Automasi Deteksi SQL Injection pada Framework CodeIgniter Menggunakan Static Analysis dan DevOps = An Automatic Detection of SQL Injection in CodeIgniter Framework using Static Analysis and DevOps

Muhammad Fahmi Al Azhar, author

Abstrak

SQL Injection adalah salah satu jenis serangan yang paling sering terjadi pada aplikasi berbasis web. Serangan ini pada umumnya terjadi karena minimnya validasi dari sisi input pada aplikasi. Meskipun penyebab terjadinya SQL Injection telah banyak diketahui, sayangnya serangan ini masih menjadi salah satu kerentanan yang sering muncul aplikasi. Penggunaan tools SAST yang digunakan selama ini seringkali tidak dapat mendeteksi adanya kerentanan SQL Injection di dalam source code, khususnya aplikasi yang menggunakan framework. Selain itu, proses pengujian yang berulang-ulang juga menjadi kesulitan tersendiri bagi tim pengembang dan keamanan aplikasi. Penelitian ini mengusulkan metode untuk mendeteksi kerentanan SQL Injection pada framework CodeIgniter.
Penelitian ini dilakukan dengan menggunakan studi kasus aplikasi berbasis PHP di instansi XYZ, khususnya pada aplikasi yang menggunakan framework CodeIgniter 3. Metode yang digunakan dalam tesis ini adalah dengan mengembangkan tool dengan nama SQLI-SA yang dapat mendeteksi kerentanan SQL Injection dengan metode static analysis. Tool ini dapat berjalan secara stand alone ataupun terintegrasi dengan platform DevOps. SQLI-SA dapat mendeteksi kerentanan SQL Injection dengan tingkat akurasi sebesar 88.8% dan dapat memberikan informasi kepada tim pengembang untuk memperbaiki source code yang terdeteksi rentan terhadap SQL Injection melalui dashboard monitoring.
.....SQL Injection is one of the most common types of attack on web-based applications. This attack generally occurs due to the lack of validation from the input side of the application. Even though the causes of SQL Injection are widely known, unfortunately, this attack is still one of the most common vulnerabilities in applications. The use of SAST tools used so far often cannot detect SQL Injection vulnerabilities in the source code, especially applications that use frameworks. In addition, the repeated testing process is also a challenge for the development team and application security. This study proposes a method for detecting SQL Injection vulnerabilities in the CodeIgniter framework.
This research was conducted using a PHP-based application case study at the XYZ agency, especially in applications that use the CodeIgniter 3 framework. The method used in this thesis is to develop a tool called SQLI-SA that can detect SQL Injection vulnerabilities using the static analysis method. This tool can run stand-alone or integrated with the DevOps platform. SQLI-SA can detect SQL Injection vulnerabilities with an accuracy rate of 88.8% and can provide information to the development team to fix source code that is detected as vulnerable to SQL Injection through the monitoring dashboard.