BAB IV

HASIL DAN UJI COBA

IV.1. Tampilan Hasil

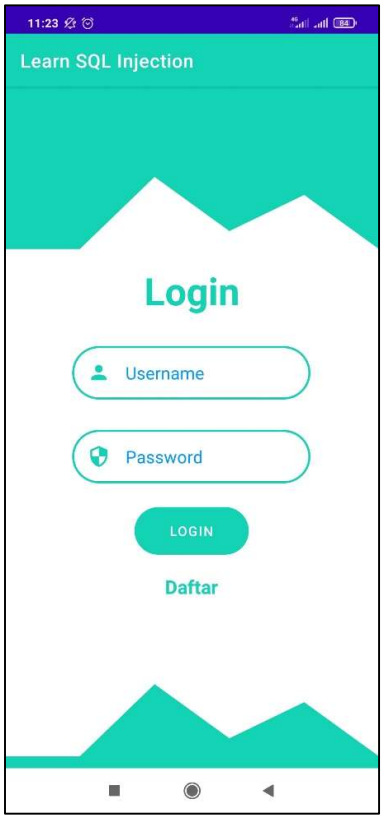
Berikut adalah tampilan dan penjelesan menu-menu dari aplikasi media pembelajaran keamanan *website* materi *SQL Injection.*

IV.1.1. Tampilan *Menu Login*

Pada *menu login* terdapat dua buah *edit text* yang harus diisi oleh mahasiswa yaitu *username* dan *password*, apabila *username* dan *password* benar maka aplikasi akan melakukan *fetching* data dari *database* berupa data id, *username*, dan level dan menyimpannya sebagai *session*. Jika level sama dengan Mahasiswa maka aplikasi akan menampilkan *Menu Home*, *List* Materi, Ujian, dan juga Profil dan jika level sama dengan Admin maka aplikasi akan menampilkan *Menu Home*, *List* Materi, Ujian, dan Daftar Mahasiswa.

Apabila mahasiswa belum mempunyai akun dapat mengklik tombol daftar maka akan langsung berpindah ke Menu Daftar.

Tampilan *Menu Login* dapat dilihat pada Gambar IV.1. dibawah ini:



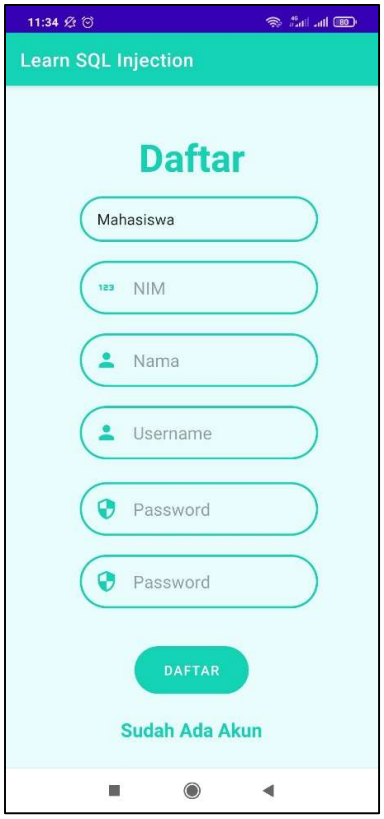
Gambar IV.1. Tampilan *Menu Login*

IV.1.2. Tampilan Menu Pendaftaran

Pada menu pendaftaran terdapat beberapa data yang perlu diisi oleh mahasiswa yaitu level, NIM, nama, username, dan juga password, terdapat dua buah edit text yang diperuntukkan untuk password, edit text password yang pertama akan dimasukkan ke database, dan edit text yang ke dua dipergunakan untuk mengkonfirmasi password yang diiisi mahasiswa pada edit text password pertama jika password yang dimasukkan berbeda antara edit text password pertama dengan yang kedua maka aplikasi akan menampilkan pesan kesalahan password tidak sama

dan apabila mahasiswa sudah memiliki akun maka dapat mengklik tombol Sudah Ada Akun dan berpindah ke menu login.

Tampilan Menu Pendaftaran dapat dilihat pada Gambar IV.2. dibawah ini:



Gambar IV.2. Tampilan Menu Pendaftaran

IV.1.3. Tampilan Menu Home

Pada *menu home* terdapat banner atau gambar yang bertuliskan *SQL Injection* dan juga ada beberapa materi yang dapat dipilih mahasiswa.

Tampilan *Menu Home* dapat dilihat pada Gambar IV.3. dibawah ini:

Gambar IV.3. Tampilan *Menu Home*

IV.1.4. Tampilan Menu List Materi

Pada menu *list* materi terdapat judul-judul materi yang dibahas, didalam setiap pilihan materi terdapat materi yang membahas tentang materi *SQL Injection* dalam bentuk video, gambar ataupun teks.

Tampilan Menu *List* Materi dapat dilihat pada Gambar IV.4. dibawah ini:

Gambar IV.4. Tampilan Menu List Materi

IV.1.5. Tampilan Menu Materi dan Latihan

Menu materi adalah menu yang berfungsi untuk menampilkan materi-materi yang membahas pembelajaran keamanan *website* materi *SQL Injection*, materi yang ada meliputi video, gambar maupun teks, setiap mahasiswa menyelesaikan satu judul materi maka akan ada latihan dalam bentuk praktek, latihan ini berguna untuk meningkatkan pemahaman mahasiswa tentang materi yang baru dipelajari.

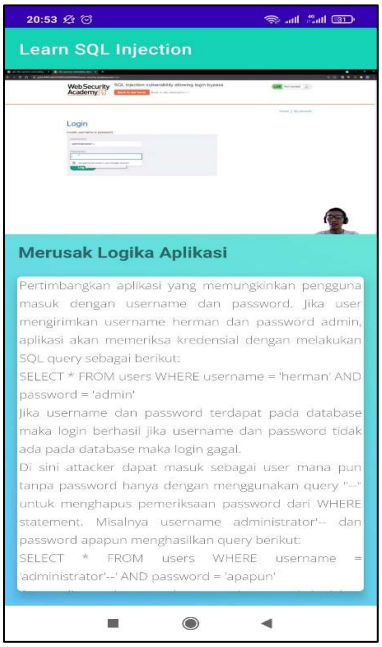
Tampilan Menu Materi dan Latihan dapat dilihat pada Gambar dibawah ini:

Gambar IV.5. Tampilan Menu Materi, Menampilkan Data Tersembunyi

Pada tampilan menu materi menampilkan data tersembunyi, menampilkan materi dalam bentuk video dan dan juga teks yang menjelaskan cara menampilkan data seluruh produk pada aplikasi baik itu yang sudah rilis maupun yang belum dirilis.

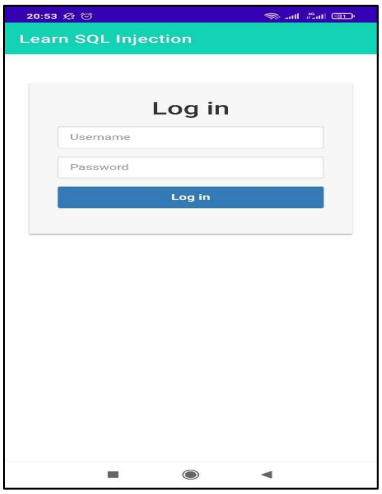
Gambar IV.6. Tampilan Menu Latihan, Menampilkan Data Tersembunyi

Pada menu latihan, menampilkan data tersembunyi mahasiswa dapat menginjekkan *query* ‘ or 1=1# karena or berarti salah satu bernilai *true* maka akan menghasilkan true dan 1=1 bernilai true, maka query akan bernilai *true* tanda pagar pada query SQL berarti komentar jadi query yang ada setelah tanda pagar akan dianggap sebagai komentar sehingga tidak dieksekusi oleh aplikasi akibatnya aplikasi akan menampilkan seluruh produk yang ada baik itu yang sudah rilis maupun yang belum dirilis



Gambar IV.7. Tampilan Menu Materi, Merusak Logika Aplikasi

Pada menu materi, merusak logika aplikasi terdapat materi dalam bentuk teks dan juga video yang menjelaskan cara melakukan serangan SQL Injection untuk login ke pada suatu sistem tanpa menggunakan password yang sah.



Gambar IV.8. Tampilan Menu Latihan, Merusak Logika Aplikasi

Pada menu latihan, merusak logika aplikasi mahasisa diberitahu username yang sah namu tidak diberikan passordnya disini mahasisa diharuskan untuk login menggunakan username administrator dengan password sembarang sehingga mahasiswa dapat menginjekkan query administrator' -- dan mengisi password sembarang maka mahasiswa akan berhasil *login* ke aplikasi.

Gambar IV.9. Tampilan Menu Materi, *Union Attack* Menentukan Jumlah Kolom

Pada tampilam menu materi , *union attack* menentukan jumlah kolom terdapat materi pelajaran dalam bentuk video dan juga teks yang membahas tentang serangan *SQL Injection* untuk mengetahui berapa jumlah kolom yang ada pada *table* yang digunakan aplikasi, pada materi diatas terdapat dua cara yang dapat dilakukan mahasiswa untuk mengetahui jumlah kolom yang ada pada *table,* cara

yang pertama dapat menggunakan query *ORDER BY* dan yang kedua dapat menggunakan query *UNION SELECT*.

Gambar IV.10. Tampilan Menu Latihan, Union Attack Menentukan Jumlah Kolom

Pada menu latihan, union attack menentukan jumlah kolom, mahasiswa dapat mempraktekkan serangan SQL Injection untuk mengetahui berapa jumlah kolom yang digunakan pada aplikasi dengan menginjekkan query ORDER BY 1, ORDER BY 2, dan seterusnya hingga aplikasi mengalami error jika aplikasi error pada query ORDER BY 4 misalnya, berarti aplikasi memiliki 3 table, dan cara yang kedua adalah UNION SELECT null, UNION SELECT null,null dan seterusnya, jika pada saat menjalankan UNION SELECT null aplikasi mengalami error berarti jumlah table yang ada lebih dari satu, lanjut ke percobaan tebakan table ada dua kita dapat menginjekkan query UNION SELECT null,null jika aplikasi kembali error

saat kita menjalankan query tadi berarti jumlah table yang ada lebih dari dua, dan seterusnya sampai aplikasi tidak mengalami error seperti gambar diatas.

Gambar IV.11. Tampilan Menu Materi, Menemukan Kolom Dengan Tipe Data Tertentu

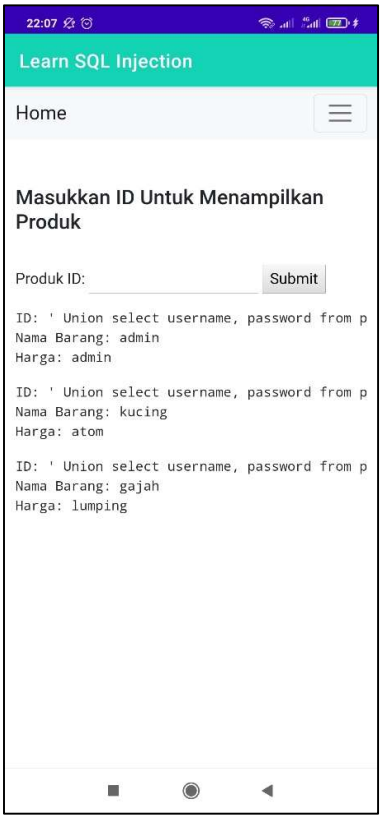
Pada menu materi, menemukan kolom dengan tipe data tertentu ini membahas tentang serangan SQL Injection untuk menemukan kolom dengan tipe data string karena umumnya data yang ingin dicuri berupa string seperti data username, dan password untuk itu kita perlu menemukan kolom dengan tipe data string untuk menampilkan data username dan password pada aplikasi.

Gambar IV.12. Tampilan Menu Latihan, Menemukan Kolom Dengan Tipe Data Tertentu

Pada Menu latihan, menemukan kolom dengan tipe data tertentu mahasiswa dapat melakukan serangan SQL Injection untuk menemukan kolom dengan tipe data string dengan menginjekkan query UNION SELECT “tes”, null jika aplikasi mengalami error berarti kolom pertama yang ada bukan bertipe data string dan jika aplikasi menampilkan hasil query yang kita injekkan berarti kolom pertama bertipe data string.

Gambar IV.13. Tampilan Menu Materi, SQL Injection Union Attack Mengambil Data Menarik

Pada tampilan menu materi, SQL Injection union attack mengambil data menarik dijelaskan proses serangan SQL Injection untuk mengambil data sensitif ataupun rahasia seperti username dan password dengan teknik union attack.



Gambar IV.14. Tampilan Menu Latihan, SQL Injection Union Attack Mengambil Data Menarik

pada menu latihan, SQL Injection union attack mengambil data menarik mahasiswa dapat melakukan serangan SQL Injection untuk mengambil data berupa username dan password dari table pengguna dengan menginjekkan query UNION SELECT username, password FROM pengguna, dan aplikasi akan menampilkan username dan password yang ada pada table pengguna seperti gambar diatas.

Gambar IV.15. Tampilan Menu Materi, Mengambil Beberapa Value Dalam Satu Kolom

Pada tampilan menu materi, mengambil beberapa value dalam satu kolom ini mahasiswa dapat berlatih serangan SQL Injection bagaimana menampilkan beberapa data pada satu kolom, pada materi sebelumnya kita sudah belajar bagaimana menampilkan username dan password namun dengan menggunakan dua kolom yang tersedia, bayangkan apabila aplikasi yang kita coba serang hanya memiliki satu kolom yang dapat digunakan untuk menampilkan data yang ingin kita curi tentu cara sebelumnya tidak efektif untuk dilakukan.

Gambar IV.16. Tampilan Menu Latihan, Mengambil Beberapa Value Dalam Satu Kolom

Pada tampilan menu latihan, mengambil beberapa value dalam satu kolom mahasiswa dapat melakukan serangan SQL Injection untuk menampilkan beberapa data pada satu kolom dengan menggunakan query group_concat() dengan fungsi ini kita dapat menggabungkan beberapa record database menjadi satu string.

Gambar IV.17. Tampilan Menu Materi, Menampilkan Tipe dan Versi Database Pada Oracle

Pada tampilan menu materi, menampilkan tipe dan versi database pada oracle ini membahas tentang bagaimana cara menampilkan versi dan tipe database pada oracle.

Gambar IV.18. Tampilan Menu Latihan, Menampilkan Tipe dan Versi Database Pada Oracle

Pada menu latihan, menampilkan tipe dan versi database pada oracle mahasiswa dapat berlatih bagaimana cara melakukan query untuk menampilkan versi dan tipe data pada database oracle, pada menu latihan ini mahasiswa dapat menginjekkan query UNION SELECT null, banner from v$version dan aplikasi akan menampilkan versi dan tipe database yang digunakan pada aplikasi.

Gambar IV.19. Tampilan Menu Materi, Menampilkan Tipe dan Versi Database Pada MySQL

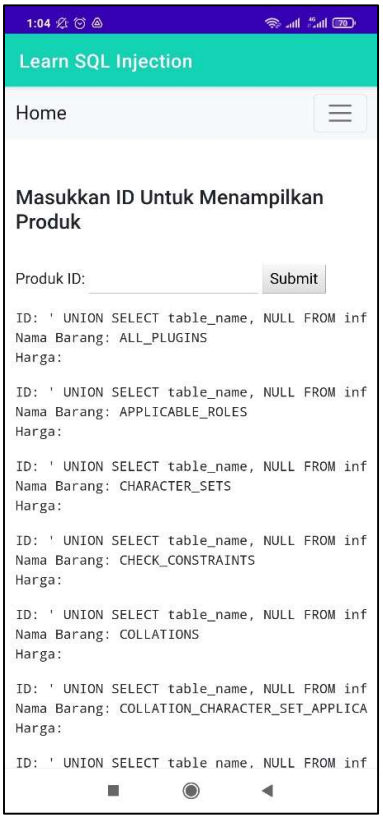
Pada menu materi, menampilkan tipe dan versi database pada MySQL ini membahas tentang bagaimana cara menampilkan tipe dan versi database pada MySQL, untuk menampilkan tipe dan versi database MySQL kita dapat melakukan query SELECT @@VERSION dan aplikasi akan menampilkan tipe dan versi database yang digunakan.

Gambar IV.20. Tampilan Menu Latihan, Menampilkan Tipe dan Versi Database Pada MySQL

Pada menu latihan ini mahasiswa dapat menginjekkan query UNION SELECT 1,@@version dan aplikasi akan menampilkan tipe dan versi database yang digunakan pada aplikasi.

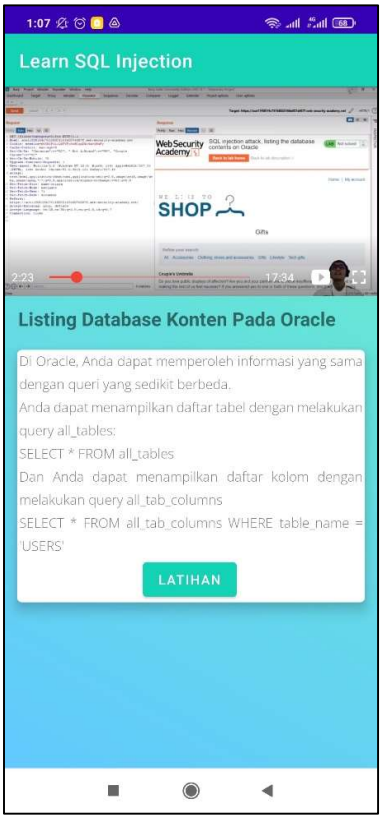
Gambar IV.21. Tampilan Menu Materi, Listing Database Konten Non Oracle

Pada tampilan menu materi, listing database konten non oracle ini membahas tentang bagaimana menampilkan seluruh struktur database yang digunakan pada suatu aplikasi dengan bantuan information_schema information schema adalah database yang terdapat pada database MySQL atau MariaDB dimana didalamnya terdapat semua data database metadata.



Gambar IV.22. Tampilan Menu Latihan, Listing Database Konten Non Oracle

Pada menu latihan, listing database konten non oracle ini mahasiswa dapat berlatih bagaimana menampilkan meta data yang ada pada database server MySQL atau MariaDB sebagai contoh disini kita dapat menampilkan seluruh nama table yang ada pada database MySQL atau MariaDB dengan query union select concat(table_name),2 from information_schema.tables where table_schema=database(). Dan aplikasi akan menampilkan seluruh table yang ada pada database.

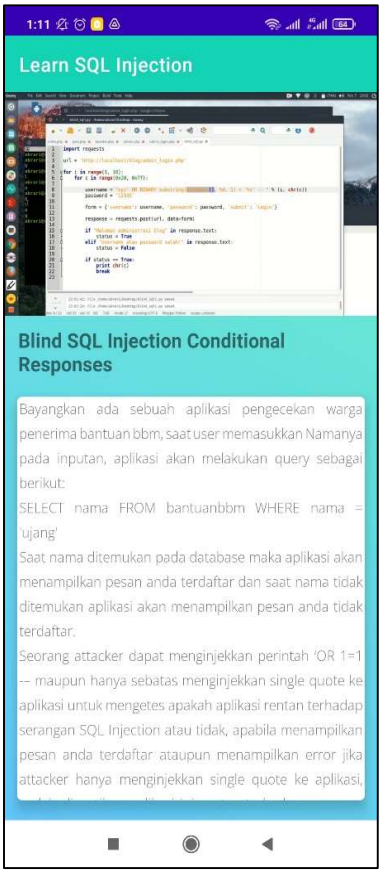


Gambar IV.23. Tampilan Menu Materi, Listing Database Konten Pada Oracle

Pada menu materi listing database konten pada oracle ini membahas tentang bagaimana menampilkan nama table yang ada pada database oracle, dengan query SELECT * FROM all_tables maka aplikasi akan menampilkan nama table yang terdapat pada database.

Gambar IV.24. Tampilan Menu Latihan, Listing Database Konten Pada Oracle

Pada menu latihan listing database konten pada oracle ini mahasiswa dapat berlatih menginjekkan query untuk menampilkan nama table yang tersedia pada database oracle dengan cara menginjekkan query UNION SELECT table_name from all_tables. Maka aplikasi akan menampilkan semua nama table yang terdapat pada database



Gambar IV.25. Tampilan Menu Materi, Blind SQL Injection Conditional Responses

Pada menu materi blind SQL Injection Conditional responses ini membahas tentang bagaimana melakukan serangan SQL Injection berdasarkan respon dari aplikasi.

Gambar IV.26. Tampilan Menu Latihan, Blind SQL Injection Conditional Responses

Pada menu latihan blind SQL Injection conditional responses mahasiswa dapat berlatih bagaimana cara mendapatkan nama database maupun table dengan teknik blind SQL Injection, pada latihan ini mahasiswa dapat menginjekkan query 1' and substring((select database()),1,1) = 'a'# untuk mengecek apakah huruf pertama nama database berhuruf a jika nama database tidak berawalan huruf a maka aplikasi akan menampilkan pesan anda belum terdaftar jika huruf a adalah huruf awal nama database maka aplikasi akan menampilkan pesan anda sudah terdaftar begitu seterusnya untuk menampilkan huruf-huruf nama database berikutnya.

Gambar IV.27. Tampilan Menu Materi, Time Based SQL Injection

Pada tampilan menu materi time based sql injection in imembahas materi tentang bagaimana melakukan serangan SQL Injection berbasis waktu. Bayangkan ada sebuah aplikasi hanya menampilkan satu respon terhadap inputan user Ketika inputan dan salah menampilkan pesan yang sama, sehingga kita tidak dapat melakukan serangan SQL Injection berdasarkan pesan yang diberikan oleh aplikasi jadi disini kita dapat melakukan serangan sql injection berbasis waktu jadi kuncinya ada pada waktu loading aplikasi saat kita menginputkan sesuatu misalnya kita menginjekkan query abc' OR IF(length(substr((select database()),1)) = 1, sleep(3),

0)# jika nama database memiliki 1 krakter maka aplikasi akan delay sekitar tiga detik dan apabila jumlah karakter huruf pada nama database tidak berjumlah satu karakter maka aplikasi akan mengeksekusi query yang kit injekkan tanpa delay.

Gambar IV.28. Tampilan Menu Latihan, Time Based SQL Injection

Pada menu latihan time based SQL Injection mahasiswa dapat berlatih bagaimana cara mendapatkan nama database maupun table dengan teknik blind SQL Injection, pada latihan ini mahasiswa dapat menginjekkan query abc' OR IF(substring(database(), 1, 1) = 'a', sleep(3), 0)# jika huruf awal nama database adalah a maka aplikasi akan delay sekitar tiga detik apabila dan apabila bukan database akan langsung mengeksekusi perintah yang kita masukkan tanpa delay.

Gambar IV.29. Tampilan Menu Materi, Cara Menangani Serangan SQL Injection

Pada menu materi cara menangani serangan SQL Injection ini membahas cara- cara yang dapat dilakukan untuk menangani serangan SQL Injection pada menu ini membahas mulai dari melakukan parameterized, mematikan error SQL, menggunakan firewall dan lain-lain.

IV.1.6. Tampilan Menu Ujian

Menu ujian adalah menu yang berfungsi untuk mengetahui hasil belajar mahasiswa maupun untuk menguji tingkat pemahaman mahasisa tentang materi-materi yang telah dipelajari, soal-soal ujian ini dibuat seperti permainan *capture the*

flag atau ctf, sehingga untuk menyelesaikan soal ujian mahasiswa diharuskan untuk mencari sebuah *String* yang telah disembunyikan yang biasa disebut dengan istilah *flag,* setiap mahasiswa berhasil menjawab soal ujian yang ada, maka akan mendapat 10 poin atau nilai, pada menu ujian ada beberapa tombol yaitu tombol mulai untuk berpindah ke soal praktek, tombol *clue* untuk menampilkan petunjuk untuk memudahkan mahasiswa dalam mengerjakan soal yang diberikan dan ada juga tombol jawab, apabila mahasiswa telah mendapatkan jawaban yang diperlukan mahasiswa dapat menginputkannya pada *edit text* yang disediakan dan menekan tombol jawab.

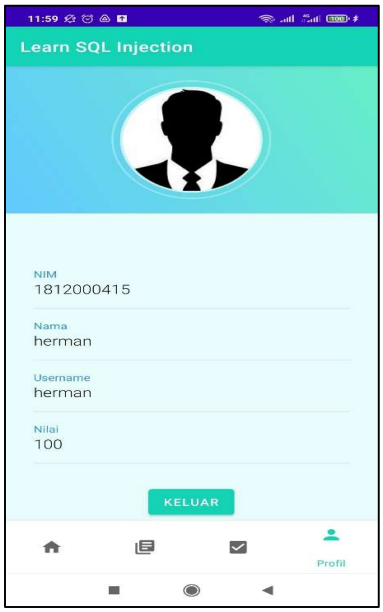
Tampilan Menu Ujian dapat dilihat pada Gambar IV.28. dibawah ini:

Gambar IV.30. Tampilan Menu Ujian

IV.1.7. Tampilan Menu Profil

Menu profil adalah menu yang berisikan data-data mahasiswa seperti nim, nama*, username* dan juga nilai, nilai ini akan didapatkan dari hasil ujian yang telah dilakukan mahasiswa pada menu ujian, pada menu profil juga ada tombol keluar, apabila mahasiswa mengklik tombol keluar maka mahasiswa akan *terlogout* dan berpindah ke menu *login*.

Tampilan Menu Profil dapat dilihat pada Gambar IV.29. dibawah ini:



Gambar IV.31. Tampilan Menu Profil

IV.1.8. Tampilan Menu Daftar Mahasiswa

Menu daftar mahasiswa adalah menu yang menampilkan data-data mahasisa berupa, nim, nama, dan nilai, halaman daftar mahasiswa ini hanya dapat

diakses oleh admin, pada menu daftar mahasiswa terdapat tombol keluar apabila *admin* mengklik tombol keluar maka akan *terlogout* dan berpindah ke menu *login.*

Tampilan Menu Daftar Mahasiswa dapat dilihat pada Gambar IV.30. dibawah ini:

Gambar IV.32. Tampilan Menu Daftar Mahasiswa

IV.2. Uji Coba

Uji coba terhadap aplikasi media pembelajaran keamanan *website* materi *SQL Injection* ini menggunakan metode pengujian *blackbox*, metode pengujian *blackbox* adalah metode pengujian yang berfokus pada uji fungsionalitas suatu

aplikasi yang telah dirancang, berikut pengujian *blackbox* aplikasi media pembelajaran keamanan *website* materi *SQL Injection*:

Tabel IV.1. Pengujian Menu Login

No.	Data Masukkan	Yang Diharapkan	Pengamatan	Kesimpulan
1	Username Salah Password Salah	Login Gagal, Tetap berada pada menu Login dan Menampilkan Pesan Error	Login Gagal, tetap berada pada menu login Dan Menampilkan Pesan Error	Valid
2	Username Benar Password Salah	Login Gagal, Tetap berada pada menu Login dan Menampilkan Pesan Error	Login Gagal, tetap berada pada menu login Dan Menampilkan Pesan Error	Valid
3	Username Salah Password Benar	Login Gagal, Tetap berada pada menu Login dan Menampilkan Pesan Error	Login Gagal, Tetap berada pada menu Login dan Menampilkan Pesan Error	Valid

4	Username Benar Password Benar	Login Berhasil Dan Berpindah Ke Menu Home	Login Berhasil Dan Berpindah Ke Menu Home	Valid

Tabel IV.2. Pengujian Menu Pendaftaran Mahasiswa

No.	Data Masukkan	Yang Diharapkan	Pengamatan	Kesimpulan
1	NIM Tidak Diisi Nama Tidak Diisi Username Tidak Diisi Password Tidak Diisi Password Konfirmasi Tidak Diisi	Pendaftaran Gagal, dan Menampilkan Pesan Error	Pendaftaran Gagal, dan Menampilkan Pesan Error	Valid
2	NIM Diisi Nama Tidak Diisi Username Tidak Diisi Password Tidak Diisi Password Konfirmasi Tidak Diisi	Pendaftaran Gagal, dan Menampilkan Pesan Error	Pendaftaran Gagal, dan Menampilkan Pesan Error	Valid
3	NIM Diisi Nama Diisi Username Tidak Diisi	Pendaftaran Gagal, dan Menampilkan Pesan Error	Pendaftaran Gagal, dan Menampilkan Pesan Error	Valid

	Password Tidak Diisi Password Konfirmasi Tidak Diisi			
4	NIM Diisi Nama Diisi Username Diisi Password Tidak Diisi Password Konfirmasi Tidak Diisi	Pendaftaran Gagal, dan Menampilkan Pesan Error	Pendaftaran Gagal, dan Menampilkan Pesan Error	Valid
5	NIM Diisi Nama Diisi Username Diisi Password Diisi Password Konfirmasi Tidak Diisi	Pendaftaran Gagal, dan Menampilkan Pesan Error	Pendaftaran Gagal, dan Menampilkan Pesan Error	Valid
6	NIM Diisi Nama Diisi Username Diisi Password Diisi Password Konfirmasi Diisi tidak sesuai dengan password	Pendaftaran Gagal, dan Menampilkan Pesan Error	Pendaftaran Gagal, dan Menampilkan Pesan Error	Valid
7	NIM Diisi	Pendaftaran Berhasil	Pendaftaran Berhasil	Valid

	Nama Diisi Username Diisi Password Diisi Password Konfirmasi Diisi sesuai dengan password	Dan Menampilkan Pesan Pendaftaran Berhasil	Dan Menampilkan Pesan Pendaftaran Berhasil	

Tabel IV.3. Pengujian Menu Pendaftaran Admin

No.	Data Masukkan	Yang Diharapkan	Pengamatan	Kesimpulan
1	Nama Tidak Diisi Username Tidak Diisi Password Tidak Diisi Password Konfirmasi Tidak Diisi	Pendaftaran Gagal, dan Menampilkan Pesan Error	Pendaftaran Gagal, dan Menampilkan Pesan Error	Valid
2	Nama Tidak Diisi Username Tidak Diisi Password Tidak Diisi Password Konfirmasi Tidak Diisi	Pendaftaran Gagal, dan Menampilkan Pesan Error	Pendaftaran Gagal, dan Menampilkan Pesan Error	Valid

3	Nama Diisi Username Tidak Diisi Password Tidak Diisi Password Konfirmasi Tidak Diisi	Pendaftaran Gagal, dan Menampilkan Pesan Error	Pendaftaran Gagal, dan Menampilkan Pesan Error	Valid
4	Nama Diisi Username Diisi Password Tidak Diisi Password Konfirmasi Tidak Diisi	Pendaftaran Gagal, dan Menampilkan Pesan Error	Pendaftaran Gagal, dan Menampilkan Pesan Error	Valid
5	Nama Diisi Username Diisi Password Diisi Password Konfirmasi Tidak Diisi	Pendaftaran Gagal, dan Menampilkan Pesan Error	Pendaftaran Gagal, dan Menampilkan Pesan Error	Valid
6	Nama Diisi Username Diisi Password Diisi Password Konfirmasi Diisi tidak sesuai dengan password	Pendaftaran Gagal, dan Menampilkan Pesan Error	Pendaftaran Gagal, dan Menampilkan Pesan Error	Valid
7	Nama Diisi Username Diisi	Pendaftaran Berhasil	Pendaftaran Berhasil	Valid

	Password Diisi Password Konfirmasi Diisi sesuai dengan password	Dan Menampilkan Pesan Pendaftaran Berhasil	Dan Menampilkan Pesan Pendaftaran Berhasil	

Tabel IV.4. Pengujian Navigasi

No.	Data Masukkan	Yang Diharapkan	Pengamatan	Kesimpulan
1	Klik Tombol Daftar	Berpindah Ke Menu Pendaftaran	Berpindah Ke Menu Pendaftaran	Valid
2	Klik Tombol Sudah Ada Akun	Berpindah Ke Menu Login	Berpindah Ke Menu Login	Valid
3	Klik Tombol Home	Berpindah Ke Menu Home	Berpindah Ke Menu Home	Valid
4	Klik Tombol List Materi	Berpindah Ke Menu List Materi	Berpindah Ke Menu List Materi	Valid
5	Klik Tombol Ujian	Berpindah Ke Menu Ujian	Berpindah Ke Menu Ujian	Valid
6	Klik Tombol Profil	Berpindah Ke Menu Profil	Berpindah Ke Menu Profil	Valid
7	Klik Tombol Daftar Mahasiswa	Berpindah Ke Menu Daftar Mahasiswa	Berpindah Ke Menu Daftar Mahasiswa	Valid

Tabel IV.5. Pengujian Menu ujian

No.	Data Masukkan	Yang Diharapkan	Pengamatan	Kesimpulan

1	Klik Tombol Mulai	Berpindah Ke Menu Lab Ujian	Berpindah Ke Menu Lab Ujian	Valid
2	Klik Tombol Clue	Menampilkan Clue	Menampilkan Clue	Valid
3	Klik Tombol Jawab Jawaban Salah	Meanmpilkan pesan Jawaban Salah	Meanmpilkan pesan Jawaban Salah	Valid
4	Klik Tombol Jawab Jawaban Benar	Menampilkan pesan Jawaban Benar dan Poin bertambah 10	Menampilkan pesan Jawaban Benar dan Poin bertambah 10	Valid
5	Klik Tombol Petunjuk	Menampilkan Petunuk	Menampilkan Petunuk	Valid

IV.2.1. Hasil Uji Coba

1. Saat *user* memasukkan *username* atau *password* yang salah aplikasi tidak berpindah ke menu *home*, dan saat *user* memasukkan *username* dan *password* yang benar maka aplikasi akan berpindah ke menu *home*.
2. Saat *user* tidak mengisi semua data yang diperlukan pada form pendaftaran maka pendaftaran akan gagal, jika *user* telah memasukkan semua data yang diperlukan namun *password* konfimasi berbeda dengan *password* maka pendaftaran gagal dan jika *user* memasukkan semua data dan *password* konfirmasi sama dengan *password* maka pendaftaran berhasil.
3. Navigasi yang ada pada aplikasi dapat berfungsi dengan baik.
4. Tombol mulai pada menu ujian dapat berjalan dengan baik, tombol *clue* dapat menampilkan *clue* saat ditekan, tombol jawaban akan menampilkan pesan jawaban salah apabila jawaban yang diinputkan

salah dan menampilkan jawaban benar serta memberi mahasiswa 10 poin apabila jawaban benar.

IV.2.2. Kelebihan Sistem

Adapun kelebihan sistem yang telah dibuat diantaranya yaitu:

1. Terdapat *lab hacking* untuk melakukan simulasi serangan *SQL Injection* didalam aplikasi.
2. Memiliki *user interface* yang mudah dipahami sehingga mudah untuk digunakan.
3. Soal ujian dirancang seperti *capture the flag* sehingga proses ujian seperti bermain *game*.

IV.2.3. Kekurangan Sistem

Adapun kekurangan sistem yang telah dibuat diantaranya yaitu:

1. Belum ada menu untuk menambah maupun mengedit materi pelajaran yang tersedia, sehingga apabila ingin menambahkan ataupun mengedit materi pelajaran, harus mengcompile ulang aplikasi.
2. Pada aplikasi ini belum ada fungsi untuk mencetak data nilai mahasiswa.
3. *Database* yang digunakan pada pembuatan aplikasi ini masih bersifat local.