BAB I
PENDAHULUAN

1. 1 Latar Belakang

Di era digital saat ini, basis data memainkan peran penting dalam berbagai sektor, termasuk keuangan, perawatan kesehatan, pemerintahan, dan e-commerce, yang bertindak sebagai tempat penyimpanan data berharga seperti informasi pribadi, catatan keuangan, kekayaan intelektual, dan data bisnis rahasia. Pentingnya keamanan basis data berasal dari potensi konsekuensi pelanggaran keamanan. Akses tidak sah, pelanggaran data, atau aktivitas jahat yang menargetkan basis data dapat mengakibatkan konsekuensi yang parah seperti pencurian identitas, kerugian finansial, pelanggaran privasi, kerusakan reputasi, dan konsekuensi hukum. Selain itu, sifat ancaman dunia maya yang terus berkembang dan lanskap peraturan yang terus berubah mengharuskan penerapan langkah-langkah keamanan yang kuat untuk melindungi data sensitif secara efektif. Keamanan basis data mencakup berbagai langkah yang ditujukan untuk menjaga integritas, kerahasiaan, dan ketersediaan data. Mekanisme autentikasi memverifikasi identitas pengguna untuk memastikan bahwa hanya individu yang berwenang yang dapat mengakses basis data. Mekanisme kontrol akses mengatur izin dan hak istimewa pengguna berdasarkan peran dan tanggung jawab mereka. Teknik enkripsi digunakan untuk melindungi data dari pengungkapan yang tidak sah, baik selama penyimpanan maupun transmisi. Reaksi cepat terhadap insiden keamanan difasilitasi oleh metode audit dan pemantauan https://www.researchgate.net/publication/372977065_A_Comprehensive_Review_of_Security_Measures_in_Database_Systems_Assessing_Authentication_Access_Control_and_Beyond [1].

Oleh karena itu, penting untuk menyadari bahwa semua aplikasi, baik aplikasi web, seluler, maupun desktop, yang terhubung ke basis data merupakan target SQLIA

yang salah satu ancaman paling umum terhadap sistem basis data di mana penyerang menambahkan pernyataan SQL ke kotak masukan formulir aplikasi, untuk mendapatkan akses ke sumber daya atau membuat perubahan pada data yang disimpan dalam basis data. Kurangnya validasi masukan dalam aplikasi menyebabkan penyerang berhasil. Dalam serangan SQL Injection, penyerang menyuntikkan input string melalui aplikasi, yang mengubah atau memanipulasi pernyataan SQL untuk keuntungan penyerang. Serangan SQL Injection dapat merusak basis data dalam berbagai cara, seperti manipulasi basis data yang tidak sah, atau pengambilan data sensitif. Serangan ini juga dapat digunakan untuk menjalankan perintah tingkat sistem yang dapat menyebabkan sistem menolak layanan ke aplikasi. Masalah ini sangat berisiko karena dapat menyebabkan hilangnya data atau penyalahgunaan data oleh pihak yang tidak berwenang dan akibatnya fungsionalitas https://www.researchgate.net/publication/372977065_A_Comprehensive_Review_of_Security_Measures_in_Database_Systems_Assessing_Authentication_Access_Control_and_Beyond [4]

Dalam implementasi basis data palsu, fokus bukan hanya pada pengembangan sistem yang aman, tetapi juga pada menjaga privasi dan keamanan data pengguna. Pendekatan ini sesuai dengan standar keamanan yang telah ditetapkan, yang menuntut perlindungan data yang baik terhadap potensi ancaman siber yang terus berkembang.

Berdasarkan Permasalahan dalam pengimplementasian pada database, pada fokus pengimplementasian maka dilakukan pengimplementasian "Basis Data Palsu Sebagai metode pengamanan" sebagai alternatif pencegahan serangan SQL Injection untuk mengurangi risiko dan dampak serangan SQL Injection dengan memanfaatkan teknik yang telah diidentifikasi oleh dengan integrasi pendekatan Sampling Plus Fake Data Random yang diusulkan oleh Rizvi dan Agrawal (2015), keamanan basis data dapat diperkuat melalui pengacauan hasil serangan dan pencegahan akses tidak sah ke data yang sebenarnya. Selain itu, penelitian ini bertujuan untuk menjaga integritas data dalam sistem basis data dengan menggunakan data palsu yang dapat memperdaya penyerang dan memberikan hasil yang tidak bermakna, sehingga mengurangi risiko kerusakan atau manipulasi data yang valid, serta melindungi kerahasiaan informasi pengguna agar tetap terjaga dari pengungkapan data sensitif.

Penelitian "Sampel Basis data sebagai metode pengamanan" 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?
2. Parameter apa saja yang digunakan untuk mengoptimalkan kinerja database palsu dalam menghadapi serangan SQL Injection?
3. Metode apa yang tepat untuk mengukur efektivitas database palsu 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 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. *Entity Relationship Diagram* (ERD) ERD dibuat untuk menggambarkan keterhubungan antar entitas yang dibangun.
c. Desain Aplikasi dan Flowchart dibuat untuk menggambarkan alur pembuatan website Pengaduan
d. 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.