BAB V

IMPLEMENTASI DAN PENGUJIAN SISTEM

5.1 HASIL IMPLEMETASI MENGGUNAKAN SINGEL SIGN-ON

Implementasi merupakan tahapan realisasi dari seluruh rancangan arsitektur sistem, antarmuka, dan alur autentikasi yang telah didefinisikan pada bab sebelumnya. Pada tahap ini, seluruh rancangan tersebut diterjemahkan ke dalam bentuk kode program dan konfigurasi sistem yang dapat dijalankan oleh komputer. Pembangunan sistem *Single Sign-On* (SSO) ini dilakukan dengan menggunakan *Keycloak* sebagai *Identity Provider* dan aplikasi berbasis Laravel sebagai Service Provider, sehingga proses autentikasi dapat dijalankan secara terpusat dan terintegrasi.

Proses implementasi tidak hanya berfokus pada tampilan halaman login dan dashboard, tetapi juga memastikan bahwa seluruh mekanisme autentikasi, pertukaran token, serta pengelolaan sesi pengguna berjalan sesuai dengan konsep *Single Sign-On* yang telah dirancang. Setiap pengguna, baik maupun mahasiswa, melakukan login melalui satu halaman autentikasi terpusat, kemudian memperoleh akses ke berbagai aplikasi layanan akademik tanpa perlu melakukan login ulang.

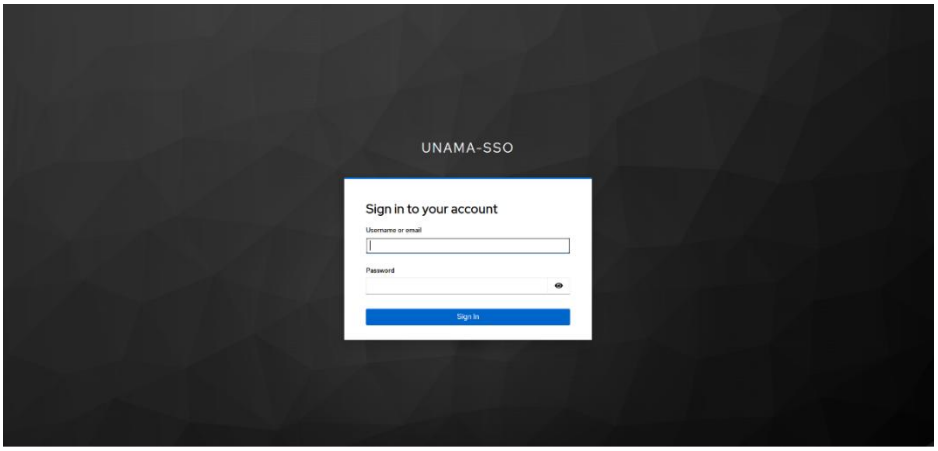
Hasil akhir dari tahap implementasi ini adalah sebuah sistem autentikasi terintegrasi berbasis web yang mampu menghubungkan aplikasi *SIAKAD*, *Presensi*, dan *E-learning* dalam satu mekanisme login terpadu. Sistem ini siap digunakan untuk mendukung layanan digital di lingkungan Universitas Dinamika Bangsa

dengan tingkat efisiensi dan keamanan yang lebih baik dibandingkan sistem autentikasi terpisah.

Berikut ini adalah penjabaran hasil implementasi antarmuka dan alur penggunaan sistem *Single Sign-On* yang telah dibangun :

1. Tampilan halaman login terpusat

   Halaman Login Terpusat merupakan halaman autentikasi utama dalam sistem *Single Sign-On* (SSO) yang digunakan oleh mahasiswa untuk mengakses seluruh aplikasi yang terintegrasi.

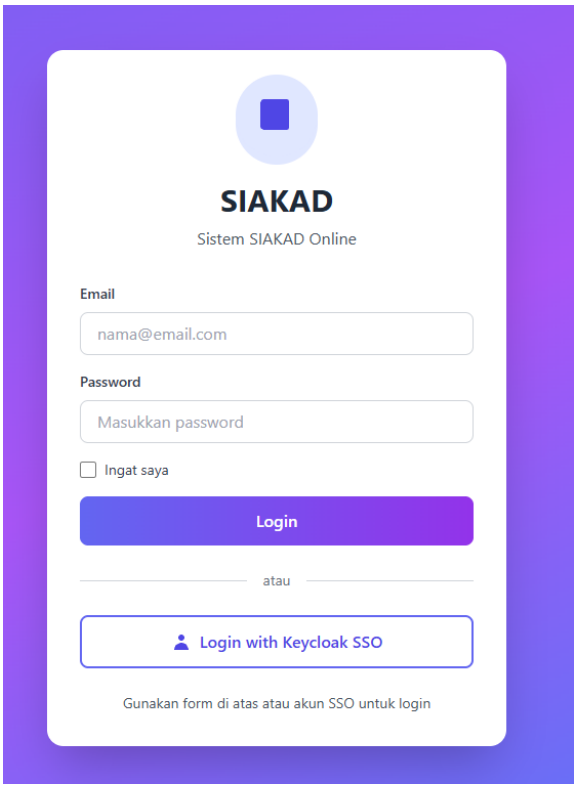


Gambar 5. 1 Login *Keycloak*

Pada halaman ini, pengguna cukup memasukkan username atau email serta kata sandi satu kali melalui sistem SSO. Setelah proses login berhasil, pengguna akan langsung mendapatkan akses ke berbagai aplikasi seperti *SIAKAD*, *Presensi*, dan *E-learning* tanpa perlu melakukan login ulang. Halaman ini berfungsi sebagai pintu masuk utama ke seluruh layanan digital Universitas Dinamika Bangsa tampilan halaman login terpusat dapat di lihat 5.1.

2. Halaman login *SIAKAD* (entry point)

   Halaman Login *SIAKAD* berfungsi sebagai halaman akses awal bagi mahasiswa untuk masuk ke dalam sistem akademik.

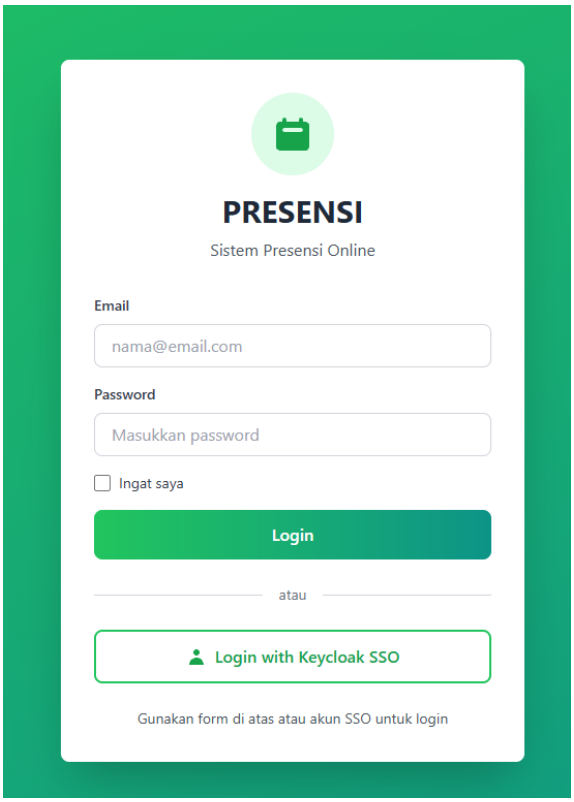


Gambar 5. 2 halaman login *SIAKAD*

Pada halaman ini pengguna diminta memasukkan email dan password untuk login secara manual atau dapat memilih login menggunakan *Keycloak Single Sign-On* (SSO). Desain menggunakan tema warna ungu dengan ikon sebagai identitas sistem akademik. Halaman ini digunakan oleh mahasiswa, dosen, maupun admin untuk mengakses layanan akademik seperti pengelolaan data akademik, KRS, KHS, dan informasi perkuliahan lainnya bisa di lihat di gambar 5.2 .

3. Halaman login *presensi*

Halaman Login *E-learning* digunakan sebagai pintu masuk bagi mahasiswa untuk mengakses layanan pembelajaran daring.

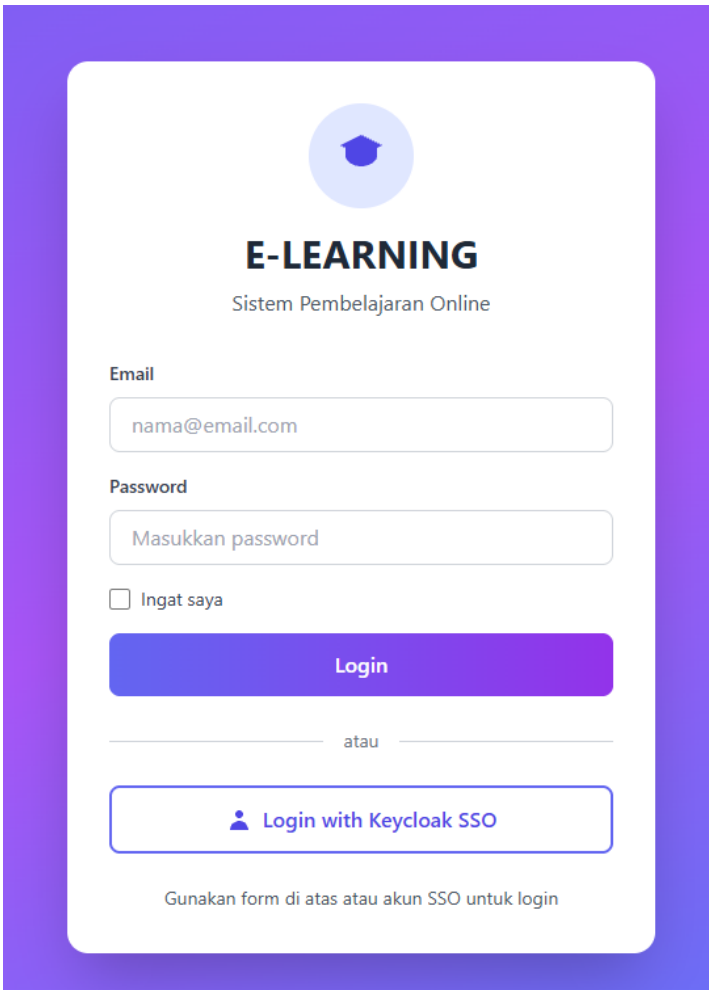


Gambar 5. 3 halaman login *presensi*

Login *PRESENSI* digunakan untuk mengakses Sistem *Presensi* Online yang berfungsi mencatat kehadiran pengguna. Tampilan halaman ini memiliki struktur yang sama dengan halaman lainnya, namun dibedakan dengan tema warna hijau dan ikon kalender yang merepresentasikan kehadiran. Pengguna dapat melakukan login menggunakan email dan password atau melalui *Keycloak* SSO, sehingga proses autentikasi menjadi lebih mudah dan terintegrasi dengan sistem lain bisa dilihat di gambar 5.3

4. Halaman login *E-learning*

Halaman Login *E-learning* digunakan sebagai pintu masuk bagi mahasiswa untuk mengakses layanan pembelajaran daring.



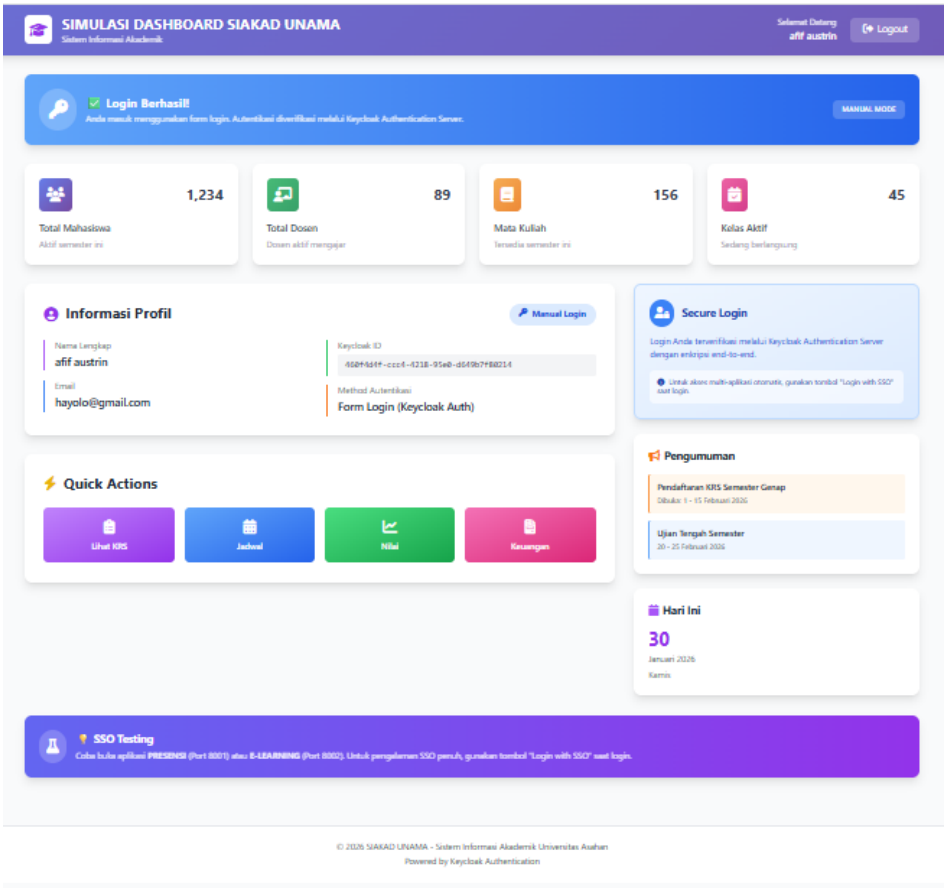
Gambar 5. 4 halaman login *E-learning*

Login *E-LEARNING* merupakan halaman autentikasi untuk Sistem Pembelajaran Online. Menggunakan ikon topi wisuda sebagai simbol kegiatan belajar mengajar dan tema warna ungu untuk menjaga konsistensi visual. Pengguna dapat masuk ke sistem melalui login manual atau menggunakan *Keycloak* SSO. Setelah berhasil login, pengguna dapat

mengakses materi pembelajaran, tugas, dan aktivitas perkuliahan secara daring bisa dilihat di gambar 5.4.

5. Halaman dashboard *SIAKAD*

Dashboard *SIAKAD* merupakan halaman utama yang ditampilkan setelah pengguna berhasil melakukan login melalui sistem *Single Sign-On* (SSO).



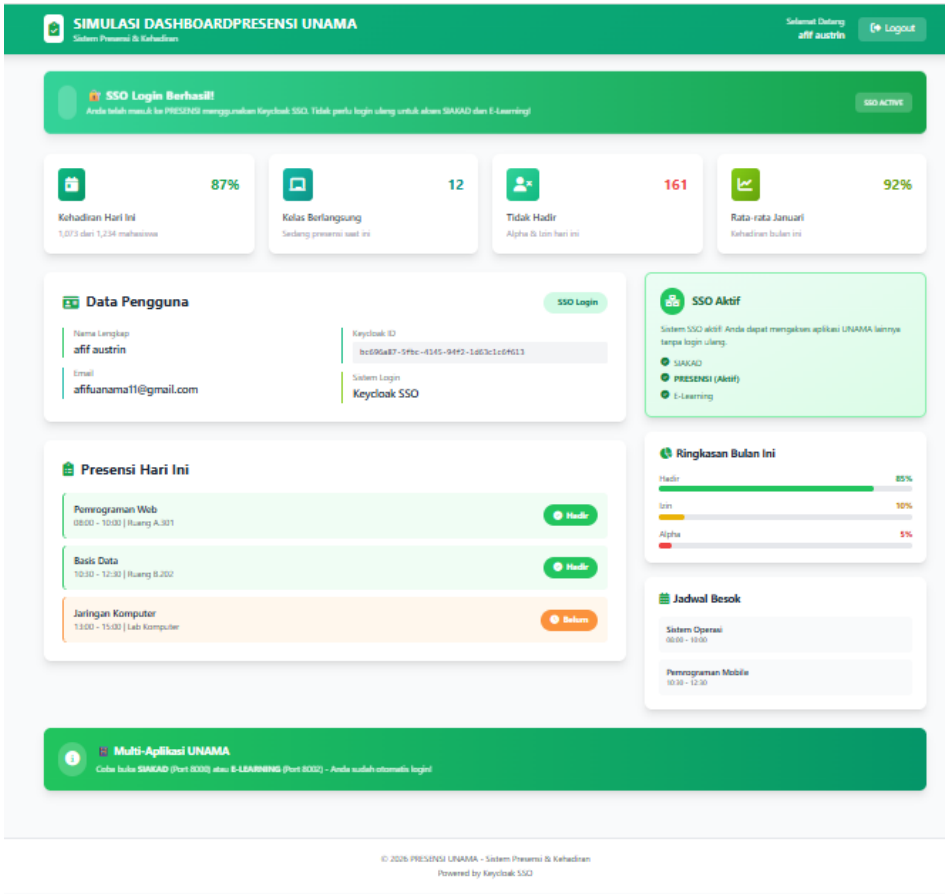
Gambar 5. 5 dashboard *SIAKAD*

Pada halaman ini ditampilkan informasi identitas pengguna seperti nama, email, dan peran (mahasiswa atau dosen) yang diperoleh dari server *Keycloak*. Selain itu, dashboard menyediakan menu akses ke fitur-fitur akademik seperti data mahasiswa, jadwal perkuliahan, nilai, dan informasi akademik lainnya. Dengan mekanisme SSO, pengguna dapat mengakses

seluruh layanan *SIAKAD* tanpa perlu melakukan login ulang bisa di lihat di gambar 5.5.

6. Halaman dashboard *Presensi*

Dashboard *Presensi* merupakan halaman utama yang muncul setelah pengguna berhasil login melalui sistem SSO.



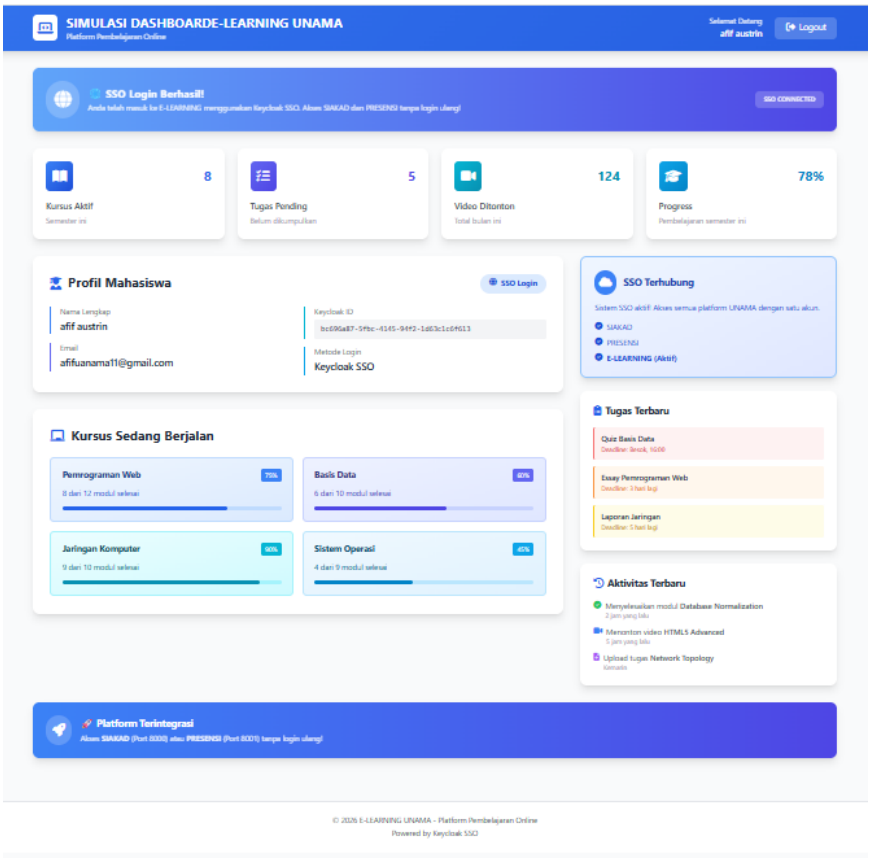
Gambar 5. 6 dashboard *presensi*

Pada halaman ini, mahasiswa dapat melakukan *presensi* kehadiran, sedangkan dapat memantau dan memverifikasi kehadiran mahasiswa. Informasi pengguna yang ditampilkan pada dashboard diambil dari server SSO, sehingga sistem *presensi* dapat memastikan bahwa hanya pengguna

yang telah terautentikasi yang dapat mengakses fitur ini bisa dilihat di gambar 5.6.

7. Halaman dashboard *E-learning*

Dashboard *E-learning* ditampilkan setelah pengguna berhasil terautentikasi melalui SSO.



Gambar 5. 7 dashboard *e-learning*

Halaman ini berfungsi sebagai pusat aktivitas pembelajaran daring, di mana mahasiswa dapat melihat daftar mata kuliah yang diikuti, materi perkuliahan, dan tugas, sedangkandapat mengelola kelas, mengunggah materi, dan memberikan penilaian. Identitas pengguna yang ditampilkan pada dashboard diperoleh langsung dari sistem SSO, sehingga konsistensi data pengguna tetap terjaga di seluruh aplikasi bisa dilihat di gambar 5.7.

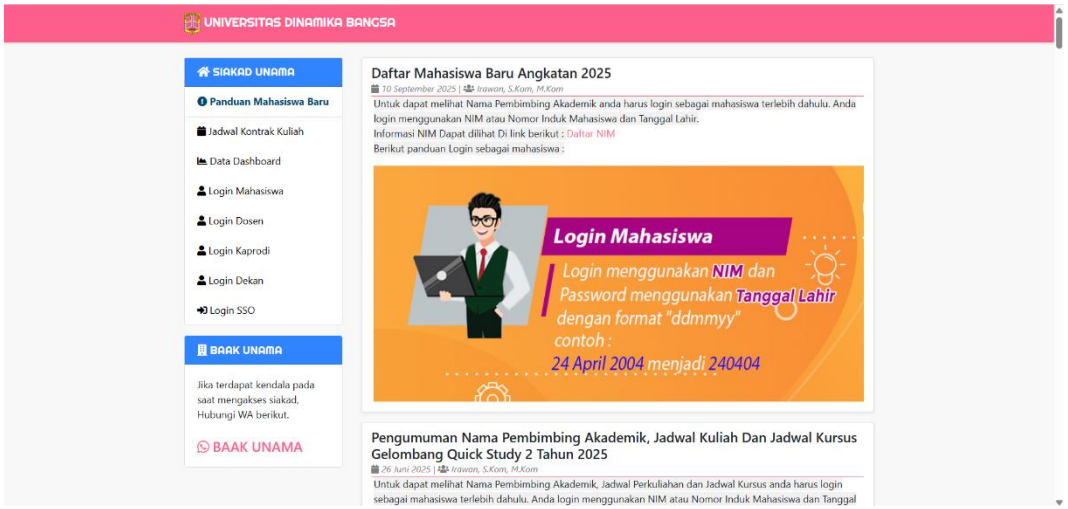
Proses Logout pada Sistem SSO logout pada sistem *Single Sign-On (SSO)* UNAMA dilakukan secara terpusat melalui *Keycloak* sebagai Identity Provider. Ketika pengguna menekan tombol Logout pada salah satu aplikasi, seperti *SIAKAD*, *E-learning*, atau *Presensi*, sistem tidak hanya mengakhiri sesi pada aplikasi tersebut, tetapi juga mengirimkan permintaan logout ke server *Keycloak*.

Keycloak kemudian akan menghapus sesi autentikasi pengguna yang sedang aktif. Setelah sesi di *Keycloak* diakhiri, seluruh aplikasi yang terhubung dengan sistem SSO secara otomatis kehilangan status login pengguna. Dengan demikian, pengguna akan keluar dari semua aplikasi yang terintegrasi tanpa perlu melakukan logout satu per satu.

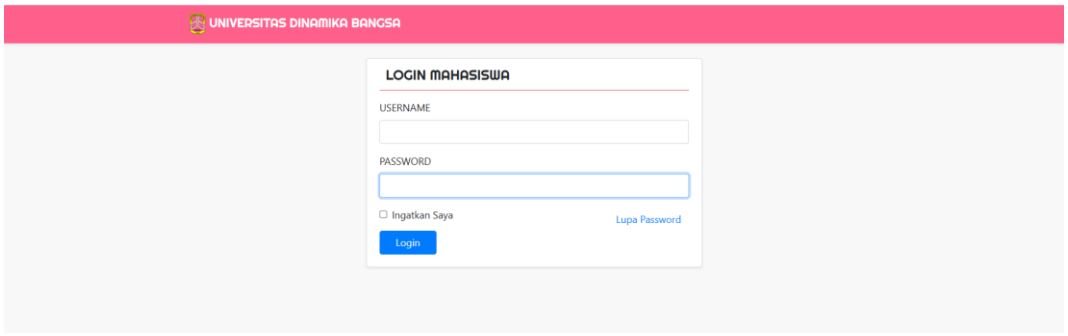
Setelah proses logout berhasil, pengguna akan diarahkan kembali ke halaman login SSO. Jika pengguna ingin mengakses kembali salah satu aplikasi, maka ia harus melakukan proses login ulang melalui halaman login *Keycloak*. Mekanisme ini memastikan keamanan sistem karena tidak ada sesi aktif yang tersisa setelah pengguna keluar dari sistem.

5.2 Mekanisme Login Sistem Akademik Sebelum Penerapan SSO

Gambar di bawah ini menampilkan halaman login Sistem Informasi Akademik (*SIAKAD*) Universitas Dinamika Bangsa yang digunakan sebelum penerapan *Single Sign-On* (SSO).



Gambar 5. 8 mekanisme login sebelum penerapkan SSO



Gambar 5. 9 halaman dashboard login UNAMA

Gambar tersebut menampilkan halaman login Sistem Informasi Akademik (*SIAKAD*) Universitas Dinamika Bangsa yang digunakan sebelum penerapan *Single Sign-On* (SSO). Pada tampilan ini, pengguna diharuskan memilih jenis login sesuai dengan perannya, seperti mahasiswa, dosen, kaprodi, atau dekan melalui menu yang tersedia di sisi kiri halaman.

Untuk dapat masuk ke sistem, mahasiswa diwajibkan mengisi Nomor Induk Mahasiswa (NIM) sebagai username dan tanggal lahir sebagai password sesuai dengan format yang telah ditentukan. Proses autentikasi ini dilakukan secara langsung oleh aplikasi *SIAKAD*, tanpa melibatkan sistem autentikasi terpusat.

Model login seperti ini mengharuskan setiap aplikasi, seperti *SIAKAD*, *Presensi*, dan *E-learning*, memiliki mekanisme login dan basis data pengguna sendiri. Akibatnya, pengguna harus melakukan login berulang kali jika ingin mengakses lebih dari satu aplikasi, meskipun menggunakan akun yang sama. Kondisi inilah yang menjadi salah satu latar belakang perlunya penerapan sistem *Single Sign-On* (SSO) pada lingkungan Universitas Dinamika Bangsa berikut perbandingan menggunakan SSO dan tidak menggunakan SSO :

Tabel 5. 1 penerapan SSO dan tidak SSO

Aspek	**Tanpa SSO (*SIAKAD* Lama)**	**Dengan SSO (Keycloak)**
Sistem login	Setiap aplikasi memiliki halaman login sendiri	Semua aplikasi menggunakan satu login terpusat
Tempat validasi akun	Di masing-masing aplikasi (*SIAKAD*, *Presensi*, *E-learning*)	Di server SSO (Keycloak)
Data akun	Tersimpan di database masing-masing aplikasi	Tersimpan terpusat di Keycloak
Cara login	Login dengan NIM/NIP dan password di setiap aplikasi	Login satu kali di halaman UNAMA-SSO
Jumlah login	Harus login ulang di setiap aplikasi	Cukup login sekali untuk semua aplikasi
Keamanan	Kurang terkontrol karena tersebar	Lebih aman karena terpusat
Manajemen pengguna	Sulit karena data tersebar	Mudah karena dikelola di satu server
Pengalaman pengguna	Tidak efisien dan merepotkan	Lebih praktis dan cepat

5.3 PENGUJIAN SISTEM

Pengujian sistem dilakukan untuk memastikan bahwa seluruh fungsi pada sistem *Single Sign-On* (SSO) Universitas Dinamika Bangsa telah berjalan sesuai dengan perancangan dan kebutuhan pengguna. Pengujian ini bertujuan untuk

memverifikasi bahwa proses autentikasi, integrasi antar aplikasi, serta pengelolaan sesi pengguna dapat bekerja secara benar, aman, dan konsisten.

Pengujian dilakukan dengan pendekatan black-box testing, yaitu pengujian yang berfokus pada fungsi sistem tanpa memperhatikan struktur kode di dalamnya. Setiap fitur diuji berdasarkan input yang diberikan oleh pengguna dan output yang dihasilkan oleh sistem.

Dalam pengujian ini, penulis melakukan simulasi login sebagai mahasiswa melalui halaman login terpusat UNAMA-SSO, kemudian mengakses aplikasi *SIAKAD*, *Presensi*, dan *E-learning* untuk memastikan bahwa mekanisme *Single Sign-On* berfungsi dengan baik berikut hasil pengujian :

Tabel 5. 2 pengujian sistem

No	Skenario Pengujian	Langkah Pengujian	Hasil yang Diharapkan	Hasil
1	Login manual *SIAKAD* dengan data valid	Pengguna membuka halaman login *SIAKAD*, memasukkan email dan password yang valid, lalu menekan tombol Login	Sistem memverifikasi data dan menampilkan dashboard *SIAKAD*	Berhasil
2	Login manual *SIAKAD* dengan data tidak valid	Pengguna memasukkan email atau password yang salah	Sistem menolak login dan menampilkan pesan kesalahan	Berhasil
3	Login *SIAKAD* menggunakan Keycloak SSO	Pengguna menekan tombol Login with Keycloak SSO pada halaman *SIAKAD*	Sistem mengarahkan ke halaman login terpusat dan berhasil masuk ke *SIAKAD*	Berhasil
4	Akses *Presensi* setelah login	Pengguna membuka aplikasi *Presensi* setelah login di *SIAKAD*	Sistem langsung menampilkan halaman *Presensi* tanpa login ulang	Berhasil

	SIAKAD (SSO)			
5	Akses *E-learning* setelah login *SIAKAD* (SSO)	Pengguna membuka aplikasi *E-learning* setelah login di *SIAKAD*	Sistem langsung menampilkan halaman *E-learning* tanpa login ulang	Berhasil
6	Login manual *Presensi* dengan data valid	Pengguna membuka halaman login *Presensi* dan memasukkan kredensial yang benar	Sistem menampilkan dashboard *Presensi*	Berhasil
7	Login manual *E-learning* dengan data valid	Pengguna membuka halaman login *E-learning* dan memasukkan kredensial yang benar	Sistem menampilkan dashboard *E-learning*	Berhasil
8	Login SSO pada *Presensi*	Pengguna menekan tombol Login with Keycloak SSO pada *Presensi*	Sistem berhasil login dan menampilkan halaman utama *Presensi*	Berhasil
9	Login SSO pada *E-learning*	Pengguna menekan tombol Login with Keycloak SSO pada *E-learning*	Sistem berhasil login dan menampilkan halaman utama *E-learning*	Berhasil
10	Logout dari sistem	Pengguna menekan tombol Logout pada salah satu aplikasi	Sistem mengakhiri sesi dan mengarahkan ke halaman login	Berhasil
11	Akses aplikasi setelah logout	Pengguna membuka kembali *SIAKAD*, *Presensi*, atau *E-learning*	Sistem menampilkan halaman login terpusat SSO	Berhasil

Pengujian modul *Single Sign-On* (SSO) dilakukan untuk memastikan integrasi autentikasi terpusat antar-layanan digital berjalan dengan lancar dan aman.

Pengujian ini mencakup validasi akses lintas aplikasi (*SIAKAD*, *Presensi*, dan *E-learning*), manajemen sesi pengguna, serta keandalan sistem dalam menangani kesalahan kredensial. Hasil pengujian secara detail dapat dilihat pada Tabel 5.4.

5.4 ANALISIS YANG DICAPAI

Berdasarkan hasil perancangan dan implementasi sistem *Single Sign-On* (SSO) menggunakan Keycloak pada lingkungan Universitas Dinamika Bangsa, diperoleh beberapa capaian utama sebagai berikut:

1. Terbentuknya Sistem Autentikasi Terpusat

   Sistem autentikasi pengguna yang sebelumnya terpisah pada setiap aplikasi (*SIAKAD*, *Presensi*, dan *E-learning*) kini berhasil dipusatkan melalui Keycloak sebagai Identity Provider. Mahasiswa hanya perlu memiliki satu akun untuk mengakses seluruh aplikasi yang terintegrasi.

2. Keberhasilan Implementasi Login SSO

   Pengguna dapat melakukan login melalui halaman UNAMA-SSO, kemudian secara otomatis memperoleh akses ke aplikasi *SIAKAD*, *Presensi*, dan *E-learning* tanpa perlu melakukan login ulang. Hal ini membuktikan bahwa mekanisme *Single Sign-On* berjalan dengan baik.

3. Integrasi Laravel dengan Keycloak Berhasil Dilakukan

   Aplikasi *SIAKAD* berbasis Laravel berhasil diintegrasikan dengan Keycloak menggunakan protokol *OpenID Connect* (OIDC). Laravel dapat menerima token autentikasi dari Keycloak dan membentuk sesi pengguna berdasarkan data yang terdapat pada token tersebut.

4. Pengelolaan Pengguna dan Peran Lebih Terstruktur

   Pengelolaan akun pengguna (mahasiswa dan dosen) serta pengaturan peran (roles) berhasil dilakukan melalui Keycloak. Hak akses pengguna terhadap aplikasi dapat diatur secara terpusat sesuai dengan perannya.

5. Peningkatan Keamanan Sistem

   Password pengguna tidak lagi disimpan pada masing-masing aplikasi, melainkan dikelola oleh Keycloak. Aplikasi hanya menerima token autentikasi, sehingga risiko kebocoran kredensial dapat dikurangi.

6. Peningkatan Efisiensi dan Kenyamanan Pengguna

   Dengan adanya SSO, pengguna tidak perlu lagi mengingat banyak username dan password. Proses login menjadi lebih cepat, praktis, dan nyaman.