create new web applications by integrating data and services from other web applications and data sources. Several technologies like Asynchronous JavaScript and XML (Ajax), Rich Site Summary (RSS), Representational State Transfer (REST), and Extensible Markup Language (XML) are used in creating Mashup. The numerous online available data sources and services make Mashup creation fast, easy and also rich in content. Mashup also results in spawning security concerns. A wide array of security issues arise while combining diverse content or services from diverse sources into a new environment. The security issues - User authentication, User/Data confidentiality, Session Fixation, Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), Ajax Vulnerabilities, iframe Security and Brute Force Attack are essential to be addressed. Many research papers aim at providing a security framework for User authentication, User/Data confidentiality and distribution of sensitive information while Session Fixation, Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), Ajax Vulnerabilities, iframe Security and Brute Force Attack are still ignored. The proposed framework system in the project successfully conceptualizes and implements all these attacks.

KEYWORDS: Cryptography, Privacy, Syndication Web 2.0, Mashup Security