

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam era digital yang semakin kompleks, keamanan basis data pada website menjadi isu krusial mengingat meningkatnya risiko serangan siber, terutama melalui teknik SQL Injection. Penelitian ini berfokus pada potensi kerentanan basis data terhadap serangan SQL Injection, yang dapat dimanfaatkan oleh peretas untuk mengakses, memanipulasi, atau mencuri data sensitif. Untuk mengatasi masalah ini, penelitian ini menggunakan metode waterfall dalam implementasi "Basis Data Palsu" sebagai strategi pengamanan. Pendekatan ini didukung dengan teknik Sampling Plus Fake Data Random yang diusulkan oleh Rizvi dan Agrawal (2015), di mana data palsu disuntikkan secara acak ke dalam basis data untuk memperdaya serangan dan menghasilkan output yang tidak bermakna bagi penyerang.

Penggunaan metode ini bertujuan untuk mengurangi risiko dan dampak serangan SQL Injection, menjaga integritas data, serta melindungi kerahasiaan informasi pengguna. Penyelesaian masalah yang diharapkan adalah peningkatan keamanan basis data web pengaduan melalui pencegahan akses tidak sah dan pengacauan hasil serangan, sehingga informasi pengguna tetap aman dari pengungkapan data sensitif. Penelitian ini dilakukan menggunakan Visual Studio Code (Text Editor), Framework Laravel (Framework PHP), Bahasa Pemrograman PHP (Hypertext Preprocessor), Database MySQL, XAMPP (Web Server), SQLMap (Tools SQL Injection), dan OWASP ZAP (Tools SQL Injection).

1.2 Rumusan masalah

Berdasarkan latar belakang masalah tersebut, untuk mengetahui Implementasi Sampel Basis Data Palsu Sebagai Metode Pengamanan. Pertanyaan yang diajukan adalah:

1. Bagaimana implementasi database palsu dapat meningkatkan keamanan terhadap serangan SQL Injection pada sistem basis data web pengaduan?
2. Parameter apa saja yang digunakan untuk mengoptimalkan kinerja database palsu web pengaduan dalam menghadapi serangan SQL Injection?
3. Metode apa yang tepat untuk mengukur efektivitas database palsu pada web pengaduan dalam mencegah serangan SQL Injection?

1.3 Tujuan Penelitian

Adapun tujuan penelitian Tugas Akhir dengan kasus pengimplementasian data palsu sebagai pengamanan adalah

1. Implementasi sampel basis data palsu guna menanggulangi pencurian data dan Injeksi SQL pada tabel users web Pengaduan.
2. Mengetahui metode yang tepat untuk kontribusi penelitian yang signifikan dalam bidang keamanan basis data, khususnya dalam penerapan teknik database palsu sebagai alternatif guna mengelabui dari serangan siber.

1.4 Batasan Masalah

Berdasarkan latar belakang masalah dan metode yang dipilih, menetapkan batasan masalah sebagai berikut:

1. Pengimplementasian serangan sql injection terhadap basis data palsu menggunakan basis data mysql
2. Framework yang digunakan untuk pengujian serangan sql injection menggunakan Framework laravel
3. Pengujian serangan sql injection menggunakan tools SQLmap dan OWASP ZAP

1.5 Manfaat Penelitian

Adapun manfaat yang dapat diperoleh dari Tugas Akhir mencakup:

1.5.1 Manfaat Bagi Universitas Amikom Yogyakarta

Dapat memberikan manfaat bagi Universitas Amikom Yogyakarta dengan menyediakan sumber informasi yang berharga dan menambah pengetahuan tentang implementasi sampel basis data palsu dan pencegahan injeksi SQL sebagai metode pengamanan. Selain itu, hasil penelitian ini dapat menjadi referensi penting bagi mahasiswa dan dosen untuk melakukan pembahasan lebih lanjut serta penelitian lanjutan dalam bidang keamanan basis data, sehingga turut meningkatkan kualitas akademik dan penelitian di universitas.

1.5.2 Manfaat bagi khalayak umum

Penelitian ini bermanfaat bagi khalayak umum dengan menambah wawasan dan pemahaman tentang penerapan teknik keamanan siber, khususnya implementasi sampel basis data palsu sebagai metode pengamanan. Informasi yang diperoleh dari penelitian ini dapat membantu individu dan organisasi dalam mengadopsi langkah-langkah efektif untuk melindungi data mereka dari ancaman injeksi SQL.

1.6 Metode Penelitian

Metode yang akan diterapkan dalam pengimplementasian dalam database palsu menggunakan Metode Waterfall.

Adapun langkah-langkah metode penelitian waterfall sebagai berikut:

1.6.1 Metode Pengumpulan Data

Dalam pengumpulan data dan informasi tentang permasalahan yang dibahas, membaca dan mempelajari dokumen - dokumen, buku - buku serta sumber lainnya yang berkaitan dengan penelitian untuk dijadikan referensi.

1.6.2 Analisis Sistem

Analisis sistem adalah penguraian dari sistem informasi utuh kedalam bagian - bagian komponen dengan maksud untuk mengidentifikasi dan mengevaluasi permasalahan-permasalahan, kesempatan-kesempatan, dan hambatan-hambatan yang terjadi dan kebutuhan yang diharapkan sehingga dapat diusulkan perbaikan.

Pada tahap analisis sistem termasuk tahap pembuatan analisa kebutuhan fungsional dan non-fungsional dari sistem yang akan dibangun.

1.6.3 Perancangan

Perancangan dilakukan dengan menggunakan teknik yang mendukung untuk sistem, seperti:

- a. Data Flow Diagram (DFD) Data Flow Diagram dibuat untuk menggambarkan aliran data pada sistem yang dibangun.
- b. Desain Aplikasi dan Flowchart dibuat untuk menggambarkan alur pembuatan website Pengaduan
- c. Perancangan Basis Data dibuat untuk menggambarkan keterhubungan antara tabel tabel yang dibangun.

1.6.4 Implementasi

Tahap implementasi adalah langkah lanjutan setelah perancangan sistem. Pada tahap ini, hasil implementasi berupa analisis sistem yang telah diuji untuk mengantisipasi serangan SQL Injection.

1.6.5 Pengujian

Pengujian dilakukan dengan menggunakan teknik SQL Injection Adapun yang dimaksud dengan SQL Injection adalah menganalisis hasil dari pengujian untuk menilai efektivitas perlindungan yang diberikan oleh basis data palsu terhadap jenis serangan SQL Injection.

1.6.6 Maintenance

Tahap Maintenance bertujuan untuk memastikan sistem tetap berfungsi dengan optimal melalui proses maintenance yang berkelanjutan. Pada tahap ini, penulis akan melakukan pemeliharaan terhadap sistem yang telah diimplementasi, contohnya melakukan perbaikan terhadap kesalahan yang tidak ditemukan pada tahap sebelumnya.

