Securing PHP written medical websites

Daniel-Corneliu LEUCUȚA

Department of Medical Informatics and Biostatistics, Iuliu Haţieganu University of Medicine and Pharmacy, Louis Pasteur Str., no. 6, 400349 Cluj-Napoca, Romania
E-mail: dleucuta@umfcluj.ro

* Author to whom correspondence should be addressed; Tel.: +4-0264-597256, int 2502

Abstract
Medical websites, as well as patient data, and user data on medical websites, have to be secured, and effort should be put to increase the privacy of the users. PHP is one of the most used scripting languages for website development. But it is highly criticized from the security point of view. Developers should build medical PHP websites with security in mind, beside their efforts to fulfill the website purpose. The most common attacks, and security issues on PHP websites are: SQL injection attack (where an attacker tries to insert malicious code in the SQL queries); cross-site scripting (where external code is injected in the output of the website); cross-site request forgery (where unwanted commands are injected from a user that the website trusts); session hijacking (where the session ID of the user is stolen); broken authentication and access control; sensitive data exposure; error logging; using components with known vulnerabilities. Their description and ways to mitigate are presented.

Keywords:
Security; PHP; Website; Medical