Scopus

Documents

El-Hajj, W., Ben Brahim, G., Hajj, H., Safa, H., Adaimy, R.

Security-by-construction in web applications development via database annotations
(2016) *Computers and Security*, 59, pp. 151-165. Cited 3 times.

Abstract
Huge amounts of data and personal information are being sent to and retrieved from web applications on daily basis. Every application has its own confidentiality and integrity policies. Violating these policies can have broad negative impact on the involved company's financial status, while enforcing them is very hard even for the developers with good security background. In this paper, we propose a framework that enforces security-by-construction in web applications. Minimal developer effort is required, in a sense that the developer only needs to annotate database attributes by a security class. The web application code is then converted into an intermediary representation, called Extended Program Dependence Graph (EPDG). Using the EPDG, the provided annotations are propagated to the application code and run against generic security enforcement rules that were carefully designed to detect insecure information flows as early as they occur. As a result, any violation in the data's confidentiality or integrity policies is reported. As a proof of concept, two PHP web applications, Hotel Reservation and Auction, were used for testing and validation. The proposed system was able to catch all the existing insecure information flows at their source. Apart from the proof of concept and to comprehensively test the performance of our system, we compared it to JLift, a state-of-the-art type-based system approach to detect information leaks. Both approaches were run against custom made PHP web applications and publicly available applications downloaded from SourceForge and GitHub. The results show that our approach outperforms JLift in terms of accuracy and the number of false alarms, and is able to catch the insecure flows at their source when they first occurred.

2-s2.0-84962330623
Document Type: Article
Publication Stage: Final
Source: Scopus