Abstract

There has been an exponential increase in the number of attacks on web applications during the recent years. This paper presents a guideline for programmers to develop robust web applications in terms of security by identification of latest web application security vulnerabilities and devising their control using open source dynamic and static web application security assessment tools. A highly vulnerable web application is taken as a sample and it is projected to dynamic tools which lookup for security loopholes in it according to its behavior in the actual working environment and static tools lookup for security loopholes in the programming logics by static analysis of the actual source code. Finally, the concept of a static analysis monitoring tool is given which can serve a fool proof solution for one of the most encountered attack namely, Cross Site Scripting (XSS).

References

- Online Web Application Security Project (OWASP).

- Building a Web Application Security Program. Securosis, L. L. C.
- A Survey on Web Application Security. Xiaowei Li, Yuan Xue.
- An Authentication Mechanism to prevent SQL Injection Attacks by Indrani Balasundaram and E. Ramaraj. IJCA Volume 19-No. 1, April 2013.
- Cross Site Scripting: An Overview by Vishwajit S. Patil, Dr. G. R. Bamnote and Sanil S. Nair. ISDmisc 2011 Proceedings published by IJCA.

Index Terms

Computer Science  Security

Keywords

OWASP  Vulnerabilities  Web Application Security Assessment  Injection  XSS
Broken Authentication and Session Management
Insecure Direct Object References
Security Misconfiguration
CSRF
Unvalidated Redirects and Forwards