

**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
2024**

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)

Kepada

**PROGRAM DIPLOMA
PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
2024**

HALAMAN PERSETUJUAN

TUGAS AKHIR

**Implementasi Sampel Basis Data Palsu Sebagai Metode Pengamanan Sebuah
Sistem**

yang dipersiapkan dan disusun oleh

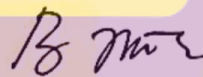
FIKRI JULIAN FEBRIANTO

21.01.4635

Telah disetujui oleh Dosen Pembimbing Tugas Akhir
pada tanggal 6 September 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

Fikri Julian Febrianto

21.01.4635

Telah dipertahankan di depan Dewan Penguji
pada tanggal 23 Agustus 2024

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Ria Andriani, M.Kom
NIK. 190302458



Surya Tri Atmaja R, S.Kom., M.Eng
NIK. 190302481



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 : Fikri Julian Febrianto
NIM : 21.01.4635

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,



Fikri Julian Febrianto

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



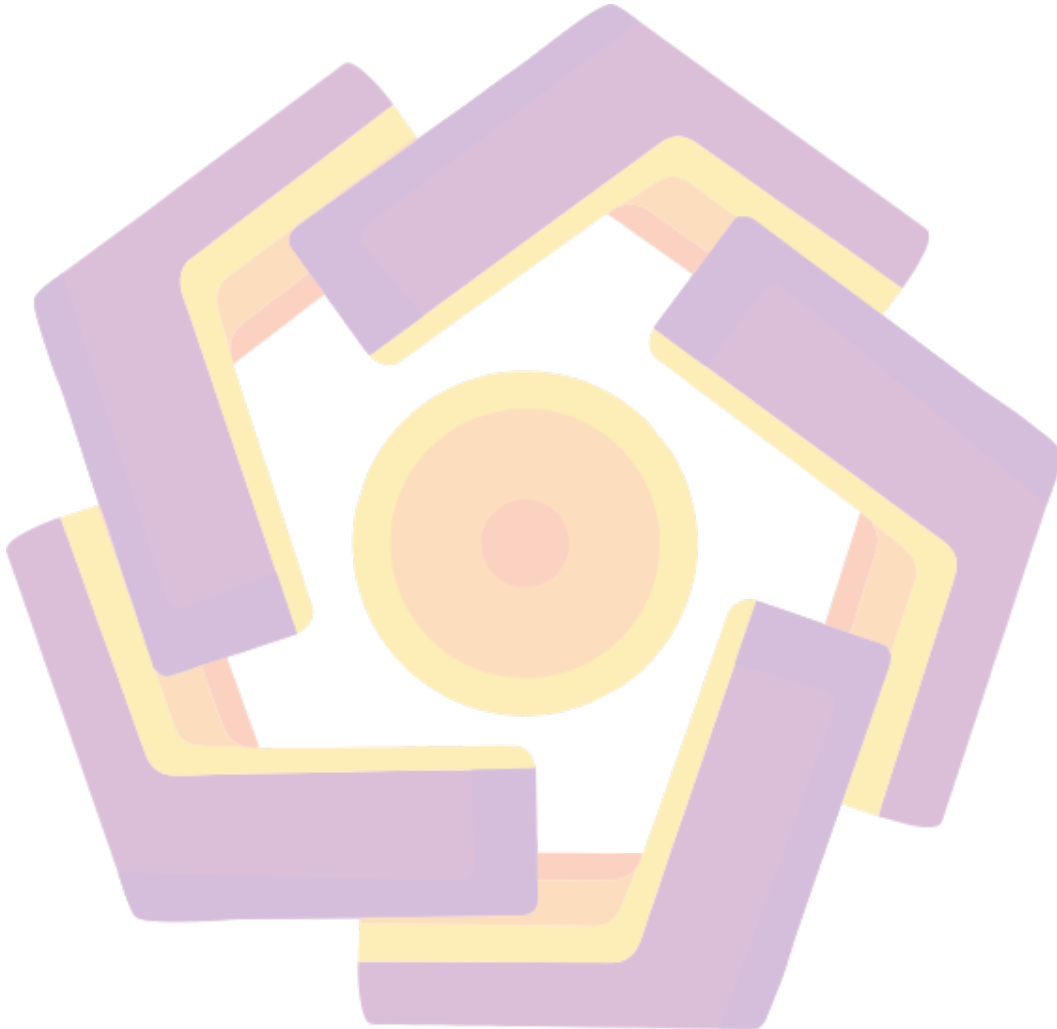
Fikri Julian Febrianto

DAFTAR ISI

HALAMAN JUDUL	ii
HALAMAN PERSETUJUAN	iii
HALAMAN PENGESAHAN	iv
HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR	v
HALAMAN PERSEMBAHAN	vi
KATA PENGANTAR	vii
DAFTAR ISI	viii
DAFTAR GAMBAR	xi
DAFTAR TABEL	xiv
DAFTAR ISTILAH	xv
INTISARI	xvi
Abstract	xvii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan masalah	2
1.3 Tujuan Penelitian	2
1.4 Batasan Masalah	2
1.5 Manfaat Penelitian	3
1.5.1 Manfaat Bagi Universitas Amikom Yogyakarta	3
1.5.2 Manfaat bagi khalayak umum	3
1.6 Metode Penelitian	3
1.6.1 Metode Pengumpulan Data	4
1.6.2 Analisis Sistem	4
1.6.3 Perancangan	4
1.6.4 Implementasi	4
1.6.5 Pengujian	5
1.6.6 Maintenance	5
BAB II LANDASAN TEORI	6
2.1 Literature Review	6
Literature Review Jurnal 1	6
Literature Review Jurnal 2	9
Literature Review Jurnal 3	11
2.2 Landasan Teori	14

2.2.1	Konsep Dasar Web	14
2.2.2	Definisi Web	14
2.2.3	Web Pengaduan	15
2.2.4	"Hypertext Preprocessor" (PHP).....	16
2.2.5	LARAVEL.....	17
2.3	Konsep Dasar Sistem Informasi.....	18
2.3.1	Definisi Sistem Informasi	19
2.3.2	Komponen Sistem Informasi	20
2.4	TEKNIK PERANCANGAN SISTEM	21
2.4.1	Definisi Perancangan Sistem	21
2.4.2	Perancangan Sistem	21
2.5	TEORI BASIS DATA	23
2.5.1	XAMPP.....	23
2.5.2	LARAVEL.....	23
2.5.3	MySQL.....	25
2.6	SOFTWARE.....	26
2.6.1	Visual Studio Code	26
2.6.2	Whimsical	27
2.6.3	SQLMap.....	27
2.6.4	OWASP ZAP.....	28
BAB III	METODOLOGI PENELITIAN	29
3.1	Alur Penelitian	29
3.1.1	Pengumpulan Kebutuhan.....	30
3.1.2	Analysis	30
3.1.3	Design	32
3.1.4	Mockup	36
BAB IV	HASIL DAN PEMBAHASAN	38
4.1	Implementasi.....	38
4.1.1	Integrasi Data Faker User	39
4.1.2	Integrasi Data Faker Pengaduan	40
4.2	Evaluasi Pengujian.....	42
4.2.1	Pengujian SQL Injection.....	42
4.2.2	Parameter Untuk Mengamankan.....	43
4.2.3	Unit Testing	50
4.2.4	Labeling Data.....	53

4.2.5 Evaluasi Pengujian Menggunakan SQLMap	56
4.2.6 Evaluasi Pengujian Menggunakan OWASP ZAP	62
4.2.7 Uji Web Pengaduan	67
BAB V KESIMPULAN DAN SARAN	73
5.1 Kesimpulan	73
5.2 Saran	73
DAFTAR PUSTAKA	74

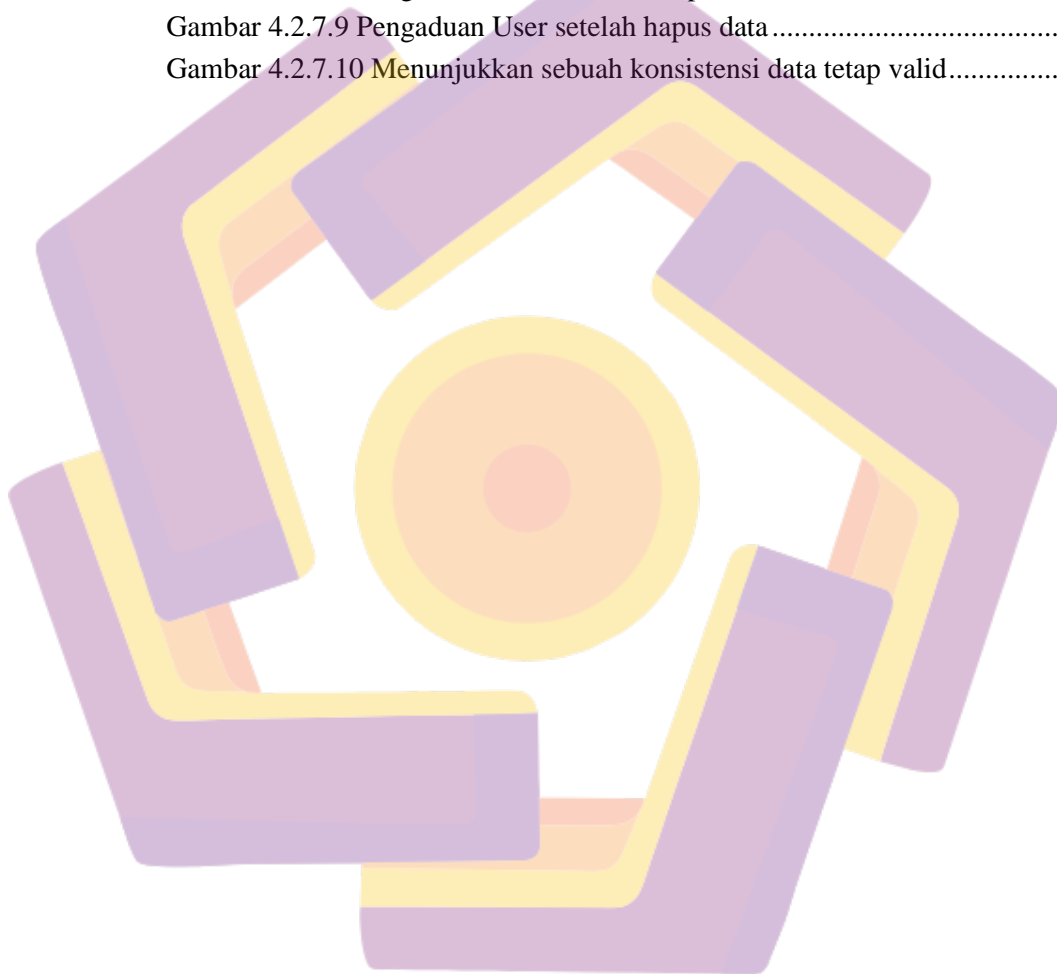


DAFTAR GAMBAR

BAB III	
METODOLOGI PENELITIAN	29
3.1 Alur Penelitian	29
Gambar 3.1 Tahap Model Proses Waterfall	29
3.1.1 Pengumpulan Kebutuhan	30
3.1.2 Analysis	30
3.1.3 Design	32
3.1.3.1 Data Flow Diagram (DFD).....	32
Gambar 3.1.3.1 Desain Diagram Konteks Web Pengaduan Sebagai level tertinggi dari Data Flow Diagram (DFD) Level 0	32
Gambar 3.1.3.2. Desain Diagram Konteks Web Pengaduan Sebagai level tertinggi dari Data Flow Diagram (DFD) Level 1	33
3.1.3.3 Flowchart.....	34
Gambar 3.1.3.3 Desain Aplikasi Web Pengaduan	34
Gambar 3.1.3.3.1 Desain Flowchart Web Pengaduan.....	35
3.1.4 Mockup	36
3.1.4.1 Tampilan User Home	36
Gambar 3.1.4.1 Desain Mockup Tampilan User Home	36
3.1.4.2 Tampilan Form Pengaduan	37
Gambar 3.1.4.2 Desain Mockup Tampilan Form Pengaduan	37
BAB IV	
HASIL DAN PEMBAHASAN	38
4.1 Implementasi	38
4.1.1 Integrasi Data Faker User	39
Gambar 4.1.1 Code - UserFactory untuk generate data faker	39
Gambar 4.1.1.1 Code - Users Seeder digunakan sebagai variabel untuk memanggil fungsi data faker dalam UserFactory	40
4.1.2 Integrasi Data Faker Pengaduan	40
Gambar 4.1.2 Code - Pengaduan Factory untuk generate data faker	40
Gambar 4.1.2.1 Code - Pengaduan Seeder digunakan sebagai variabel untuk memanggil fungsi data faker dalam Pengaduan Factory	41
Gambar 4.1.2.2 Hasil- Integrasi Data Faker data User.....	41
4.2 Evaluasi Pengujian	42
4.2.1 Pengujian SQL Injection.....	42
Gambar 4.2 Pengujian- SQL Injection Sebelum Menambahkan parameter	42
Gambar 4.2 Pengujian- SQL Injection Sesudah Menambahkan parameter	43
4.2.2 Parameter Untuk Mengamankan	43
4.2.2.1 Validasi dan Sanitasi Input pada AuthController	43

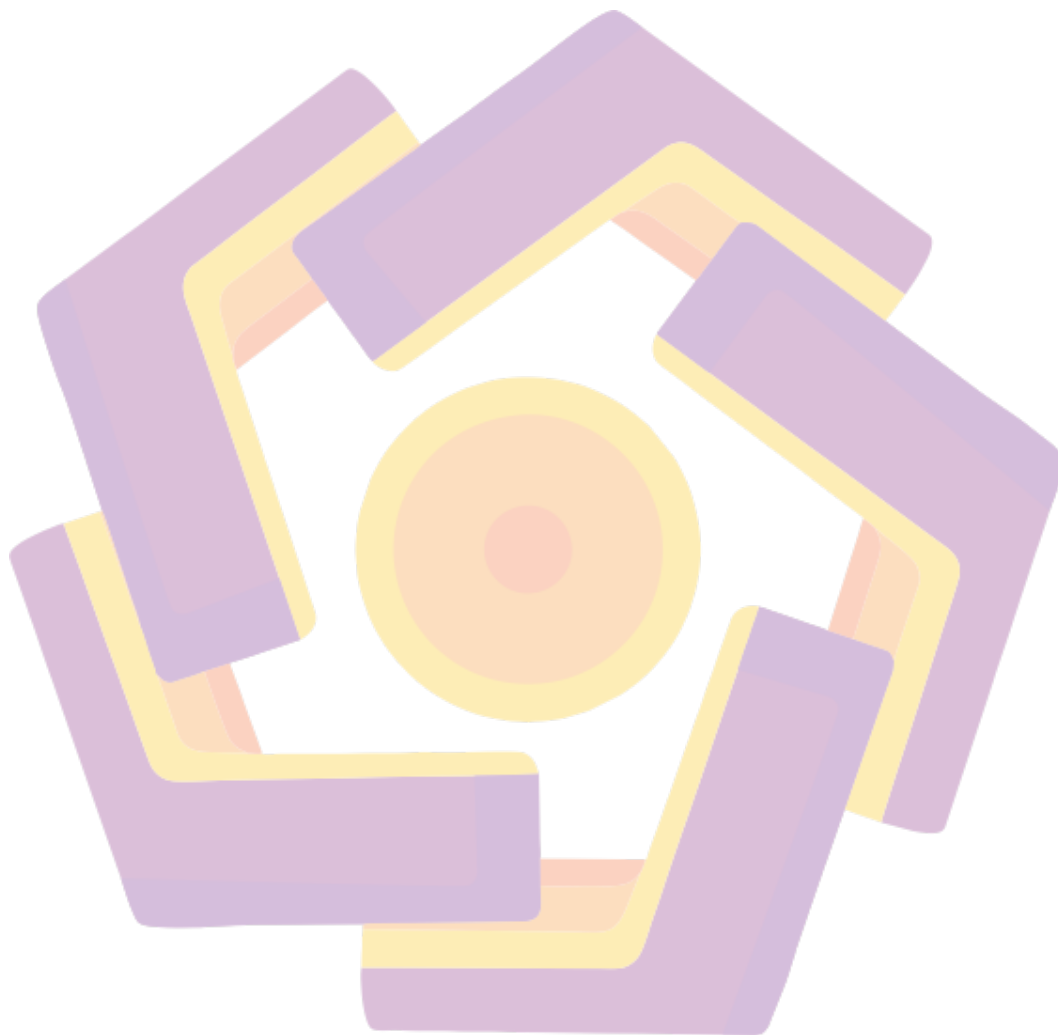
Gambar 4.2 Code - Validasi Form Parameter Register	44
Gambar 4.2 Code - Validasi Form Parameter Login	45
4.2.2.2 Validasi Form	46
Gambar 4.2 Code - Validasi Form sebagai pengaman pembatasan minimal dan maksimal input user	46
Gambar 4.2 Proses - Input Form Validasi dan Sanitasi Input dengan menerapkan pengamanan validasi (misalnya, email unik, tidak ada kolom yang diizinkan kosong kecuali diizinkan, dll.)	47
Gambar 4.2 Hasil - Validasi dan Sanitasi Input sebagai pengaman pembatasan minimal, maksimal, dan inputan acak user maupun sisi penyerang yang berhasil tercover.	48
4.2.2.3 Enkripsi Data User	48
Gambar 4.2 Code - Enkripsi Password dengan memasukan Hash untuk hashing password.....	48
Gambar 4.2 Code - Enkripsi Password dengan memasukan Hash untuk hashing password.....	49
Gambar 4.2 Hasil- Enkripsi Password dengan menerapkan Hash untuk hashing password.....	49
4.2.3 Unit Testing	50
Gambar 4.2.3 Unit Testing	50
4.2.3.1 Controller Layer Test	51
Gambar 4.2.3.1 Auth Controller Test.....	51
4.2.3.2 Model Layer Test	51
Gambar 4.2.3.2 Model User Test	51
4.2.3.3 Middleware Layer Test	52
Gambar 4.2.3.3 AuthMiddlewareTest.....	52
4.2.4 Labeling Data.....	53
Gambar 4.2.4 Code - Labelling untuk membedakan data asli dengan palsu	53
Gambar 4.2.4.1 Code - Labelling untuk membedakan data palsu dengan asli... ..	54
Gambar 4.2.4.2 Hasil- Labelling antara data asli dengan data palsu	55
4.2.5 Evaluasi Pengujian Menggunakan SQLMap	56
Gambar 4.2.5 Pengujian Bypass admin login Menggunakan SQLMap	56
Gambar 4.2.5.2 Pengujian Bypass admin login Menggunakan SQLMap.....	57
Gambar 4.2.5.3 Pengujian Bypass admin login Menggunakan SQLMap.....	58
Gambar 4.2.5.4 Pengujian Bypass admin login Menggunakan SQLMap.....	59
Gambar 4.2.5.5 Pengujian Bypass admin login Menggunakan SQLMap.....	60
4.2.6 Evaluasi Pengujian Menggunakan OWASP ZAP	62
Gambar 4.2.6 Owasp Zap - Tampilan awal.	62
Gambar 4.2.6.2 Owasp Zap - Tampilan Automated Scan.....	63
Gambar 4.2.6.3 Owasp Zap - Tampilan Proses Automated Scan.	63
Gambar 4.2.6.4 Owasp Zap - Tampilan Hasil Kerentanan.	64

4.2.7 Uji Web Pengaduan	67
Gambar 4.2.7 Form - Registrasi.....	67
Gambar 4.2.7.2 Hasil - Data Registrasi berhasil tersimpan dalam database	68
Gambar 4.2.7.3 Isi Data pada form Sign Register.....	68
Gambar 4.2.7.4 Show Data Akun User	69
Gambar 4.2.7.5 Pengaduan User sebelum update data	69
Gambar 4.2.7.6 Pengaduan User proses update/pembaruan data.....	70
Gambar 4.2.7.7 Pengaduan User setelah update/pembaruan data.....	70
Gambar 4.2.7.8 Pengaduan User sebelum hapus data.....	71
Gambar 4.2.7.9 Pengaduan User setelah hapus data	71
Gambar 4.2.7.10 Menunjukkan sebuah konsistensi data tetap valid.....	72




DAFTAR TABEL

Tabel 1. Literature Review Jurnal 1.....	6
Tabel 2. Literature Review Jurnal 2.....	9
Tabel 3. Literature Review Jurnal 3.....	11
Tabel 4. Hasil Vulnerability Assessment.....	65



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 adalah media digital yang digunakan untuk menyimpan dan mentransfer data, menggantikan metode kertas tradisional. Keamanan database sangat penting untuk melindungi data dari ancaman, seperti *SQL Injection*, yang memanfaatkan kelemahan pada sistem atau aplikasi untuk menyuntikkan kode *SQL* berbahaya. Serangan ini memungkinkan hacker mengakses, memanipulasi, atau mencuri data sensitif. Penyebab utama *SQL Injection* adalah kurangnya validasi input, di mana aplikasi langsung mengeksekusi data yang dimasukkan oleh pengguna tanpa pemeriksaan yang memadai. Untuk melindungi database dari serangan ini, penting menerapkan pengamanan seperti validasi data input, kontrol akses ketat, enkripsi data, dan pemantauan aktif. Selain itu, rutin memperbarui sistem keamanan dan mengikuti praktik terbaik dalam manajemen keamanan informasi adalah langkah penting. Dengan pengamanan yang tepat, integritas, kerahasiaan, dan ketersediaan data dalam database dapat terjamin.

Kata kunci: Database, Pengamanan Database, SQL Injection

ABSTRACT

“Database is a digital medium used for storing and transferring data, replacing traditional paper methods. Database security is crucial for protecting data from threats like SQL Injection, which exploits vulnerabilities in systems or applications by injecting malicious SQL code. This type of attack allows hackers to access, manipulate, or steal sensitive data. The primary cause of SQL Injection is inadequate input validation, where applications execute user-provided data without proper scrutiny. To safeguard databases from such attacks, it is essential to implement security measures like input validation, strict access controls, data encryption, and active monitoring. Regularly updating security systems and adhering to best practices in information security management are also vital steps. With proper safeguards in place, the integrity, confidentiality, and availability of data within a database can be ensured.”

Keyword: SQL Injection, SQL code, Database.

