IMPLEMENTASI SAMPEL BASIS DATA PALSU SEBAGAI METODE PENGAMANAN SEBUAH SISTEM

TUGAS AKHIR

diajukan oleh:

M Gilang Faizal R NIM(21.01.4585)
Agung Yuniarto NIM(21.01.4613)
Fikri Julian F NIM(21.01.4635)
Ilham Mufid NIM(21.01.4640)

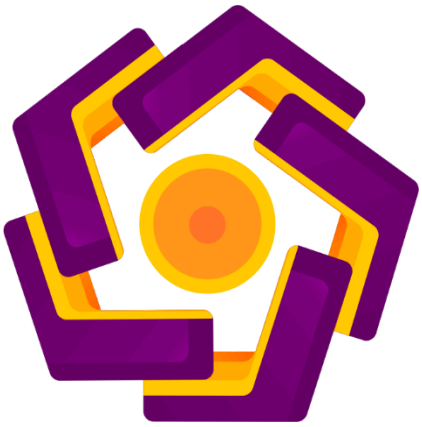
PROGRAM DIPLOMA
PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA

2025

IMPLEMENTASI SAMPEL BASIS DATA PALSU SEBAGAI METODE PENGAMANAN SEBUAH SISTEM

TUGAS AKHIR

Diajukan untuk memenuhi salah satu syarat mencapai gelar Ahli Madya Komputer Program Diploma – Program Studi Teknik Informatika



diajukan oleh

M Gilang Faizal R NIM(21.01.4585)

Agung Yuniarto NIM(21.01.4613)

Fikri Julian F NIM(21.01.4635)

Ilham Mufid NIM(21.01.4640)

PROGRAM DIPLOMA

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

2025

HALAMAN PERSETUJUAN

TUGAS AKHIR

Implementasi Sampel Basis Data Palsu Sebagai Metode Pengamanan Sebuah Sistem

yang dipersiapkan dan disusun oleh

ILHAM MUFID

21.01.4640

Telah disetujui oleh Dosen Pembimbing Tugas Akhir

pada tanggal 10 Agustus 2024

Dosen Pembimbing,

a.n

Ainul Yaqin, S.Kom., M.Kom

NIK. 190302255

HALAMAN PENGESAHAN

TUGAS AKHIR

IMPLEMENTASI SAMPEL BASIS DATA PALSU SEBAGAI METODE PENGAMANAN SEBUAH SISTEM

yang disusun dan diajukan oleh

ILHAM MUFID

21.01.4640

Telah dipertahankan di depan Dewan Penguji
pada tanggal 23 Agustus 2024

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Hastari Utama, M.Cs **NIK. 190302230**	
Arvin Claudy Frobenius, M.Kom **NIK. 190302495**	

Tugas Akhir ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Ahli Madya komputer
Tanggal 23 Agustus 2024

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, S.Kom., M.Kom., Ph.D.
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertandatangan di bawah ini,

Nama mahasiswa : Ilham Mufid
NIM : 21.01.4640

Menyatakan bahwa Tugas Akhir dengan judul berikut:

IMPLEMENTASI SAMPEL BASIS DATA PALSU SEBAGAI METODE PENGAMANAN SEBUAH SISTEM

Dosen Pembimbing : Ainul Yaqin, S.Kom., M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 23 Agustus 2024

Yang Menyatakan,

Ilham Mufid

v

HALAMAN PERSEMBAHAN

Puji Syukur Kami panjatkan kepada Allah SWT, yang telah memberikan kesehatan, rahmat dan hidayah, sehingga penulis masih diberikan kesempatan untuk menyelesaikan tugas akhir ini, sebagai salah satu syarat untuk mendapatkan gelar Diploma III. Walaupun jauh dari kata sempurna, namun penulis bangga telah mencapai pada titik ini, yang akhirnya tugas akhir ini bisa selesai di waktu yang tepat, Seorang teman seangkatan pernah berkata, “Selesaikanlah apa yang sudah kau mulai”, sehingga hal inilah yang membuat penulis memacu dirinya untuk menyelesaikan semaksimal mungkin sehingga dapat menyelesaikan tugas akhir ini, diwaktu yang tepat. Tugas akhir ini saya persembahkan untuk :

- Ayah dan Ibu, terimakasih atas doa, semangat, motivasi, pengorbanan, nasehat serta kasih sayang yang tidak pernah henti sampai saat ini.
- Dosen Pembimbing kami Pak Ainul Yaqin, S.Kom., M.Kom yang sudah membimbing serta memberi masukan dan saran selama ini, sehingga saya dapat menyelesaikan tugas akhir ini.
- Teman - Teman Seangkatan D3 Teknik Informatika Angkatan 2021 teman-teman lainya yang sudah memberikan motivasi dalam mengerjakan Tugas Akhir ini.
- Dosen D3 Teknik Informatika, yang telah memberikan ilmu dan motivasi dalam mengerjakan Tugas Akhir ini.
- Semua Komponen Amikom Yogyakarta, yang telah menerima kami dengan baik selama menempuh jenjang perkuliahan di Amikom Yogyakarta Hingga dapat menyelesaikan Tugas Akhir ini.

KATA PENGANTAR

Puji syukur ke hadirat Allah SWT, atas rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan laporan tugas akhir yang berjudul " Implementasi Sampel Basis Data Palsu Sebagai Metode Pengaman Sebuah Sistem " dengan baik dan lancar. Laporan ini disusun sebagai salah satu syarat untuk menyelesaikan program studi di Universitas Amikom Yogyakarta. Penyusunan laporan ini tidak lepas dari bantuan, bimbingan, dan dukungan dari berbagai pihak. Oleh karena itu, kami ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada Pak Ainul Yaqin, S.Kom., M.Kom selaku Dosen Pembimbing, yang telah memberikan bimbingan, saran, dan motivasi selama penyusunan tugas akhir ini. Teman-teman dan semua pihak yang telah memberikan dukungan, baik secara langsung maupun tidak langsung. Kami menyadari bahwa laporan ini masih jauh dari sempurna, baik dari segi penyusunan maupun isi. Oleh karena itu, kami mengharapkan kritik dan saran yang membangun dari pembaca demi perbaikan dan penyempurnaan laporan ini di masa yang akan datang. Akhir kata, kami berharap semoga laporan tugas akhir ini dapat memberikan manfaat bagi pengembangan sistem informasi keamanan dan dapat menjadi referensi bagi penelitian selanjutnya.

Yogyakarta, 23 Agustus 2024

Ilham Mufid

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR ISTILAH

SQL	Structured Query Language
SQLIAs	SQL Injection Attacks
OWASP	Open Web Application Security Project
de facto	"Sebenarnya" atau "dalam praktiknya."
DFD	Data Flow Diagram
ERD	Entity Relationship Diagram
RS+FD	Random Sampling plus Fake Data
UNION	Penggabungan dua data
HTTP	Hypertext Transfer Protocol
XAMPP	Web Server localhost
UNION	Penggabungan dua data
WWW	World Wide Web
URI	Uniform Resource Identifier
FTP	File Transfer Protocol
IP	Internet Protocol
PHP	Hypertext Preprocessor
HTML	Hypertext Markup Language

Out-of-band Komunikasi atau data dikirim melalui saluran berbeda dari yang biasanya digunakan.

Piggy-backed Teknik di mana penyerang menyisipkan query tambahan ke dalam permintaan yang sah yang dikirimkan ke database.

INTISARI

Database atau Basis data adalah media yang digunakan oleh orang-orang yang ingin mentransfer dan menyimpan data dari metode kertas tradisional ke metode digital menggunakan komputer. Kelebihan database adalah data dalam database dikelompokkan menjadi tabel dan kolom sehingga memudahkan dalam pencarian data. Namun data yang dimasukkan ke dalam database tidak mengalami perubahan, Maka dari itu diperlukan pengamanan Database. Pengamanan database merupakan fondasi krusial dalam melindungi integritas dan kerahasiaan data dari berbagai ancaman yang dapat mengintai. Oleh karena itu, dengan menerapkan lapisan keamanan yang kuat seperti kontrol akses yang ketat, enkripsi data, dan pemantauan aktif, database dapat dijaga dari ancaman tersebut. Dengan demikian, pengamanan database tidak hanya memberikan perlindungan terhadap serangan, tetapi juga memastikan bahwa data tetap aman dan dapat diandalkan. Beberapa Jenis serangan siber yang umum terjadi dan dapat menyebabkan kerusakan pada sebuah data, pencurian data, kehilangan data, dan bahkan hacker dapat mengambil alih dari kontrol sebuah database yaitu SQL Injection. SQL Injection ini memanfaatkan celah keamanan yang biasanya terdapat pada sebuah sistem atau aplikasi untuk menyerang database pada sebuah website[2], dengan cara melakukan penginjeksian atau mengirimkan kode SQL yang berbahaya ke dalam database yang digunakan sebuah website, sehingga hacker berbagai jenis penyerangan seperti pemanipulasian sebuah data dengan mudah dan dapat mengakses data yang seharusnya tidak dapat diakses. SQL Injection dapat terjadi karena kurangnya pengamanan pada validasi data input, seperti karakter yang diizinkan, format data, dan jumlah data, sehingga membuat aplikasi langsung mengeksekusi input yang dimasukkan oleh user secara langsung[3].

Kata kunci: Database, Pengamanan Database, SQL Injection

Abstract

"SQL injection attacks (SQLIAs) pose a major security risk for web applications. The Open Web Application Security Project (OWASP), an international consortium of web developers, consistently ranks SQLIAs among the top ten web application security risks. Despite increasing awareness, many common vulnerabilities persist. While robust Network SQL Injection Intrusion Detection Systems (IDS) are often implemented to counter these attacks, internal or subordinate employees can sometimes bypass these defenses. Consequently, Network Intrusion Detection Systems alone are insufficient to fully safeguard databases from such threats. This paper examines recent techniques in SQL injection attacks and their corresponding prevention methods. SQLIAs can allow attackers to read, alter, or delete database information. The proposed system aims to detect both external and insider attacks, mitigating web application vulnerabilities by implementing SQL Injection Prevention Techniques. To demonstrate these prevention techniques, a PHP-based web application called "Pengaduan" has been developed, capable of detecting various forms of SQL injection attacks."

Keyword: SQL Injection Attacks, SQLIAs, PHP, Website.