PERNYATAAN ORISINILITAS PENELITIAN

PERNYATAAN

Saya yang bertanda tangan dibawah ini, menyatakan bahwa tugas akhir yang saya ajukan ini adalah hasil karya saya sendiri, tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu perguruan tinggi atau karya yang pernah ditulis atau diterbitkan oleh orang lain kecuali yang secara tertulis diacu dalam naskah ini disebutkan dalam daftar pustaka. Karya ini adalah milik saya dan pertanggungjawaban sepenuhnya berada di pundak saya.

Bandar Lampung, September 2019

TIO ADITYA PUTRA

NPM 1511010077

HALAMAN PERSETUJUAN

Judul Skirpsi : PENERAPAN SISTEM SINGLE SIGN-ON BERBASIS WEB PADA INSTITUT INFORMATIKA DAN BISNIS DARMAJAYA.

Nama Mahasiswa : **Tio Aditya Putra**

No. Pokok Mahasiswa : 1511010077

Jurusan : Teknik Informatika

Menyetujui,

Dosen Pembimbing	Ketua Jurusan
Sulyono, S.Kom., M.Ti	**Yuni Arkhiansyah, S.Kom., M.Kom**
NIK. 00480802	**NIK. 00480802**

HALAMAN PENGESAHAN

Telah Diuji dan Dipertahankan Didepan Tim Penguji Skripsi
Jurusan Teknik Informatika Insitut Informatika dan Bisnis Darmajaya
Bandar Lampung dan Dinyatakan Diterima untuk
Memenuhi Syarat Guna Memperoleh
Gelar Sarjana Komputer

Mengesahkan

1. Tim Penguji **Tanda Tangan**

Ketua : Yuni Arkhiansyah, S.Kom., M.Kom .....

Anggota : Rionaldi Ali, S.Kom., M.Ti .....

2. Dekan Fakultas Ilmu Komputer

Sriyanto,S.Kom.,M.M

NIK. 00210800

ABSTRACT

APPLICATION OF WEB-BASED SINGLE SIGN-ON SYSTEM IN DARMAJAYA INFORMATICS AND BUSINESS INSTITUTE

By:
Tio Aditya Putra

In this technological era, single sign-on technology is a technology of interest, especially in very large and heterogeneous networks (in the current operating system and applications used by computers from many vendors are asked to fill the information itself to each different platform to be accessed by users). By using SSO, users only have to try to authenticate once to get permission, access to all services contained in the network. By using the OAuth2 protocol, users can authorize clients to access protected data already on the server by providing tokens without submitting usernames and passwords. OAuth2 allows users to provide access to third party sites to access information stored with other service providers without having to share access rights or all their data. Single sign-on systems with the OAuth2 protocol used are authentication technologies with a sign code instead of username and passwords. This research can make it easier for users to authenticate applications by using an account provider that supports the OAuth2 protocol.

Keywords: single sign-on system, sso, web portal

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Dengan pesatnya perkembangan teknologi informasi dan internet, banyak institusi atau perusahaan yang menyediakan berbagai layanan berbasis website yang saling terintegrasi satu sama lain. Layanan *web* sendiri memiliki kelebihan yaitu bisa diakses dari manapun dan kapanpun. Namun layanan *web* sendiri memiliki kelemahan yaitu karena bisa diakses dari manapun dan kapapun maka layanan website rentang terhadap berbagi serangan yang dilakukan oleh para *cracker*. Selain itu jika setiap aplikasi memiliki sistem login yang sendiri sendiri maka bisa membuat beban server menjadi lebih berat karena server harus melayani request login *user* yang ingin mengakses semua layanan yang tersedia. Untuk itu ada sistem *Single Sign-On* yang bisa menggabungkan sistem *authentifikasi* login dari beberapa aplikasi menjadi satu dan juga penyimpanan data *user* menjadi terpusat sehingga bisa membuat beban server menjadi lebih ringan karena server hanya perlu melayani satu kali *request* login user yang ingin mengakses semua layanan yang disediakan.

SSO adalah sebuah sistem dimana pengguna cukup menggunakan satu *username* dan *password* untuk mengakses dan menggunakan layanan pada semua aplikasi yang ada. Sistem *SSO* memberikan efisiensi dan keamanan bagi pengguna dalam mengelola serta mengakses berbagai layanan aplikasi. Dengan adanya *SSO* semua aplikasi yang ada dimasukkan kedalam sebuah *site* sehingga terbentuk sebuah integrasi aplikasi dalam bentuk *web* portal. Pengguna hanya perlu satu kali *login* agar bisa menggunakan semua aplikasi yang ada didalam *web* portal tersebut. Pengguna juga tidak perlu menghafal banyak *account,* cukup satu *account.* Dengan demikian pengorganisasian data pengguna dapat dipermudah, sehingga keamanan data pengguna lebih terjamin, karena tempat yang digunakan untuk penyimpanan data pengguna menjadi terpusat.

Menjadi suatu masalah ketika seorang pengguna memiliki banyak aplikasi *web* yang membutuhkan otentikasi. Dia harus banyak menghafal banyak *password*, walaupun banyak orang membuat *password* yang sama untuk berbagai aplikasi *web*. Terdapat masalah lagi jika pengguna membuat satu *password* untuk berbagai aplikasi *web*, karena pengguna harus memasukkan *password* berulang kali. Oleh karena itu dibutuhkan suatu sistem yang dapat mengintegrasikan seluruh layanan aplikasi dan mengelola proses autentikasi masing-masing sistem layanan, menjadi proses autentikasi. Proses autentikasi pada sistem yang terintegrasi ini memerlukan sebuah sistem tambahan yang menjadi penghubung antara sistem *integrator* dengan sistem layanan aplikasi.

Untuk itu salah satu solusi terhadap sistem otentikasi pengguna secara terpusat agar dapat mengakses semua aplikasi di Institut Informatika dan Bisnis Darmajaya yang diharap dapat diterapkan dilakukan dengan cara melakukan penerapan *SSO* yang dimana pada penelitian ini bisa membantu untuk kemudahan dan keamanan pengguna dalam mengakses semua aplikasi. Berdasarkan latar belakang yang telah disampaikan, maka dibuatlah suatu penelitian dengan judul "**PENERAPAN SISTEM *SINGLE SIGN-ON* BERBASIS WEB PADA INSTITUT INFORMATIKA DAN BISNIS DARMAJAYA**" yang diharapkan membantu mahasiswa agar lebih mudah mengakses website dengan hanya sekali login.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijabarkan diatas maka rumusan masalah untuk pembuatan sistem login adalah :

a. Apakah metode *Single Sign-On* dapat diterapkan untuk autentikasi akun pengguna pada beberapa aplikasi yang terdaftar dalam sistem?
b. Apakah sistem dapat mengjinkan pengguna untuk login pada aplikasi tersebut atau autentikasi secara otomatis dan registrasi data secara otomatis?
c. Apakah sistem dapat mengijinkan autentikasi pengguna menggunakan autentikasi eksternal dari media sosial seperti *Facebook*, *Google*?

1.3 Batasan Masalah

Berdasarkan rumusan masalah di atas, maka batasan-batasan masalah dalam penelitian ini adalah :

1. Penelitian sistem *single sign-on* yang dibangun berbasis *web*.
2. Kategori sistem *single sign-on* yang dibangun berbasis Authentication (*Autentikasi*) Ouath2.
3. Tidak membahas manajemen akun.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai peneliti pada penelitian ini adalah sebagai berikut :

a. Membangun sistem *Single Sign-On* yang dapat diakses Mahasiswa IIB Darmajaya.
b. Membantu mahasiswa dalam mengakses *web* login tanpa perlu mengingat banyak password.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah sebagai berikut:

1. Memberikan inovasi baru bagi semua kalangan tentang manfaat Sistem *Single Sign-On.*
2. Bisa memahami Teknologi *Single Sign-On* dengan baik untuk kemudahan dan keamanan pengguna.
3. Memahami kelebihan dan kekurangan dari sistem dalam mengintegrasikan aplikasi yang sebelumnya masih terpisah, yang akan diuji coba diterapkan di Institut Informatika dan Bisnis Darmajaya.
4. Memberikan keamanan pada mahasiswa karena tidak perlu menghafal lebih dari satu *username* dan *password.*
5. Untuk penulis dapat memahami, menambah wawasan berpikir dan meningkatkan pengetahuan terhadap sistem yang aman untuk pengguna.

1.6 Sistematika Penulisan

Uraian singkat mengenai sistematika penulisan pada masing-masing bab adalah sebagai beriku :

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang masalah, perumusan masalah, ruang lingkup penelitian, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini berisi tentang teori-teori yang mendukung penelitian yang akan dilakukan oleh penulis/peneliti.

BAB III METODOLOGI PENELITIAN

Bab ini berisi tentang metode-metode pendekatan penyelesaian permasalahan yang dinyatakan dalam perumusan masalah pada penelitian yang dilakukan.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab ini berisi tentang pemaparan hasil analisa persoalan yang dibahas dengan berpedoman pada teori-teori yang dikemukakan pada Bab II.

BAB V SIMPULAN DAN SARAN

Bab ini berisi tentang rangkuman dari pembahasan, yang terdiri dari jawaban atas perumusan masalah, tujuan

penelitian, dan hipotesis. Selain itu berisi tentang saran bagi perusahaan/instansi (objek penelitian) dan saran untuk penelitian selanjutnya, sebagai hasil pemikiran penelitian atas keterbatasan penelitian yang dilakukan.

DAFTAR PUSTAKA

LAMPIRAN

BAB II
LANDASAN TEORI

2.1 *Single Sign-On* (SSO)

Teknologi *Single Sign-On* (sering disingkat menjadi SSO) adalah suatu teknologi yang mengizinkan pengguna jaringan agar dapat mengakses sumber daya dalam jaringan hanya dengan menggunakan satu akun pengguna saja. Dengan menggunakan SSO, seorang pengguna hanya cukup melakukan proses autentikasi sekali saja untuk mendapatkan izin akses terhadap semua layanan yang terdapat didalam jaringan. Untuk menggabungkan beberapa aplikasinya maka dibutuhkan site yang dikenal dengan *web portal*. Dengan adanya *web portal* ini menggunakan metode *Single Sign On*, berarti user hanya memerlukan satu *username* dan satu *password*. Dan apabila ingin mendapatkan layanan atau fasilitas di *web portal*, user hanya perlu login satu kali saja agar bisa menggunakan semua fasilitas atau layanan aplikasi yang ada dalam *web portal* tersebut. Ini mempermudah user menggunakan aplikasi yang ada karena user tidak perlu menghapal banyak account, cukup satu account dan tidak perlu berulang kali login untuk mendapatkan layanan atau fasilitas yang ada pada *web portal*. Hal ini juga mempermudah dalam pengorganisasian data user yang ada, sehingga keamanan data user lebih terjamin, karena menggunakan sebuah tempat penyimpanan data user yang terpusat.

Beberapa kategori sistem Sistem s*ingle sign-on* yaitu:

1. **Autentikasi (*Authentication*)**

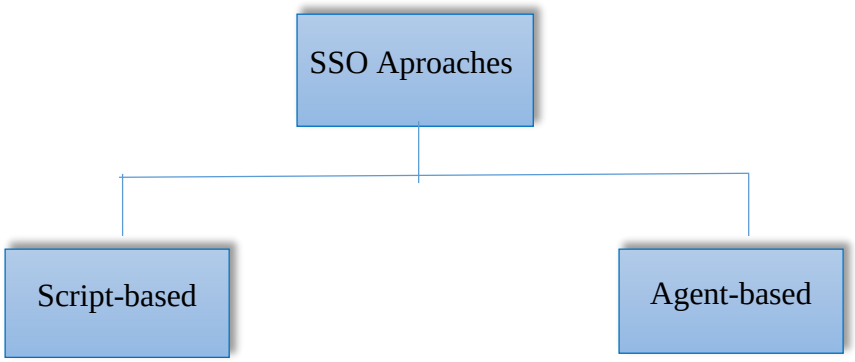
   Sistem *single sign-on* berbasis autentikasi yang mana SSO *server* hanya memberikan *services* apakah *user* A telah ter-autentikasi atau belum, SSO *server* tidak melakukan proses otorisasi atas *user* yang sedang aktif tersebut. *Authentication* dapat dikenali dengan memberikan kerahasiaan informasi seperti *password, pin,* atau *private key*. Dengan memberikan salah satu kerahasiaan informasi tersebut situs *web* dapat mengenali identitas pengunjung misalnya *authentication* menggunakan proses *login* dengan memasukkan *username* dan *password* yang benar maka situs *web*

akan mengenali pengunjung tersebut. *Authentication* memerlukan sebuah kerahasiaan dari seorang pengguna aplikasi *web* agar dapat dikenali, maka setiap kali mengakses situs *web* yang memerlukan *authentication*. Pengguna harus memasukkan *username* dan *password* untuk mengakses setiap situs *web* tersebut. Proses ini akan mempersulit pengguna aplikasi karena setiap kali mengakses situs *web* yang berbeda pengguna harus melakukan *login* ulang jika mengakses *server* yang berbeda, untuk mengatasi hal tersebut dapat menggunakan *authorization.*

2. Otoriasi (*Authorization*)

Tugas SSO *server* untuk SSO-otorisasi memiliki tugas sedikit lebih berat, karena setelah memastikan *user* telah ter-autentikasi, SSO *server* masih harus menghandle otorisasi *user* tersebut.

3. Arsitektur Sistem SSO



Gambar 2.1 Pendekatan Sistem SSO

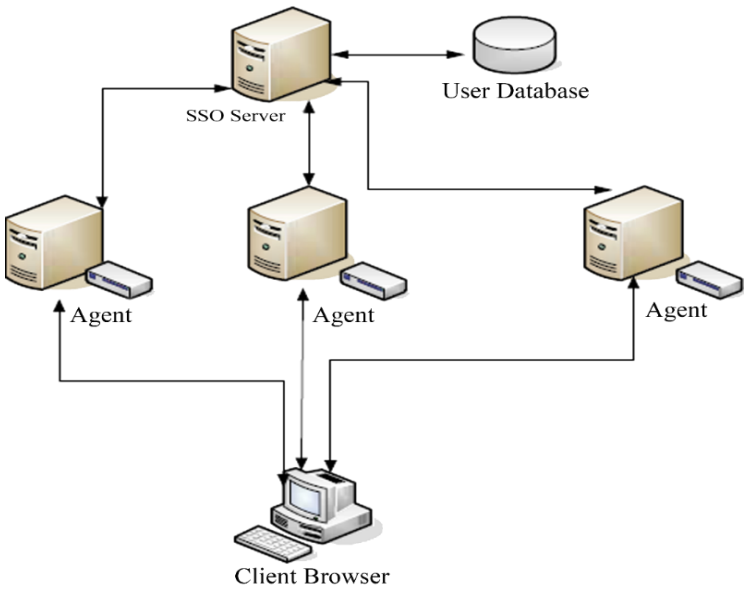
(Sumber : Springer-Verlag Berlin Heidelberg, 2003)

Solusi sistem SSO didasarkan pada salah satu dari dua tingkat pendekatan-pendekatan *script* dan pendekatan *agent*. Pendekatan agent lebih digunakan dalam Tugas Akhir ini karena dianggap lebih cocok untuk aplikasi berbasis

web atau *services provider* (SP). Gambar 2.1 menunjukkan pembagian dari pendekatan sistem SSO.

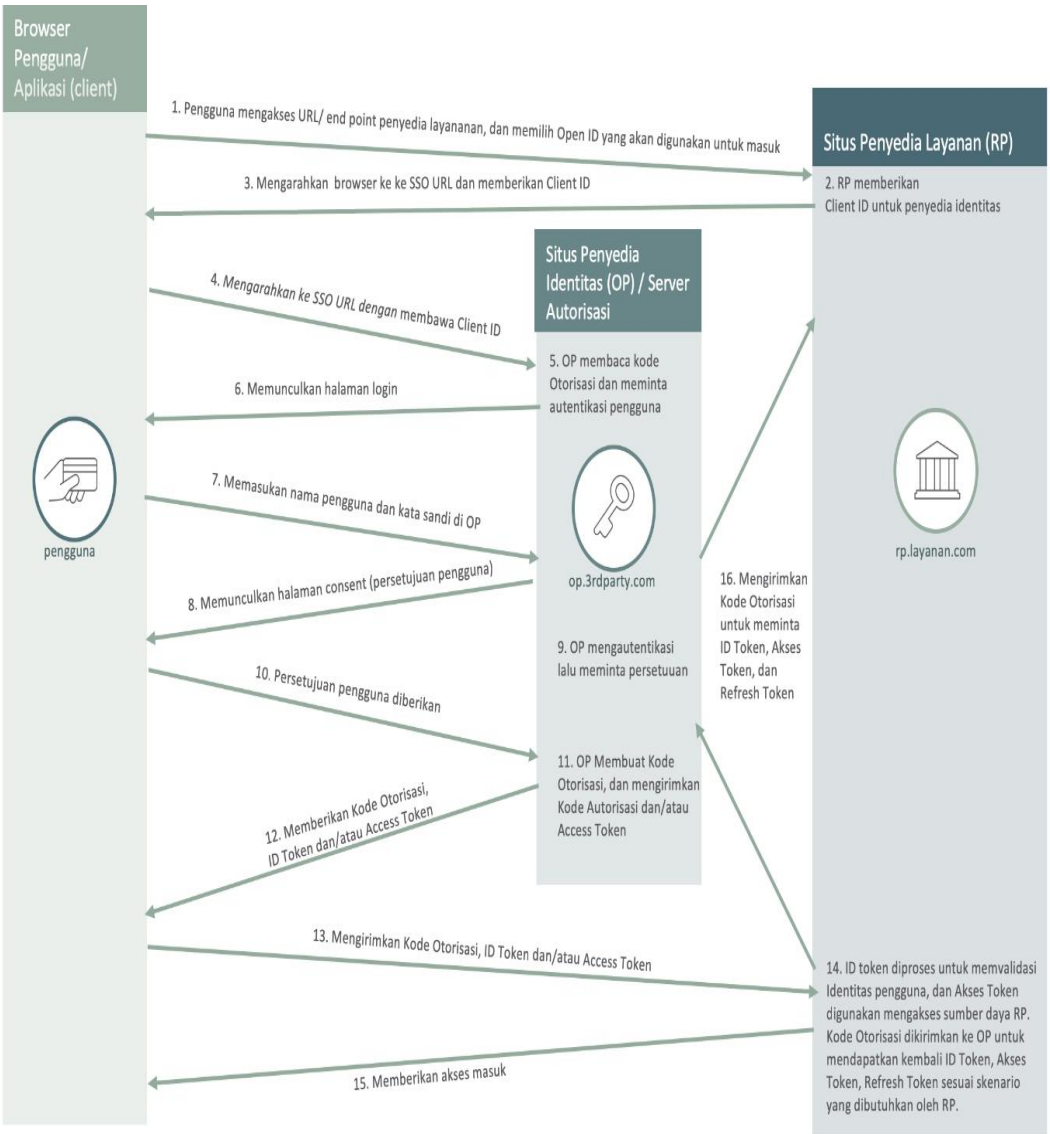
Agent merupakan sebuah program kecil yang berjalan pada tiap-tiap *web server*. *Agent* ini membantu mengkoordinir aliran kerja dari SSO dalam hal otentikasi pengguna dan penanganan sesi. Solusi dari arsitektur sistem SSO ditunjukkan oleh Gambar 2.2. Arsitektur SSO memiliki dua bagian utama; *agent* yang berada di *web server* atau SP dan sebuah *server* SSO yang berdedikasi yang mana akan dijelaskan berikut ini :

1. ***Agent* :** Sebuah *agent* menterjemahkan setiap permintaan HTTP yang masuk ke *web server*. Hanya ada satu *agent* di tiap-tiap *web server*, yang mana *host* bagi aplikasi/SP. *Agent* tersebut akan berinteraksi dengan *browser* klien pada sisi pengguna, dan dengan *server* SSO pada sisi SP.
2. **SSO *server* :** *server* SSO menggunakan *cookies temporer* (sementara) untuk menyediakan fungsi manajemen sesi. Sebuah *cookies* terdiri dari informasi seperti *user-id, session-id, session creation time, session expiration time* dan lain-lain.



Gambar 2.2 Arsitektur Sistem SSO

(Sumber : Springer-Verlag Berlin Heidelberg, 2003)



Gambar 2.3 Cara kerja SSO

2.2 Pengertian *Handshaking*

Handshaking adalah proses negosiasi otomatis yang secara dinamis menentukan parameter dalam pembentukan kanal komunikasi Antara dua entitas normal sebelum komunikasi melalui kanal dimulai. Seperti ketika komputer berkomunikasi dengan perangkat lain seperti printer, modem, atau server jaringan. Salah satu contoh klasik adalah handshaking modem, yang biasanya bernegosiasi parameter komunikasi untuk periode singkat bila sambungan pertama kali

didirikan, dan setelah itu gunakan parameter untuk memberikan mentransfer informasi yang optimal melalui saluran sebagai fungsi dari kualitas dan kapasistas.

Handshaking memungkinkan untuk menghubungkan system yang relative heterogen atau peralatan melalui saluran komunikasi tanpa membutuhkan intervensi manusia untuk mengatur parameter.

Proses negosiasi SSL atau "*Handshake*" melibatkan pertukaran *cryptographic keys*, *certificate*, dan informasi lain, random data digunakan untuk membuat enkripsi satu waktu, dan valuenya digunakan untuk mengindentifikasi SSL yang dibuat dari Handshake. Handshake memiliki tiga tujuan :

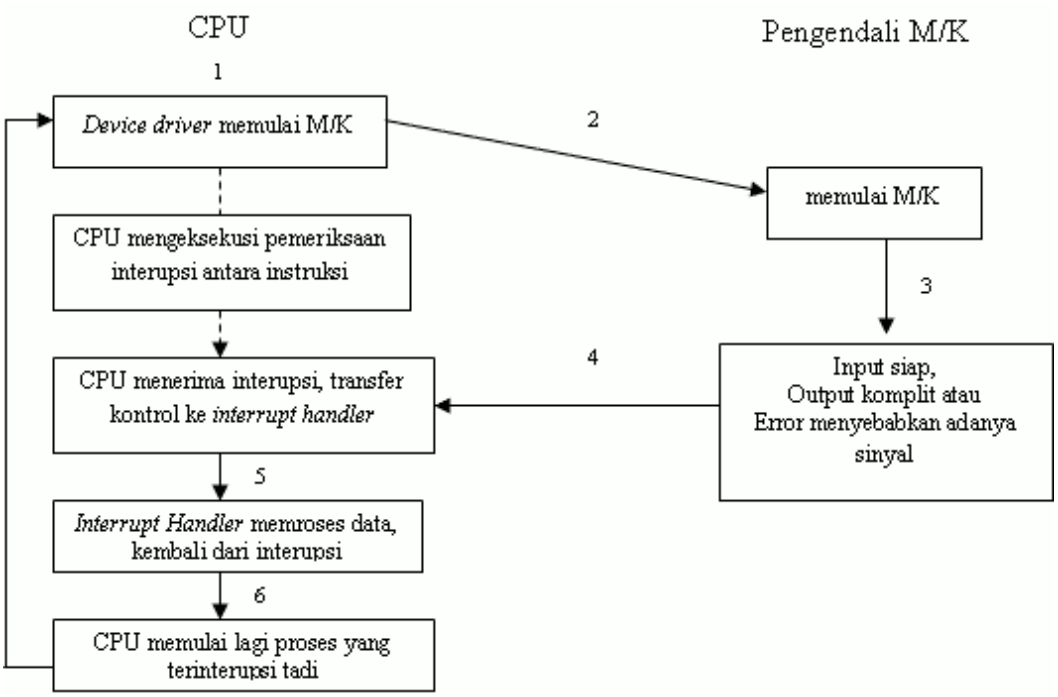
1. Untuk membolehkan *client* dan *server* setuju mengenai algoritma yang akan mereka gunakan.
2. Untuk melibatkan kumpulan dari *crypto keys* untuk digunakan oleh algoritma tersebut.
3. Untuk mengautentikasi *client.*

Handshaking memungkinkan terjadinya sesi komunikasi data yang berlangsung dari mulai perencanaan komunikasi sampai dengan komunikasi tersebut selesai. Proses ini diawali proses prakomunikasi, yaitu proses pencarian host tujuan (*destination*) oleh host yang bertindak sebagai pengirim. Proses ini diakhiri dengan kesepakatan antara kedua belah pihak untuk melaksanakan pertukaran data (*connection establish*), yaitu proses pengiriman informasi berupa request dan tanggapan antara kedua belah pihak.

Dua proses awal ini disebut proses pembentukan koneksi. Artinya untuk melakukan komunikasi, perangkat yang dituju harus menerima koneksi awalan terlebih dahulu sebelum mengirimkan data atau menerima data. Proses yang dilakukan sebelum pengiriman data terdiri atas :

1. Pengirim (*sender*) mengirimkan sinyal sinkronasi (SYN) terlebih dulu ke tujuan.
2. Penerima akan membalas sinyal SYN dengan *Negotiate Connection*.

3. Penerima mengirimkan SYN ulang, apa benar pengirim akan mengirimkan data.
4. Pengirim akan membalas dengan sinyal *Acknowledge* (*ACK*), artinya sudah siap untuk mengirimkan data sampai saat ini. Prosesnya telah mencapai status *Connection Establish*.
5. Kemudian segmen data dikirim. Proses terakhir adalah ketika terjadi pengiriman kodeBYE atau *FIN ACK* atau *CLOSED* atau kode lainnya bergantung aplikasi komunikasi yang digunakan.



Gambar 2.4 Cara kerja *Handshake*

2.3 Aspek-Aspek Keamanan Komputer

Keamanan computer meliputi beberapa aspek diantaranya (Adid Dana, 2018) :

1. *Authentication* : penerima informasi dapat memastikan keaslian sebuah pesan, bahwa dengan pesan itu dating dari orang yang diminta informasi. Dengan kata lain, informasi itu dating dari orang yang benar benar di kehendaki.

2. *Integrity* : keaslian sebuah pesan yang dikirim melalui jaringan dapat dipastikan informasi yang dikirim tersebut tidak dimodifikasi orang yang tidak berhak.
3. *Non-repudiation* : merupakan hal yang berhubungan dengan pengirim. Pengirim tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut.
4. *Authority* : informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak mengaksesnya.
5. *Confidentiality* : sebuah usaha untuk menjaga informasi dari orang yang tidak berhak mengaksesnya. Kerahasiaan ini biasanya berhubungan dengan informasi yang diberikan ke pihak lain.
6. *Privacy* : data-data yang bersifat pribadi.
7. *Availability* :Berhubungan dengan ketersediaan informasi yang dimana nantinya dibutuhkan. Sistem informasi yang diserang ataupun di jebol dapat menghambat atau meniadakannya akses ke suatu informasi.
8. *Access Control* : berhubungan dengan cara pengaturan akses ke suatu informasi. Biasanya berhubungan dengan masalah otentikasi dan sebuah privasi. Kontrol akses seringkali dilakukan dengan menggunakan kombinasi *user id* dan *password* ataupun dengan mekanisme lainnya.

2.4 Metode-Metode Identifikasi dan Otentikasi

Elemen *interface* yang pertama kali ditemui kebanyakan subjek ketika mengakses sistem informasi adalah identifikasi dan otentikasi. Tahap identifikasi memperkenankan subjek mengklaim sebagai entitas tertentu dengan menunjukkan bukti-bukti identitas. Bukti-bukti tersebut dapat berupa ID pengguna atau nomor PIN (*Personal Identification Number*), atau yang lebih kompleks seperti atribut fisik. Setelah subjek mengklaim suatu identitas, sistem memvalidasi apakah pengguna tersebut terdaftar dalam *database* pengguna dan membuktikan bahwa subjek tersebut adalah benar-benar sebagai entitas yang diklaimnya.

Tahap otentikasi meminta objek menunjukkan informasi tambahan yang sesuai dengan informasi tentang subjek tersebut yang telah disimpan. Dua tahap ini sering disebut dengan otentikasi dua factor, yang memberikan proteksi terhadap subjek yang tidak memiliki otoritas untuk mengakses sistem. Setelah subjek di otentikasi, sistem control akses mengevaluasi hak dan izin subjek untuk mengabulkan atau menolak permintaan terhadap objek. Tahap ini disebut dengan tahap otoritas.

Tabel 2.1 Tipe-Tipe Otentikasi

Authentication Type	Description	Examples
Type 1	What you know	**Password, passphrase, PIN, lock combination**
Type 2	What you have	**Smart card, token device**
Type 3	What you are	**Biometrics,-fingerprint, palm print, retina/iris pattern, voice pattern.**

Ada tipe kategori/tipe umum dari informasi otentikasi. Praktek pengamanan yang baik biasanya membuat tahap identifikasi dan otentikasinya memerlukan input setidaknya dari dua tipe berbeda. Tiga tipe umum data otentikasi dijelaskan pada Tabel 2.3.

Tipe otentikasi yang paling umum dan paling mudah untuk diimplementasikan adalah otentikasi tipe 1. Yang dilakukan adalah meminta subjek membuat *password*, *passphrase*, atau nomor PIN. Alternative lain adalah perlunya mendorong subjek untuk membuat *frase* yang sangat sulit diterka oleh orang lain, namun tidak terlalu rumit sehingga sulit untuk diingat. *Password* (*frase* atau PIN) yang sulit diingat akan mengurangi nilai dari *password* itu sendiri. Hal tersebut dapat terjadi bila *administrator* terlalu sering memerlukan penggantian *password* sehingga pengguna kesulitan untuk mengingat *password* terbaru. Jadi, yang

disarankan adalah menjaga *password* secara rahasia dan aman. Aturan-aturan berikut ini adalah petunjuk yang baik untuk membuat *password* yang aman :

1. *Password* setidaknya memiliki panjang 6 karakter.
2. *Password* setidaknya mengandung sebuah angka atau karakter tanda baca.
3. Tidak menggunakan kosakata atau kombinasi kosakata.
4. Tidak menggunakan data pribadi, seperti tanggal kelahiran, nama anggota keluarga atau binatang peliharaan, atau lagu atau hobi favorit.
5. Tidak sesekali menuliskan *password*.
6. Membuat *password* yang mudah diingat tapi sulit diterka.

Data otentikasi tipe 2 lebih rumit untuk dilakukan karena subjek perlu membawa suatu alat atau sejenisnya. Alat tersebut umumnya perangkat elektronik yang menghasilkan suatuu nilai yang bersifat sensitive terhadap waktu atau suatu jawaban untuk di *input*. Meskipun otentikasi tipe 2 lebih rumit, tipe ini hamper selalu lebih aman dibandingkan dengan otentikasi tipe 1. Otentikasi tipe 3, atau biometrik adalah yang paling canggih. Biometrik menggambarkan pendeteksian dan pengklasifikasian dari atribut fisik. Terdapat banyak teknik biomterik yang berbeda diantaranya :

1. Pembacaan sidik jari/telapak tangan.
2. Geometri tangan
3. Pembacaan retina/iris
4. Pengenalan suara
5. Dinamika tanda tangan

Karena kerumitannya, biometric adalah tipe otentikasi yang paling mahal untuk diimplementasikan. Tipe ini juga lebih sulit untuk dipelihara karena sifat ketidak-sempurnaan dari analisis *biometrik*. Dianjurkan untuk berhati-hati beberapa masalah-masalah utama dari *eror-eror biomterik*. Pertama, sistem mungkin menolak subjek yang memiliki otoritas. Ukuran kesalahan semacam ini disebut *false rejection rate* (FRR). Di sisi lain, sistem *biometrik* mungkin menerima subjek yang salah. Ukuran kesalahan semacam ini disebut dengan *false acception rate* (FAR). Yang menjadi masalah adalah ketika sensitifitas sistem *biometric* diatur untuk menurunkan FRR, maka FAR meningkat. Begitu juga berlaku

sebaliknya. Posisi pengaturan yang terbaik adalah bila nilai FRR dan FAR seimbang, ini terjadi pada *crossover eror rate* (CER).

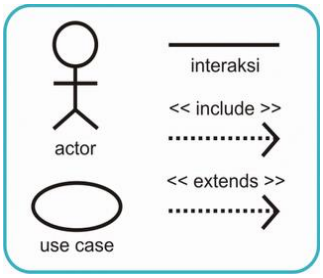
2.5 Diagram *Use Case*

Sukamto dan Shalahuddin (2014:155) menjelaskan bahwa Use Case atau diagram *use case* merupakan pemodelan untuk kelakukan (*behavior*) sistem informasi yang akan dibuat. *Use case* mendeskripsikan sebuah interaksi antara satu atau lebih aktor dengan sistem yang akan dibuat. *Use Case* digunakan untuk mengetahui fungsi apa saja yang ada di dalam sebuah sistem informasi dan siapa saja yang berhak menggunakan fungsi-fungsi itu. Berikut adalah simbol-simbol yang ada pada diagram *use case.* Sedangkan aktor bisa berupa orang, peralatan, atau sistem lain yang berinteraksi terhadap sistem yang akan dibangun.

Karakteristik *Use case diagram.*

1. *Use cases* adalah interaksi atau dialog antara sistem dan actor, termasuk pertukaran pesan dan tindakan yang dilakukan oleh sistem.
2. *Use cases* diprakarsai oleh actor dan mungkin melibatkan peran actor lain. *Use cases* harus menyediakan nilai minimal kepada satu actor.
3. *Use cases* bisa memiliki perluasan yang mendefinisikan tindakan khusus dalam interaksi atau use case lain mungkin disisipkan.
4. *Use case* class memiliki objek use case yang disebut skenario. Skenario menyatakan urutan pesan dan tindakan tunggal.

Komponen komponen dalam *use case* diagram dapat dilihat pada gambar 2.2



Gambar 2.3 Komponen *Use Case* Diagram

2.6 *Activity Diagram*

Rosa A.S dan Shalahuddin (2014) mengatakan bahwa *Activity Diagram* adalah representasi grafis dari workflow dari kegiatan dan tindakan bertahap dengan dukungan untuk pilihan, iterasi dan *concurrency*. Dalam Unified Modeling Language , diagram aktivitas dimaksudkan untuk model kedua proses komputasi dan organisasi (yaitu *workflow*). Activity diagram menunjukkan aliran keseluruhan kontrol.

Activity diagram dibangun dari sejumlah bentuk, dihubungkan dengan panah. Jenis Bentuk yang paling penting:

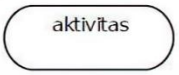
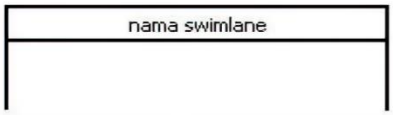
Persegi panjang bulat merupakan tindakan;

1. Berlian merupakan keputusan;
2. Bar mewakili awal (split) atau akhir (bergabung) kegiatan bersamaan;
3. Lingkaran hitam merupakan awal (initial state) dari alur kerja;
4. Lingkaran hitam dikelilingi mewakili akhir (keadaan akhir).
5. Panah dijalankan dari awal menuju akhir dan merupakan urutan kegiatan terjadi.

Oleh karena itu mereka dapat dianggap sebagai bentuk flowchart . Teknik flowchart Khas kekurangan konstruksi untuk mengekspresikan concurrency . Namun, bergabung dan simbol perpecahan dalam diagram aktivitas hanya menyelesaikan ini untuk kasus-kasus sederhana, makna dari model tersebut adalah tidak jelas kapan mereka sewenang-wenang dikombinasikan dengan keputusan atau loop.

Komponen-komponen *Activity* diagram ditunjukan pada tabel 2.1

Tabel 2.2 Komponen *Activity Diagram*

Simbol	Deskripsi
status awal 	status awal aktivitas sistem, sebuah diagram aktivitas memiliki sebuah status awal
aktivitas 	aktivitas yang dilakukan sistem, aktivitas biasanya diawali dengan kata kerja
percabangan / *decision* 	asosiasi percabangan dimana jika ada pilihan aktivitas lebih dari satu
penggabungan / *join*	asosiasi penggabungan dimana lebih dari satu aktivitas digabungkan menjadi satu
status akhir 	status akhir yang dilakukan sistem, sebuah diagram aktivitas memiliki sebuah status akhir
swimlane 	memisahkan organisasi bisnis yang bertanggung jawab terhadap aktivitas yang terjadi
fork, 	digunakan utk menunjukkan kegiatan yg dilakukan secara paralel
join, 	digunakan utk menunjukkan kegiatan yg digabungkan

2.7 Penelitian Sebelumnya

Penelitian sebelumnya digunakan agar dapat menjadi bahan pertimbangan dan bisa membantu dalam pembuatan teknologi baru yang diharapkan. Menurut penelitian sebelumnya oleh Mochamad Yoga Tritama (2015) dengan judul penelitian "Crayonpedia Education Ecosystem *Single Sign On* TADJ, YOOPA,

MOODLE, WORDPRESS, dan PHPBB berbasis web". Penelitian ini dilakukan untuk

Membantu mahasiswa untuk bimbingan jarak jauh dengan dosen pembimbing secara online. Sistem ini juga menggunakan satu akun untuk beberapa aplikasi, Antara lain tadj, yoopa, *e-learning*, blog, dan forum.

Sedangkan pada penelitian selanjutnya yang dilakukan oleh Novera (2013) dengan judul penelitian "*Single Sign On* (*SSO)* dengan menggunakan *Lightweight Directory Access Protocol (LDAP)*". Dalam penelitian ini, Novera mencoba untuk membangun *SSO* dengan menggunakan *LDAP* untuk diterapkan pada Universitas Bina Darma dengan tujuan untuk membantu dalam pengorganisasian pengguna karena digunakannya *LDAP* sebagai single data *user*. Dan pembuatan *SSO* ini terbukti telah menggabungkan sistem-sistem yang ada di Universitas Bina Darma seperti *zimbra mail, moodle, radius server hotspot* sehingga terjadi integrasi dengan menggunakan *LDAP*.

Dari kedua penilitian sebelumnya diatas, dapat melakukan penelitian dengan judul "Penerapan Sistem *Single Sign On* Berbasis Web Pada Institut Informatika Dan Bisnis Darmajaya". Dimana pada penelitian ini merupakan yang pertama dilakukan di Institut Informatika dan Bisnis Darmajaya dan juga sebuah kelanjutan atau penyempurnaan dari penelitian sebelumnya yang dilakukan oleh saudara Mochamad Yoga Tritama (2015) dari Institut Teknologi Bandung dan saudara Dian Novera (2013) dari Universitas Bina Darma.

BAB III
METODE PENELITIAN

3.1 Metode Pengumpulan Data

Upaya mendukung penelitian yang dilakukan maka dibutuhkan pengumpulan data dengan menggunakan beberapa metode pengumpulan data yaitu sebagai berikut:

1. Wawancara (*Interview*)

   Pengumpulan data dengan metode *interview* yaitu metode pengumpulan data dengan cara tanya jawab secara langsung dengan orang-orang yang terkait yaitu kepada Anggota *ICT Center (Information & communication Technology)* yaitu Bapak Fajrin Armawan yang beralamat di Jl. Z.A. Pagar Alam, No. 93 Labuhan Ratu, Bandar Lampung, Lampung 35141 Indonesia. Melakukan pertanyaan seputar sejarah, keadaan dan juga keamanan Server yang ada di Institut Informatika dan Bisnis Darmajaya.

2. Pengamatan (*Observation*)

   Pengumpulan data dengan mengamati atau *observation* yaitu metode pengumpulan data dengan cara pengamatan dan pencatatan secara langsung.

   Mempelajari segala sesuatu yang berhubungan dengan sistem yang akan dibangun. Mengamati secara langsung seputar sistem yang berjalan mengenai informasi tentang Siska.

3. Dokementasi (*Document*)

   Merupakan metode pengumpulan data dengan cara membaca, mencatat, mengutip, dan mengumpulkan data-data secara teoritis dari Internet sebagai landasan penyusunan penelitian. Peneliti mencari dari internet juga dilakukan untuk referensi laporan ini, dimana teori tersebut diletakkan pada landasan teori.

4. Studi Kepustakaan (*Literature*):

Pada studi kepustakaan guna memperoleh data adalah dengan cara mencari bahan di internet, perpustakaan dan jurnal serta buku yang sesuai dengan objek yang akan diteliti.

3.2 Metode Pengembangan Perangkat Lunak

Dari penelitian ini akan diketahui kemudahan perancangan web login OAuth2 sebagai dasar SSO yang mengacu pada jurnal, artikel, thesis dan tutorial yang memudahkan dalam pembuatan sistem login, serta bagaimana proses dari sistem login central authentication service dan open authorization sebagai sistem login dalam SSO. Pembuatan web login ini berdasarkan pada kebutuhan dari dua sistem yang akan dijadikan sebagai contoh, dimana default konfigurasi untuk OAuth2 dan simple web login dengan google account untuk oauth.

Test performa sistem login OAuth2 menggunakan Apache Benc, test yang dilakukan adalah *Response Time*, dimana dalam test ini akan diketahui performa kedua sistem login dalam menangani *request* per satuan detik. Tools Apache Benc dapat dibuka lewat cmd, setelah masuk ke path C:\xampp\apache\bin, maka perintah yang dimasukkan adalah >ab –t [waktu (s)] [http://]hostname[:port]/path. Disini hasil yang dapat diamati adalah jumlah request yang dapat ditangani oleh sistem dalam selang waktu yang telah ditentukan.

3.3 Alat dan Bahan

Peralatan Untuk membangun sebuah sistem *Single Sign-On* berbasis web, diperlukan beberapa perangkat lunak. Perangkat lunak yang digunakan untuk membuat sebuah sistem login dan juga untuk meng-Edit sebuah bahasa pemograman. Bahasa pemograman yang digunakan untuk membangun sistem adalah PHP dengan *database* MySQL. Setelah mempelajari dan mempertimbangkan beberapa hal maka dipilihlah perangkat lunak sebagai berikut:

1. Sistem Operasi Windows 10 Profesional sebagai *Operating System* yang dipakai untuk membuka *Software* yang dibutuhkan untuk membuat SSO dan lebih ringan.

2. Code Igniter sebagai *Framework* yang dipakai untuk membuat sistem Login
3. Sublime Text sebagai *Software* editor programming untuk memudahkan pengetikan program
4. *Database* MySQL sebagai *Software* untuk menjalankan aplikasi SSO dan menyimpan data.

3.3.1 Analisis Kebutuhan Perangkat Keras

Untuk menjalankan perangkat lunak diatas membutuhkan perangkat keras dengan spesifikasi yang cukup, minimal menggunakan perangkat keras dengan spesifikasi berikut :

1. Processor Intel Core i3-6006U (2.0 GHz, 3MB L3 Cache)
2. Ram 4 Gb DDR4 Memory
3. Intel HD Graphics 520
4. Harddisk 500 GB

Sedangkan lingkungan pengembangan sistem tersebut memiliki spesifikasi perangkat lunak sebagai berikut:

1. Sistem Operasi Microsoft Windows 10 Profesional
2. XAMPP for windows 1.6.4 dengan PHP update dan *Database SQLyog* update
3. *Web browser* Mozilla Firefox dan Google Chrome
4. Sublime Text

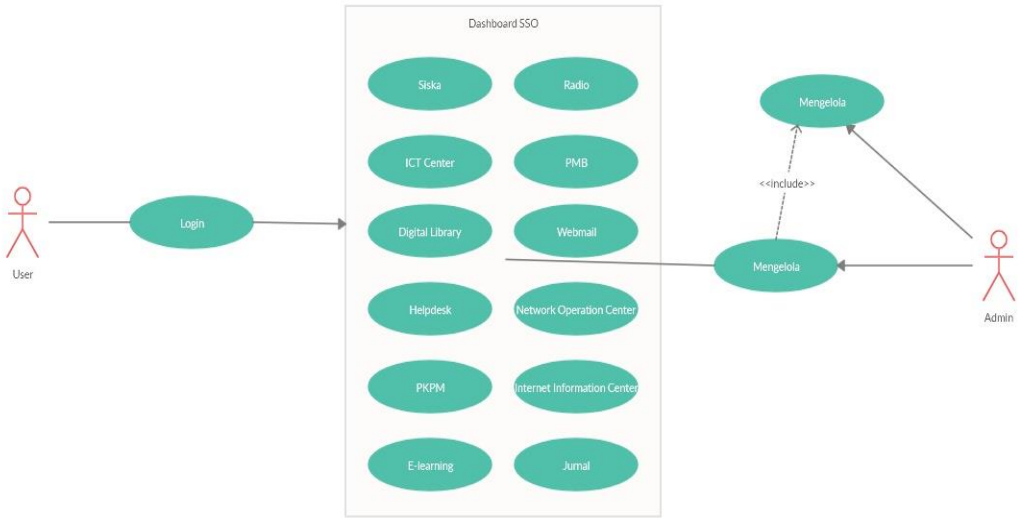
Spesifikasi di atas tidak bersifat mutlak dan menurut peneliti sudah lebih dari cukup.

3.4 Rancangan Sistem

Pada tahapan ini diuraikan tentang perancangan sistem yang akan dibuat untuk terwujudnya aplikasi yang diinginkan, dengan memodelkan permasalahan dalam bentuk diagram-diagram UML, diagram yang digunakan adalah *use case diagram* dan *activity diagram* karena lebih muda untuk dipahami. Berikut adalah penjelasan dari diagram-diagram UML yang digunakan :

1. *Use Case Diagram*

   Use case diagram Dibawah ini menggambarkan sistem dari sudut pandang pengguna sistem tersebut (user) sehingga pembuatan *use case diagram* ini lebih dititik beratkan pada fungsionalitas yang ada pada sistem, bukan berdasarkan alur atau urutan kejadian, sistem yang di usulkan akan di gambarkan dalam *use case diagram*, ditunjukkan pada gambar 3.1 dibawah ini.



Gambar 3.1*Use Case Diagram* web portal

Berdasarkan gambar *use case* di atas dapat kita lihat bahwa pada saat *user* mengakses aplikasi, terdapat 3 menu utama yaitu : *Login, Change Password, Forgot Password*. Pada pilihan menu *Login, user* memasukkan username dan password untuk mengakses layanan yang ada pada SSO, pada pilihan menu *Change Password* dapat digunakan untuk mengubah password, terahir pada pilihan menu *Forgot Password* dapat digunakan untuk mengetahui password yang lupa.

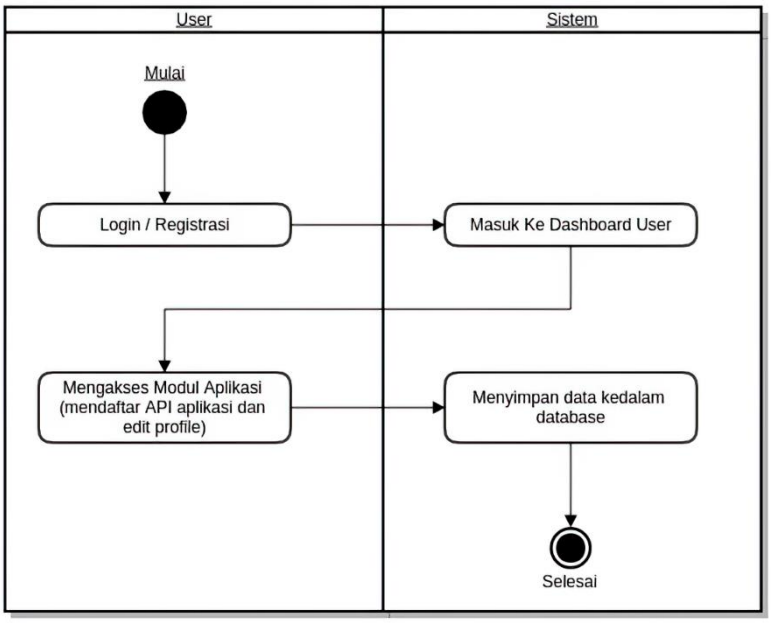
a) Nama use case : Menu Login
   Actor : User
   Tujuan : Untuk Masuk kedalam Layanan web
   Deskripsi : Pada menu ini menampilkan kolom username dan password.

b) Nama use case : Menu Change Password
   Actor : User
   Tujuan : Untuk mengubah password user
   Deskripsi : Pada menu ini menampilkan kolom password lama, password baru, verifikasi password baru.

c) Nama use case : Menu Forgot Password
   Actor : User
   Tujuan : Untuk mengetahui password yang tidak diingat
   Deskripsi : Pada menu ini menampilkan kolom nomor handphone yang terdaftar

2. *Activity Diagram*

   Activity diagram menggambarkan rangkaian aliran dari aktifitas, digunakan untuk mendeskripsikan aktivitas yang dibentuk dalam suatu operasi sehingga dapat juga digunakan untuk aktifitas lainnya seperti *use case* atau interaksi.*Activity diagram* dibawah ini untuk menjelaskan alur SSO dari membuka menu login sampai selesai. *Activity diargram* dapat dilihat pada gambar 3.2 dibawah ini.



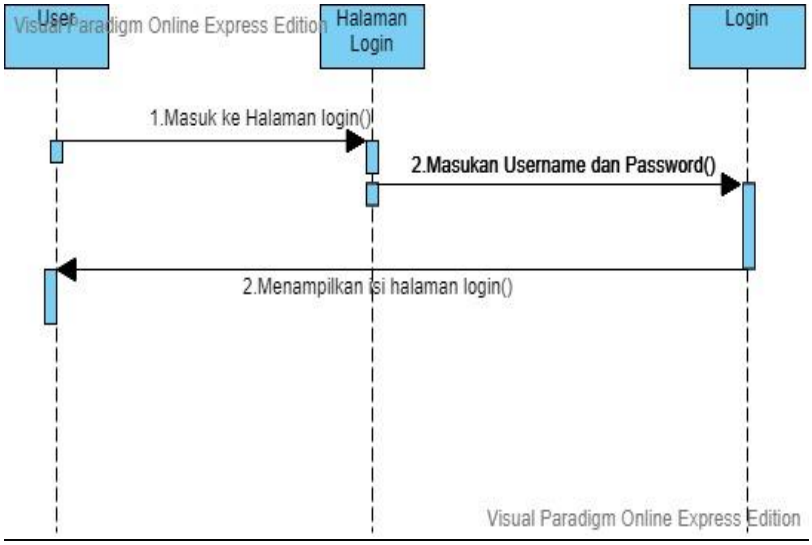
Gambar 3.2 *Activity Diagram* Sistem

3. Sequence Diagram

Pada sequence diagram akan menjelaskan interaksi antar objek dan bagaimana alur yang akan dijalankan pada aplikasi sistem tersebut. Adapun sequence diagram sebagai berikut :

a. Sequence diagram Login SSO

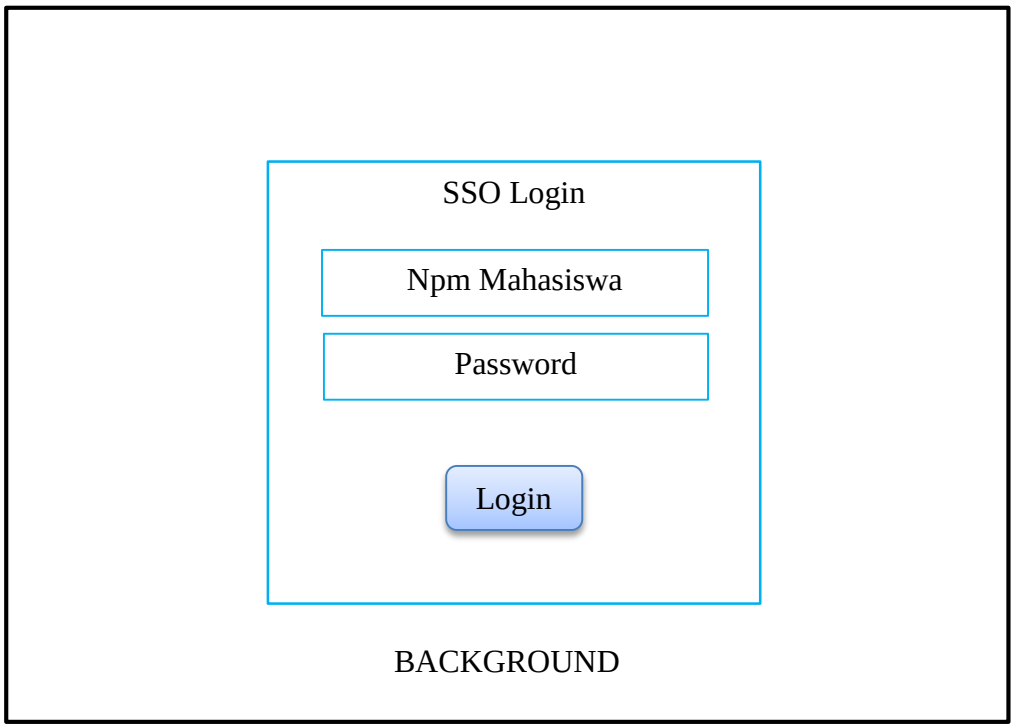
Pengguna (User) akan masuk pada halaman login SSO dan akan muncul tombol login dan juga kolom username password untuk memasuki *web portal*. Gambar 3.3 menjelaskan sequence diagram menu login



Gambar 3.3 Sequence Diagram Login

3.4.1 Rancangan Interface Menu Login

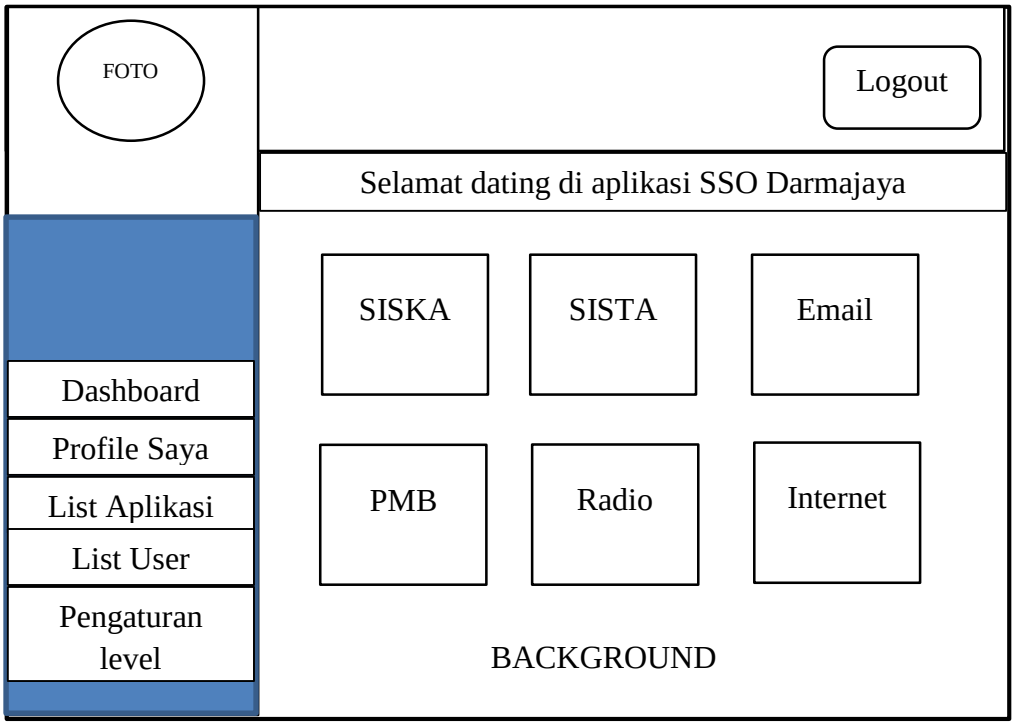
Menu login merupakan interface yang muncul ketika website baru dijalankan, terdiri dari kolom username dan kolom password yang harus di isi untuk memasuki website sso. Dengan background Darmajaya dan di bagian bawah login ada tombol *Change Password,* dan *Forgot Password*.



Gambar 3.3 Rancangan Interface Menu Login.

3.4.2 Rancangan Interface Menu Dashboard

Menu Dashboard merupakan interface yang muncul ketika sudah memasuki tahap login yang diharuskan mengisi npm dan juga password. Terdapat tombol logout yang berada di dibagian ujung kanan atas dashboard. Aplikasi-aplikasi yang ada pada sso terdapat di bagian tengah dashboard.



Gambar 3.4 Rancangan Menu Dashboard SSO

3.4.3 Rancangan Interface Menu Email

Menu Email merupakan interface yang menampilkan webmail yang ada di Darmajaya yang dimana untuk login hanya memerlukan verifikasi apakah dosen/karyawan ataupun mahasiswa.

Gambar 3.6 Rancangan Menu Interface Email yang sudah ada

3.4.4 Rancangan Interface Menu Internet

Menu Internet merupakan interface yang menampilkan layanan bantuan seputar internet IIB Darmajaya untuk mengganti password.

Gambar 3.7 Rancangan Menu Interface Internet yang sudah ada

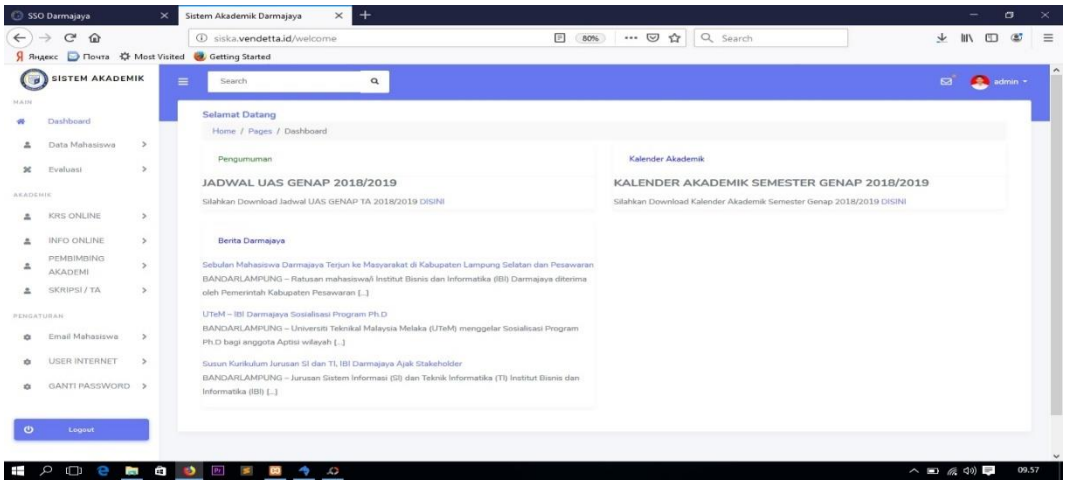
3.4.5 Rancangan Interface Menu SITES

Menu SITES merupakan interface yang menampilkan website/blog untuk sivitas Akademika IIB Darmajaya.

Gambar 3.9 Rancangan Menu Interface SITES

3.4.6 Rancangan Interface Menu Siska

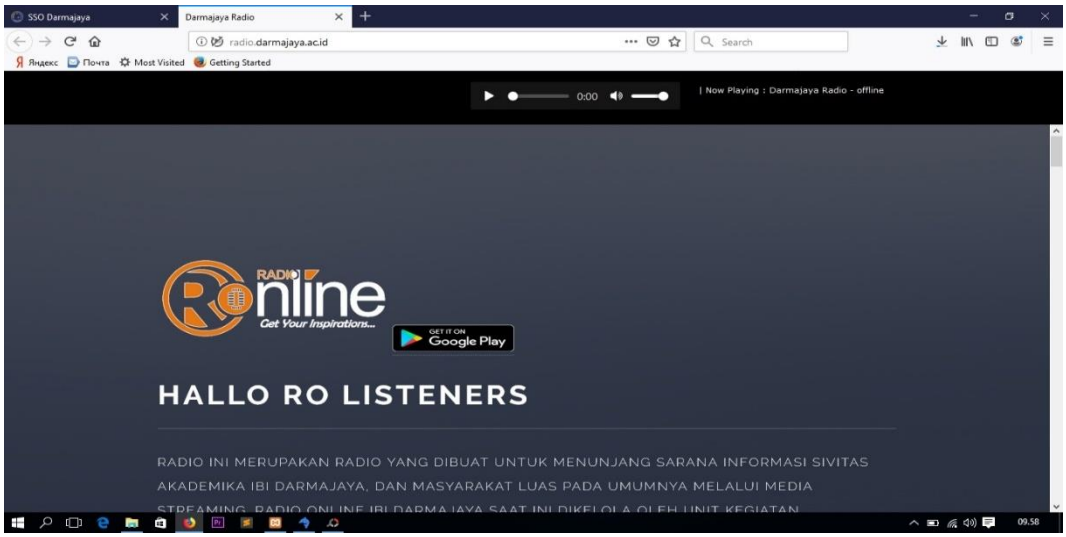
Menu Siska merupakan interface yang menampilkan website/blog untuk sivitas Akademika IIB Darmajaya.



Gambar 3.10 Siska Darmajaya

3.4.7 Rancangan Interface Menu Radio

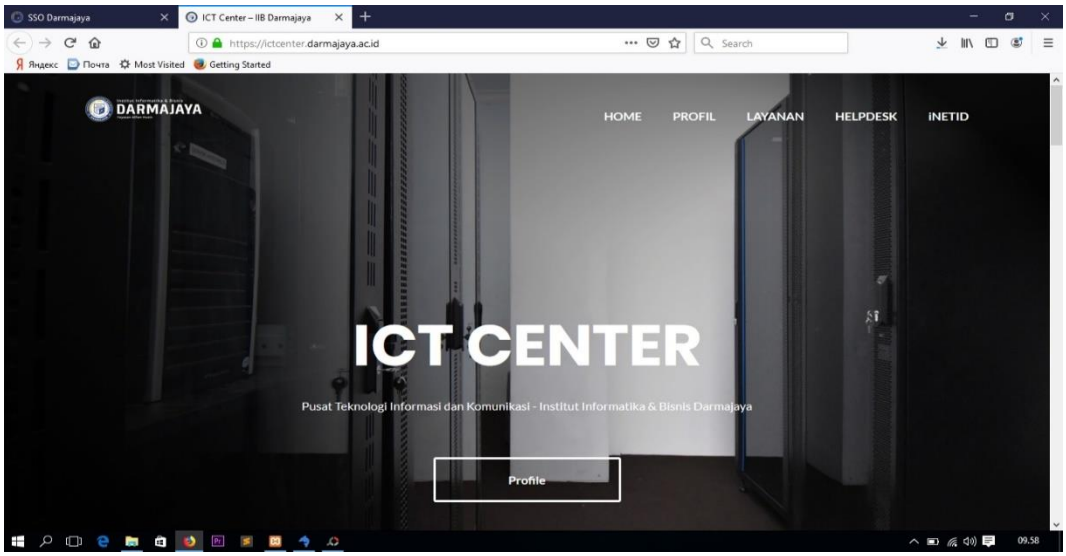
Menu Radio merupakan interface yang menampilkan website/blog untuk Mendengar radio di IIB Darmajaya.



Gambar 3.11 Radio Darmajaya

3.4.8 Rancangan Interface Menu ICT

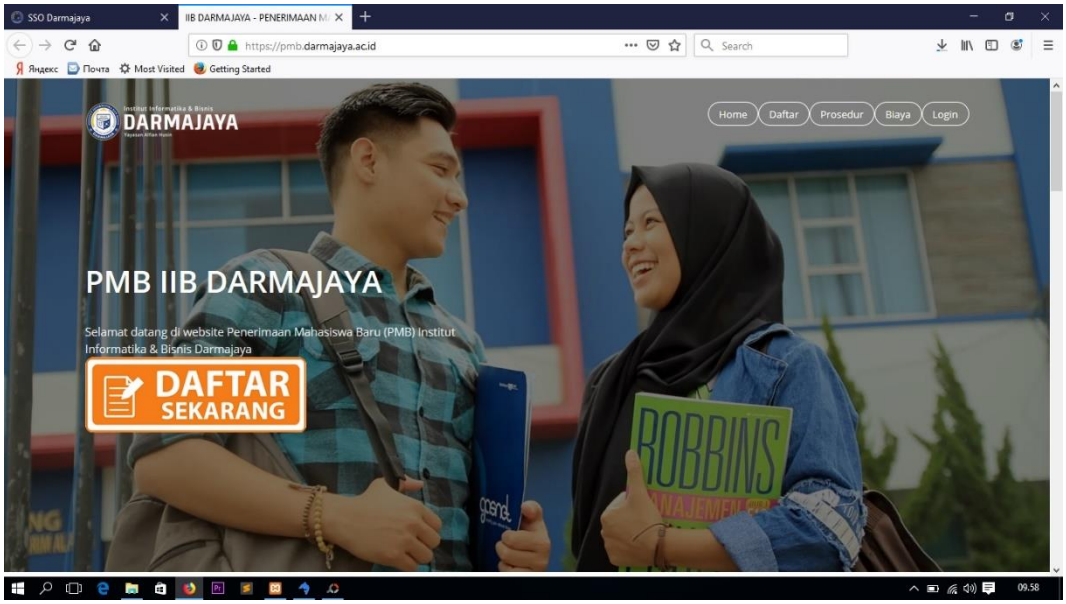
Menu ICT merupakan interface yang menampilkan website/blog untuk Layanan ICT di IIB Darmajaya.



Gambar 3.12 ICT Center Darmajaya

3.4.9 Rancangan Interface Menu PMB

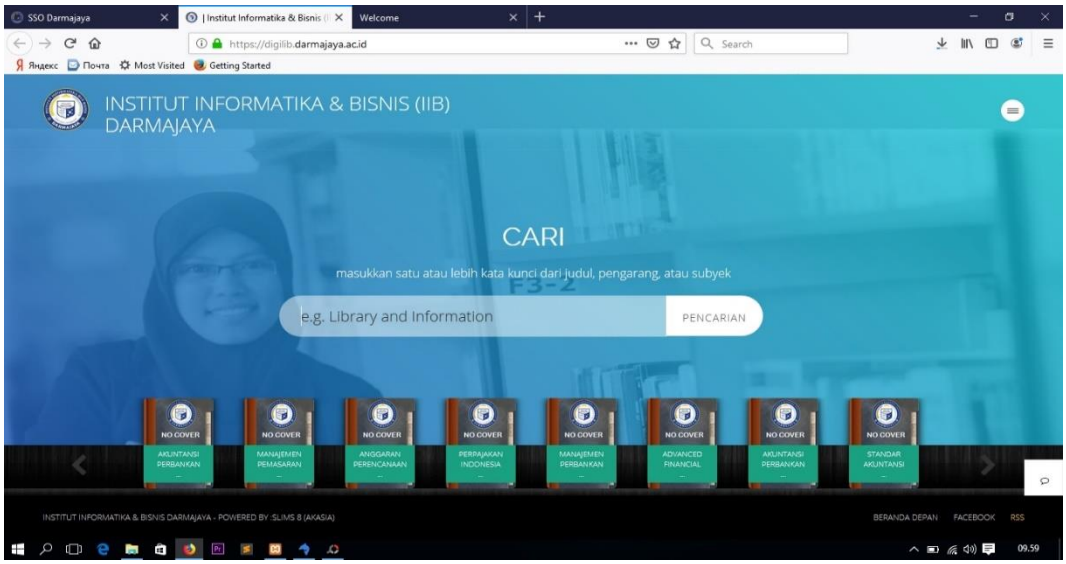
Menu PMB merupakan interface yang menampilkan website/blog untuk Informasi dan pendaftaran mahasiswa baru di IIB Darmajaya.



Gambar 3.13 Aplikasi PMB Darmajaya

3.4.10 Rancangan Interface Menu Digital Library

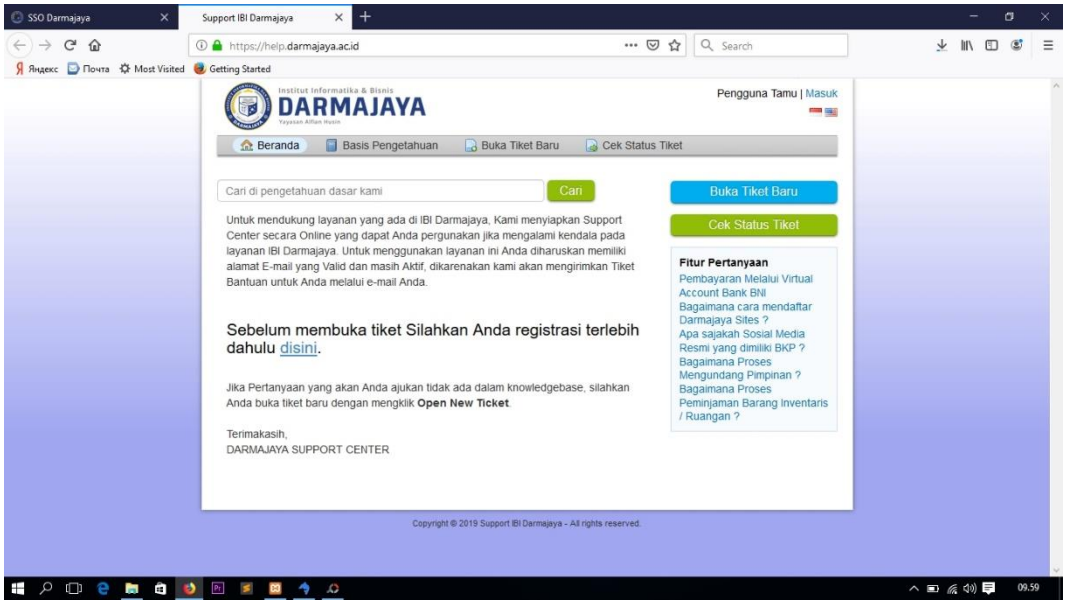
Menu Dilig merupakan interface yang menampilkan website/blog untuk Perpustakaan digital di IIB Darmajaya.



Gambar 3.14 Aplikasi Digital Library Darmajaya

3.4.11 Rancangan Interface Menu Helpdesk

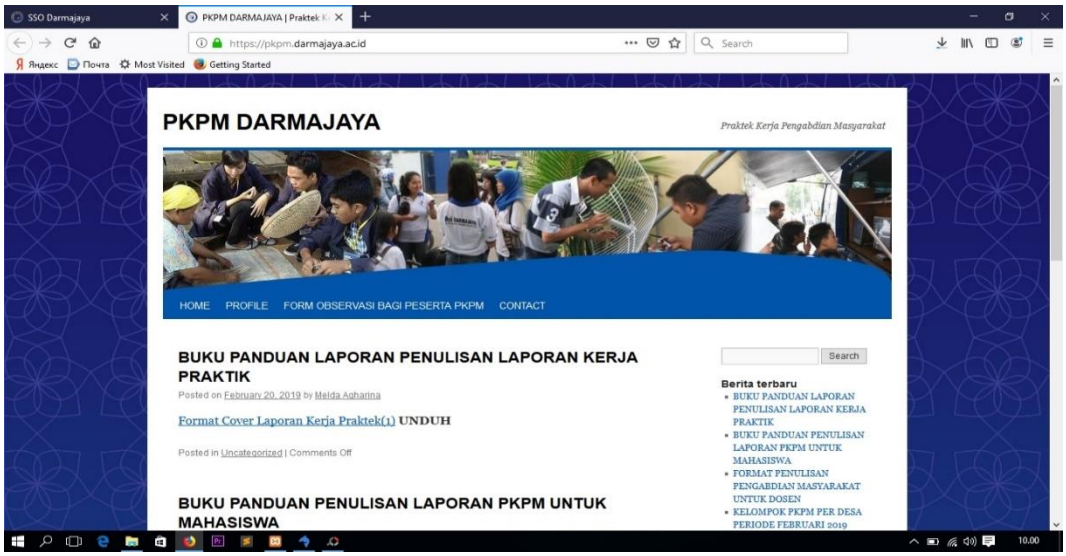
Menu Helpdesk merupakan interface yang menampilkan website/blog untuk Bantuan Informasi di IIB Darmajaya.



Gambar 3.15 Helpdesk Darmajaya

3.4.12 Rancangan Interface Menu PKPM

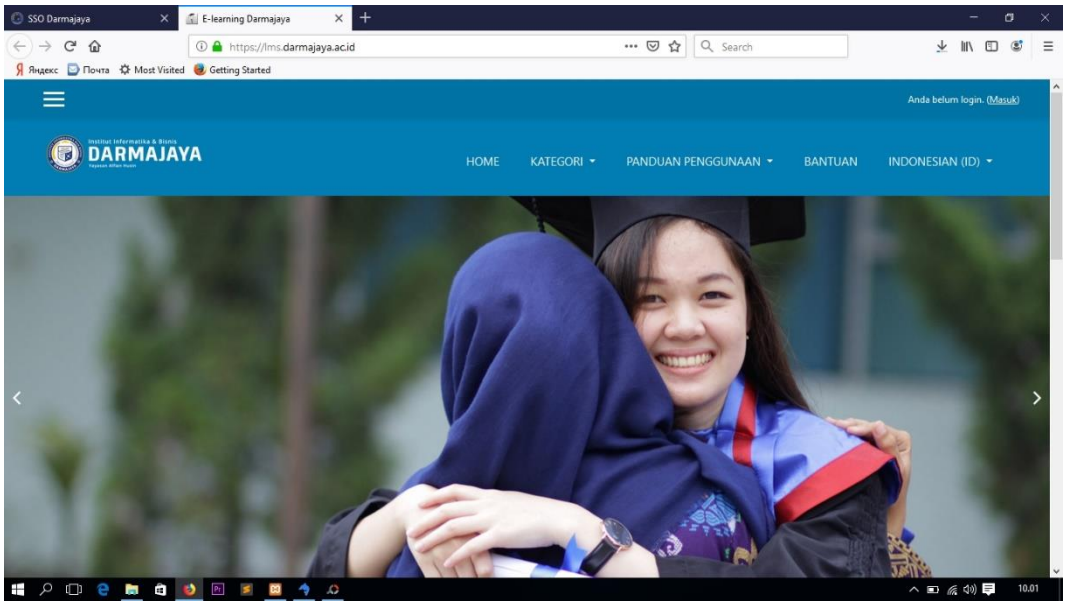
Menu PKPM merupakan interface yang menampilkan website/blog untuk Informasi mengenai PKPM di IIB Darmajaya.



Gambar 3.16 PKPM Darmajaya

3.4.13 Rancangan Interface Menu E-learning

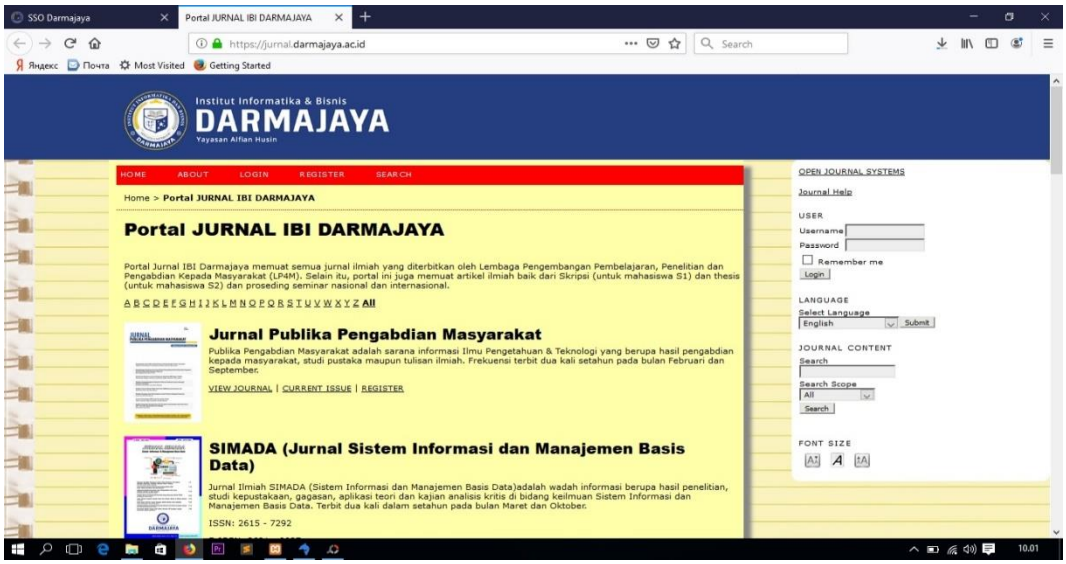
Menu E-learning merupakan interface yang menampilkan website/blog untuk buku pembelajaran elektronik di IIB Darmajaya.



Gambar 3.17 E-learning Darmajaya

3.4.14 Rancangan Interface Menu Jurnal

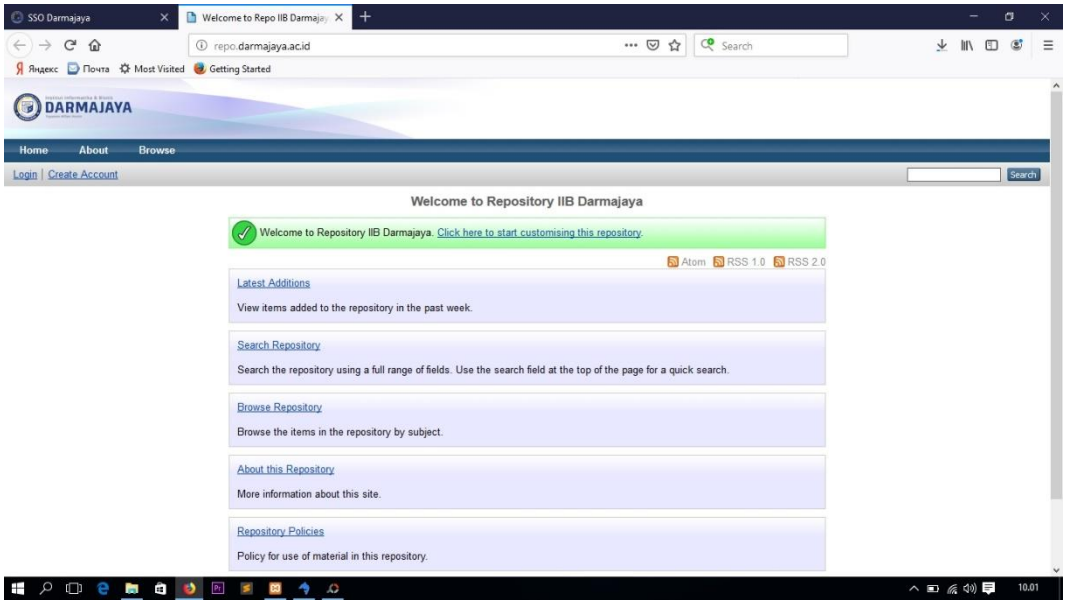
Menu Jurnal merupakan interface yang menampilkan website/blog untuk Melihat jurnal yang ada di IIB Darmajaya.



Gambar 3.18 Portal Jurnal Darmajaya

3.4.15 Rancangan Interface Menu Repository

Menu Repository merupakan interface yang menampilkan website/blog Melaporkan jika terjadi kesalahan pada subdomain di IIB Darmajaya.



Gambar 3.19 Repository Darmajaya

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

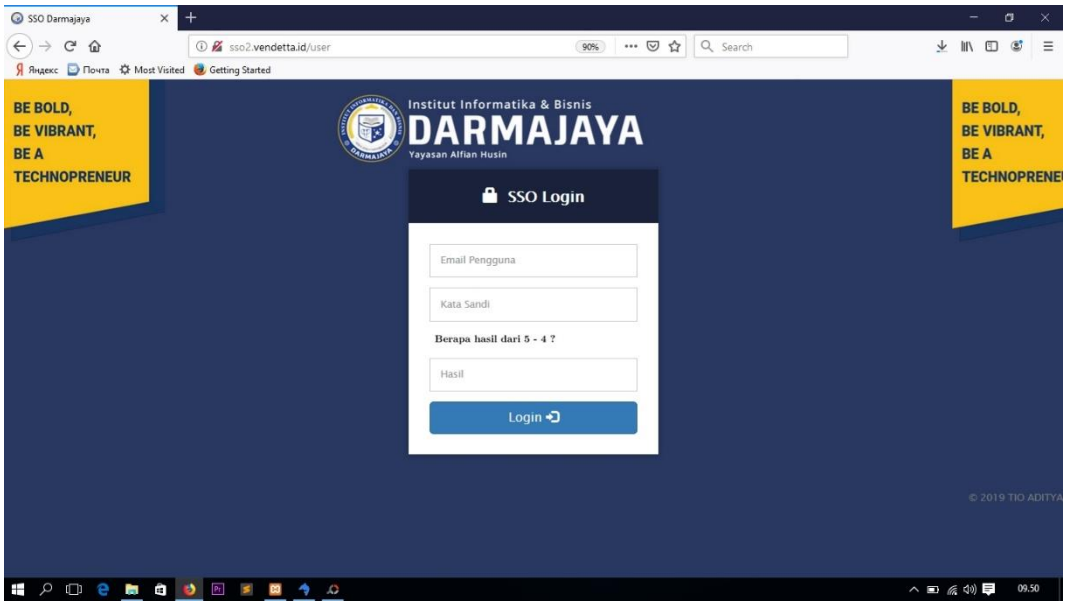
4.1 Hasil

Hasil rancangan program merupakan tahap mewujudkan perancangan menjadi sebuah aplikasi. Berikut ini akan dijelaskan mengenai hasil program SSO (*Single Sign-On*) yang akan diterapkan di Institut Informatika dan Bisnis Darmajaya Berbasis Web.

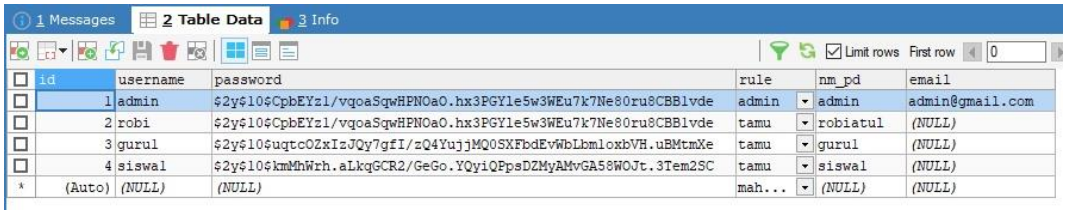
4.1.1 Tampilan SSO

4.1.1.1 Tampilan Halaman Login SSO

Halaman Login SSO adalah tampilan yang menampilkan menu untuk login, yang dimana terdapat kolom *username*, *password* dan Autentikasi penjumlahan angka yang harus di input untuk dapat mengakses masuk ke dalam sistem. Dapat dilihat pada gambar dibawah ini :



Gambar 4.1 Tampilan Login SSO

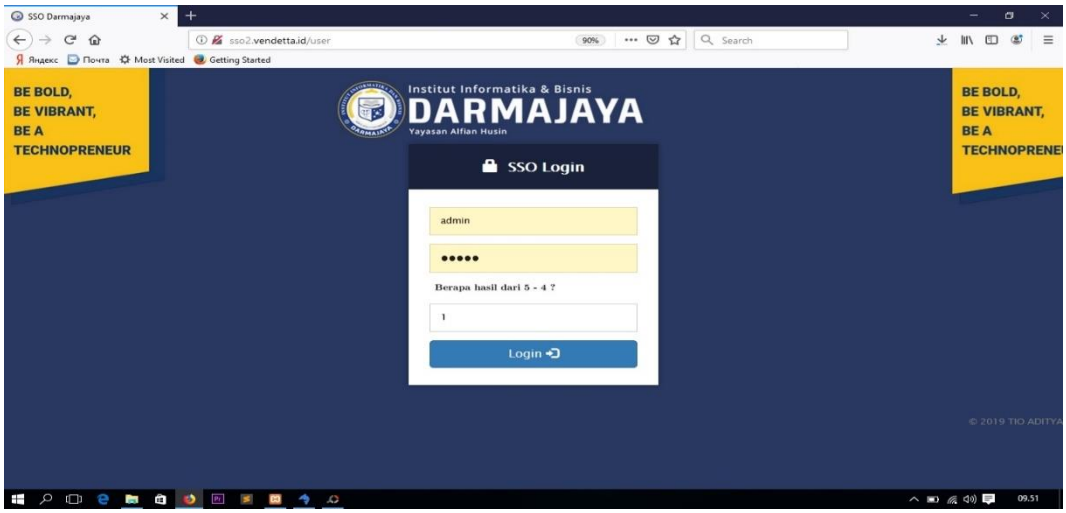


1 Messages | 2 Table Data | 3 Info

Limit rows | First row | 0

id	username	password	rule	nm_pd	email
1	admin	$2y$10$CpbEYzl/vqoaSqwHPNOaO.hx3PGYle5w3WEu7k7Ne80ru8CBBlvde	admin	admin	admin@gmail.com
2	robi	$2y$10$CpbEYzl/vqoaSqwHPNOaO.hx3PGYle5w3WEu7k7Ne80ru8CBBlvde	tamu	robiatul	*(NULL)*
3	gurul	$2y$10$uqtcOZxIzJQy7gfI/zQ4YujjMQ0SXFbdEvWbLbmloxbVH.uBMtmXe	tamu	gurul	*(NULL)*
4	siswal	$2y$10$kmMhWrh.aLkqGCR2/GeGo.YQyiQPpsDZMyAMvGA58WOJt.3Tem2SC	tamu	siswal	*(NULL)*
(Auto)	*(NULL)*	*(NULL)*	mah...	*(NULL)*	*(NULL)*

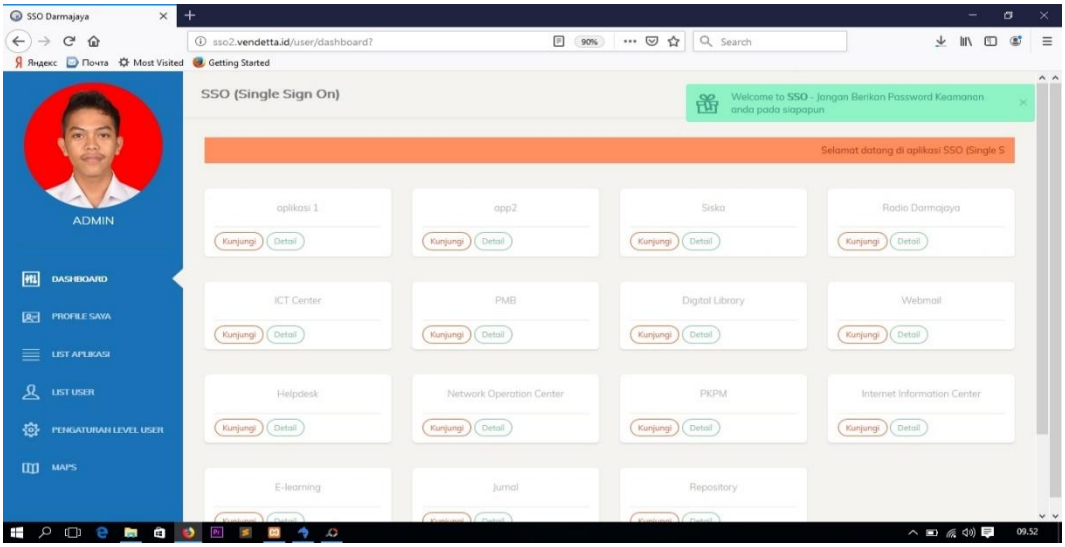
Gambar 4.2 Database user



Gambar 4.3 Login dengan username “Admin” dan password “Admin”

4.1.1.2 Tampilan Dashboard SSO

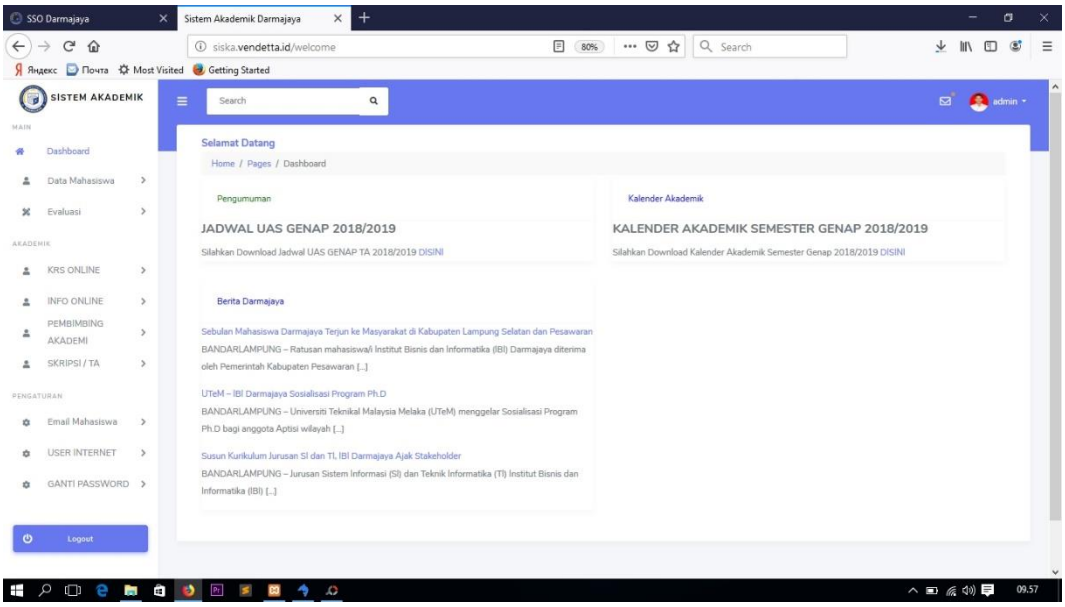
Berikut ini merupakan tampilan Dashboard SSO setelah login dengan menggunakan username dan password. Tampilan dashboard dapat dilihat pada gambar 4.4 :



Gambar 4.4 Dashboard SSO

4.1.1.2.1 Tampilan Aplikasi Siska

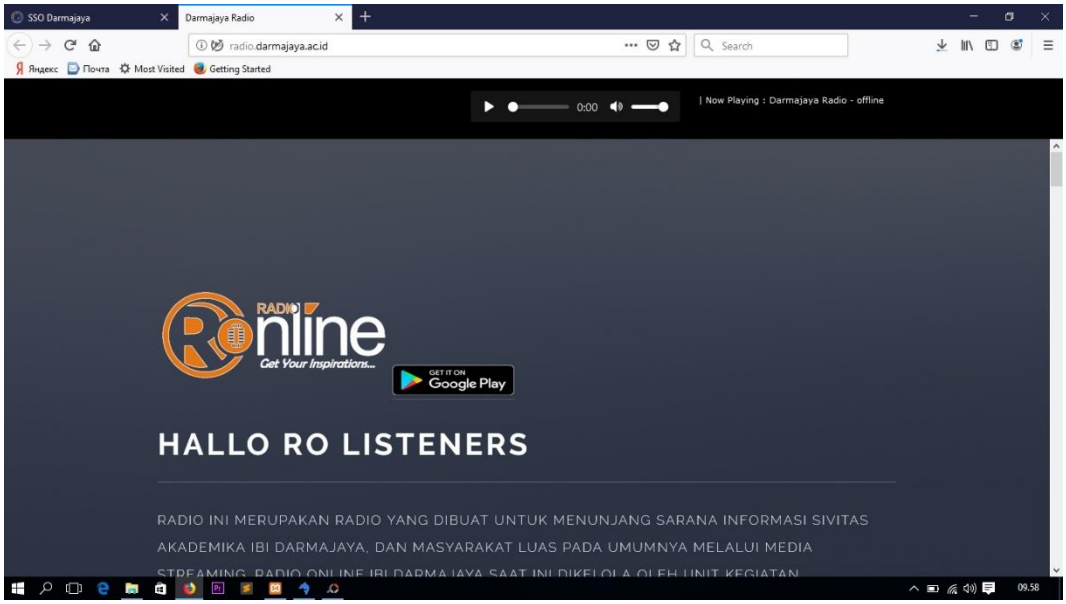
Berikut ini merupakan tampilan Aplikasi Siska (Sistem Akademik) yang ada pada SSO Darmajaya. Dapat dilihat pada gambar 4.5 :



Gambar 4.5 Siska Darmajaya

4.1.1.2.2 Tampilan Aplikasi Radio

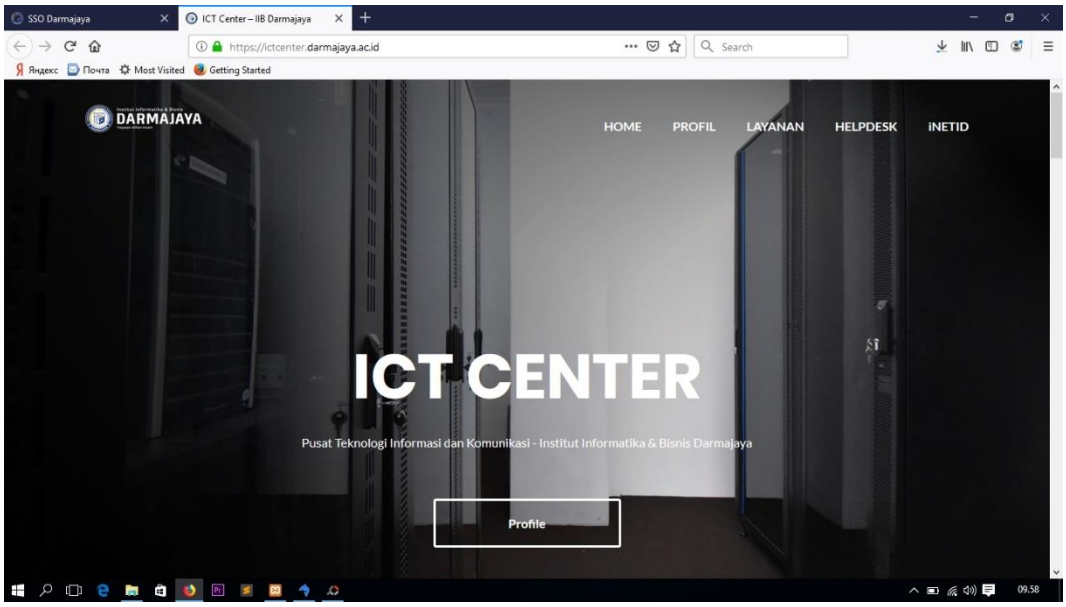
Berikut ini merupakan tampilan Aplikasi Radio yang ada pada subdomain Darmajaya. Dapat dilihat pada gambar 4.6 :



Gambar 4.6 Radio Darmajaya

4.1.1.2.3 Tampilan Aplikasi ICT Center

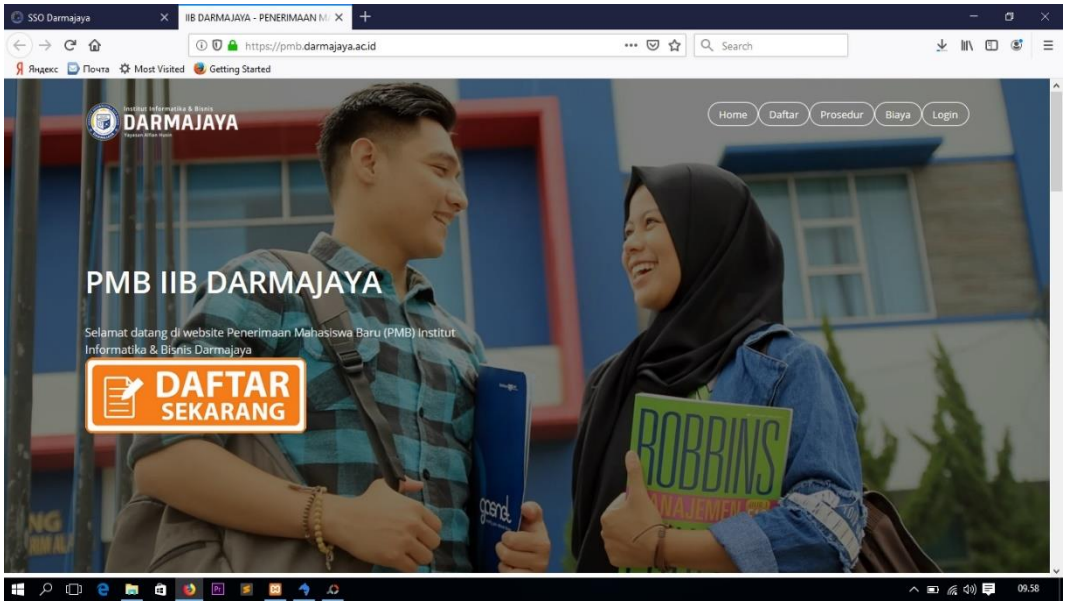
Berikut ini merupakan tampilan Aplikasi ICT Center yang ada pada subdomain Darmajaya. Dapat dilihat pada gambar 4.7 :



Gambar 4.7 ICT Center Darmajaya

4.1.1.2.4 Tampilan Aplikasi PMB

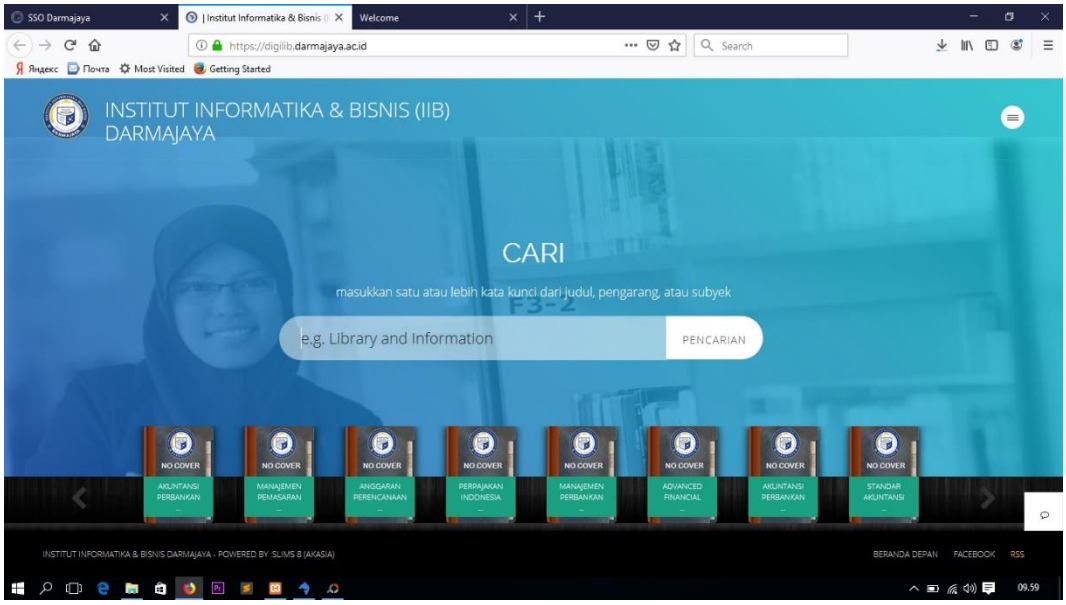
Berikut ini merupakan tampilan Aplikasi PMB (Penerimaan Mahasiswa Baru) yang ada pada subdomain Darmajaya. Dapat dilihat pada gambar 4.8 :



Gambar 4.8 Aplikasi PMB Darmajaya

4.1.1.2.5 Tampilan Aplikasi Digital Library

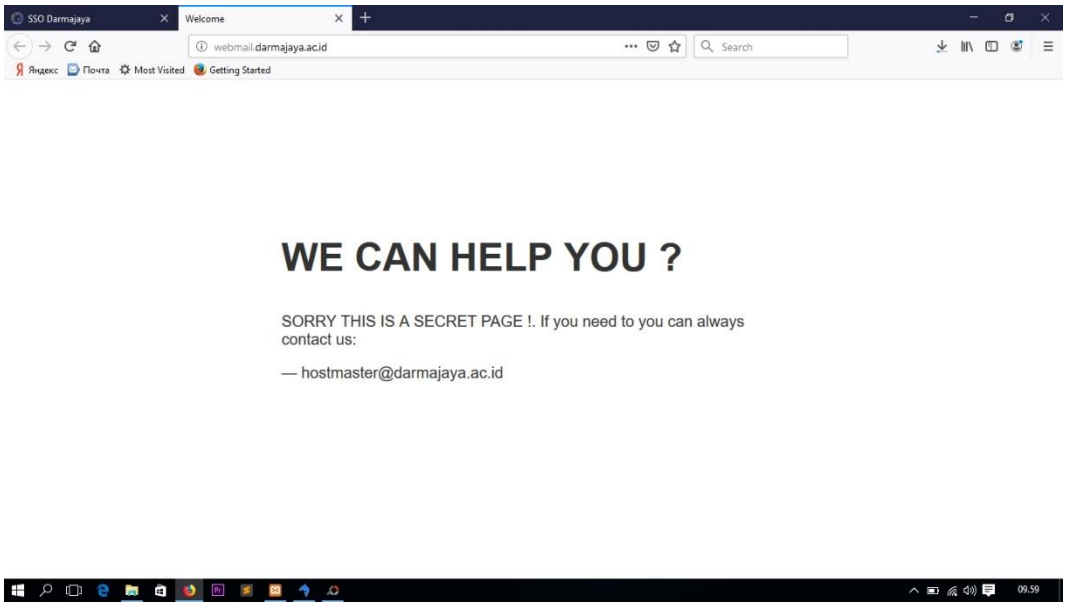
Berikut ini merupakan tampilan Aplikasi Digital Library yang ada pada subdomain Darmajaya. Dapat dilihat pada gambar 4.9 :



Gambar 4.9 Aplikasi Digital Library Darmajaya

4.1.1.2.6 Tampilan Aplikasi Webmail

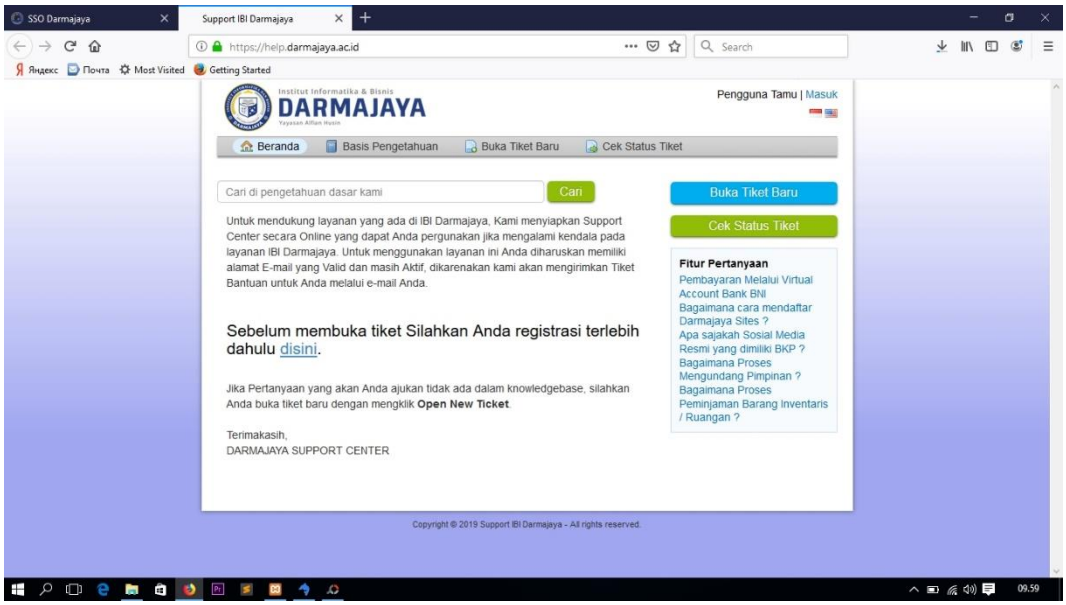
Berikut ini merupakan tampilan Aplikasi Webmail yang ada pada subdomain Darmajaya. Dapat dilihat pada gambar 4.10 :



Gambar 4.10 Webmail Darmajaya

4.1.1.2.7 Tampilan Aplikasi Helpdesk

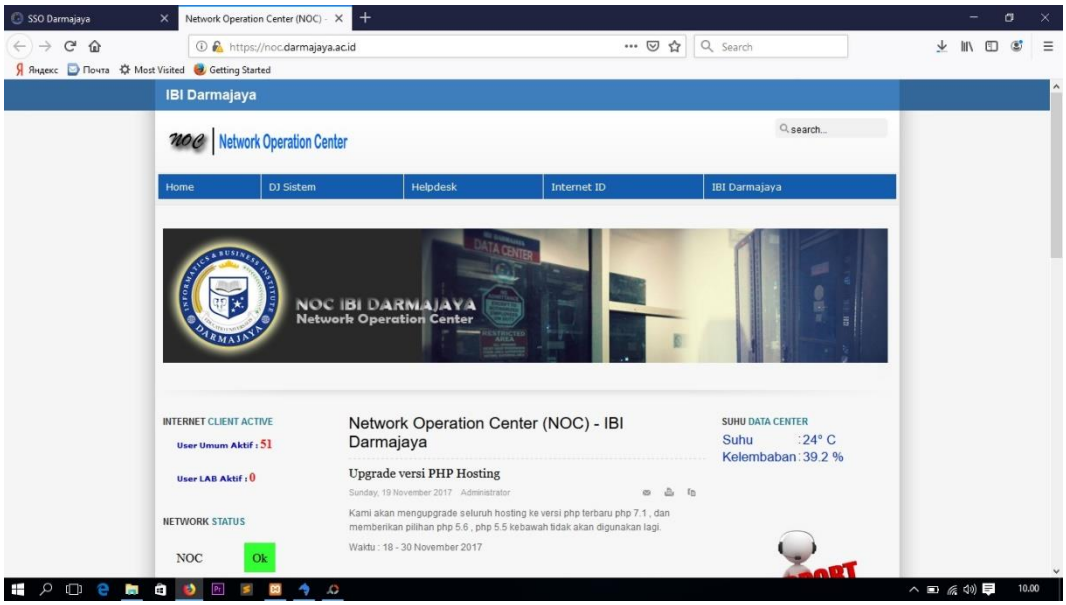
Berikut ini merupakan tampilan Aplikasi Helpdesk yang ada pada subdomain Darmajaya. Dapat dilihat pada gambar 4.11 :



Gambar 4.11 Helpdesk Darmajaya

4.1.1.2.8 Tampilan Aplikasi Network Operation Center

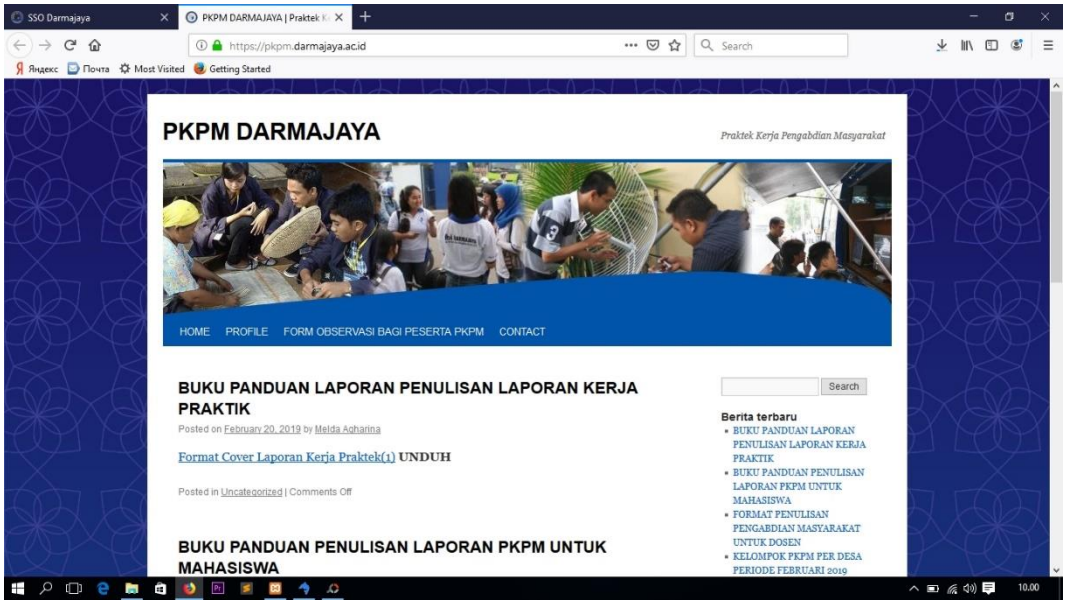
Berikut ini merupakan tampilan Aplikasi Network Operation Center yang ada pada subdomain Darmajaya. Dapat dilihat pada gambar 4.12 :



Gambar 4.12 Network Operation Center Darmajaya

4.1.1.2.9 Tampilan Aplikasi PKPM

Berikut ini merupakan tampilan Aplikasi PKPM (Program Kerja Pengabdian Masyarakat) yang ada pada subdomain Darmajaya. Dapat dilihat pada gambar 4.13:



Gambar 4.13 PKPM Darmajaya

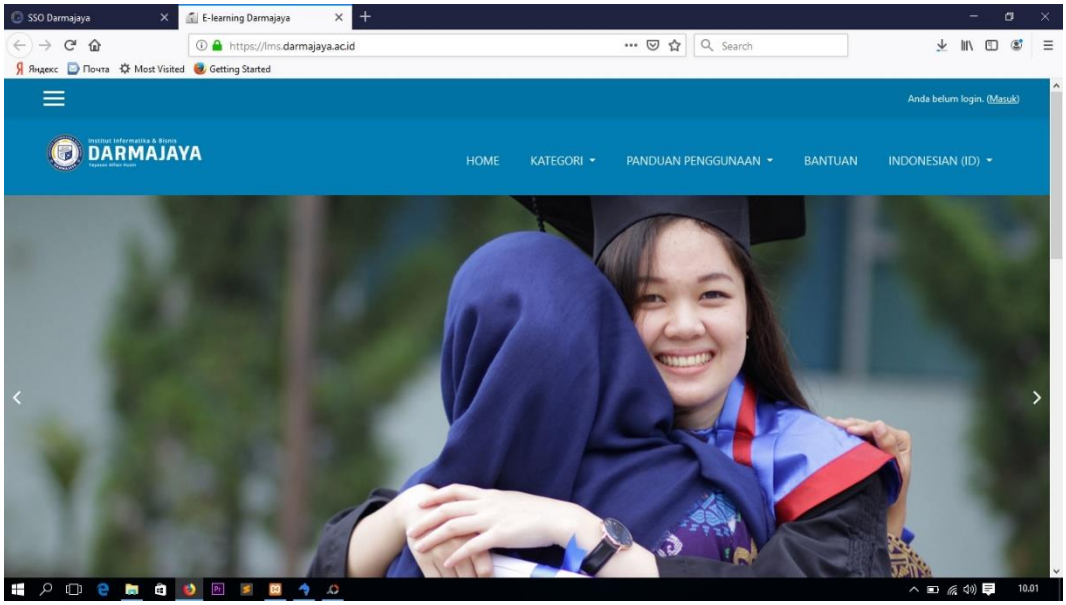
4.1.1.2.10 Tampilan Aplikasi Internet Information Center

Berikut ini merupakan tampilan Aplikasi Internet Information Center yang ada pada subdomain Darmajaya. Dapat dilihat pada gambar 4.14 :

Gambar 4.14 Internet Information Center Darmajaya

4.1.1.2.11 Tampilan Aplikasi E-learning

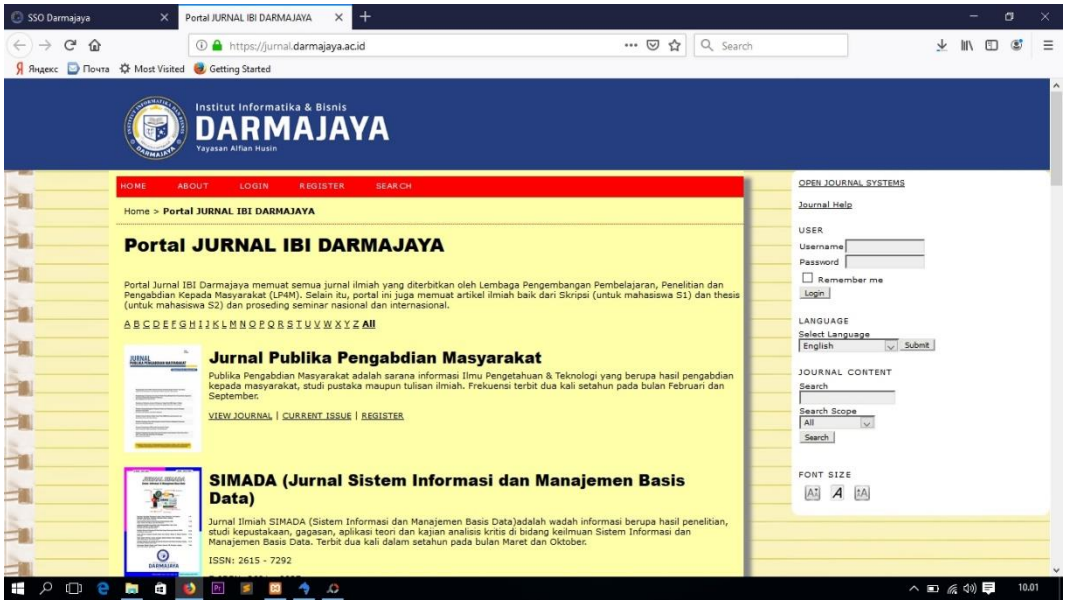
Berikut ini merupakan tampilan Aplikasi E-learning yang ada pada subdomain Darmajaya. Dapat dilihat pada gambar 4.15 :



Gambar 4.15 E-learning Darmajaya

4.1.1.2.12 Tampilan Aplikasi Jurnal

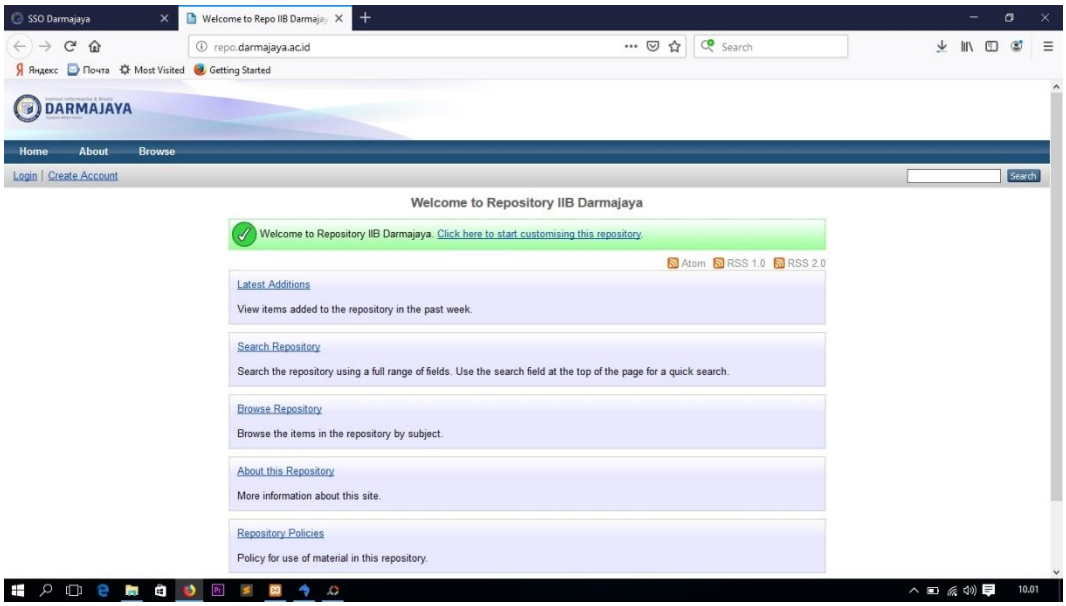
Berikut ini merupakan tampilan Aplikasi Jurnal yang ada pada subdomain Darmajaya. Dapat dilihat pada gambar 4.16 :



Gambar 4.16 Portal Jurnal Darmajaya

4.1.1.2.13 Tampilan Aplikasi Repository

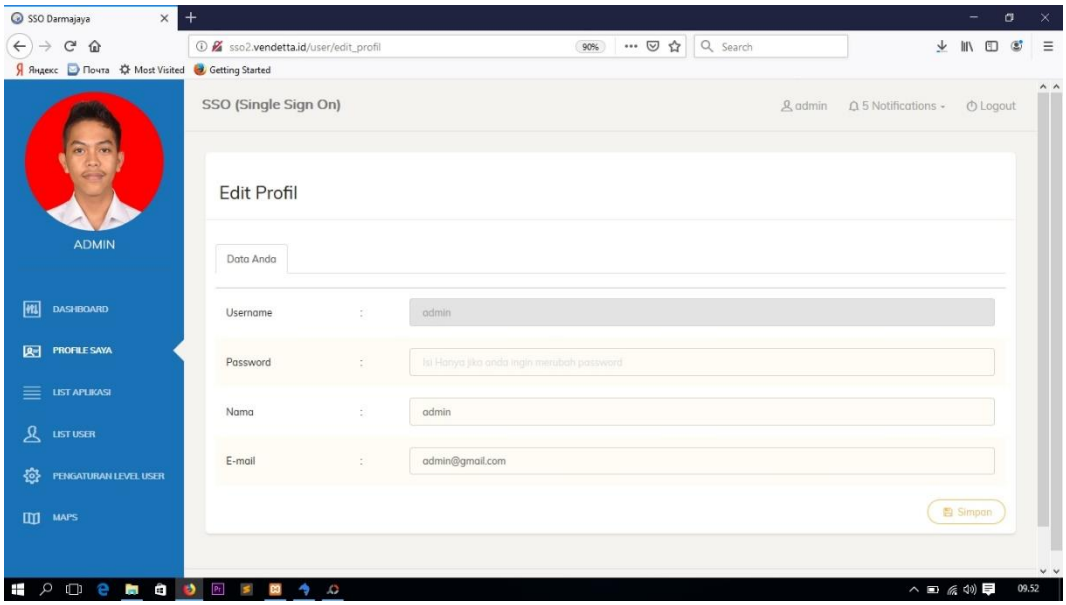
Berikut ini merupakan tampilan Aplikasi Repository yang ada pada subdomain Darmajaya. Dapat dilihat pada gambar 4.17 :



Gambar 4.17 Repository Darmajaya

4.1.1.3 Tampilan Menu Profile

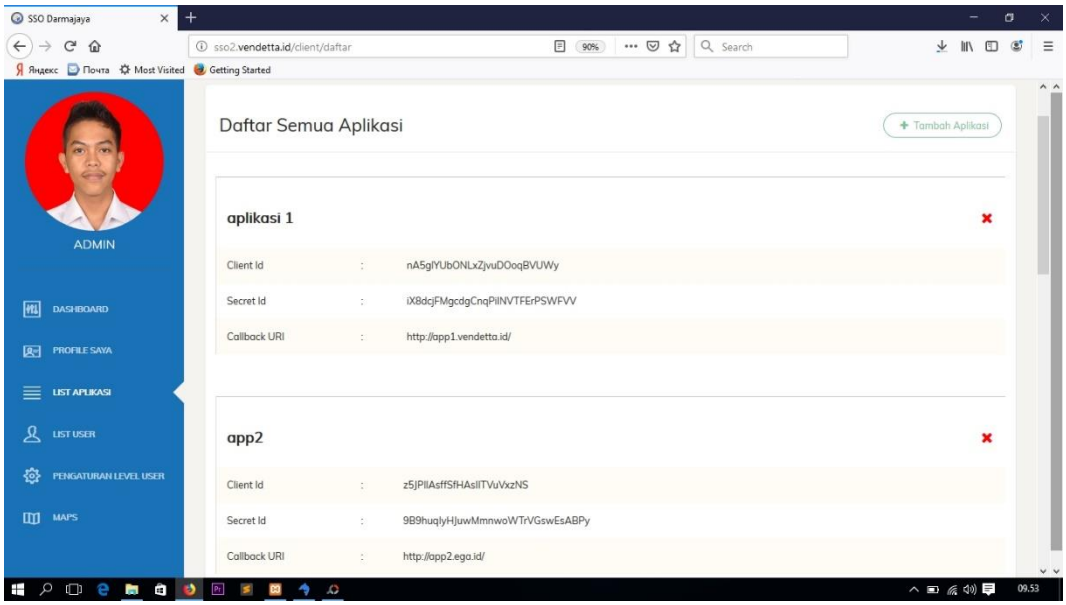
Berikut ini merupakan tampilan menu Profile Saya pada Dashboard SSO. Dapat dilihat pada gambar 4.5 :



Gambar 4.18 Menu Profile

4.1.1.4 Tampilan Menu List Aplikasi

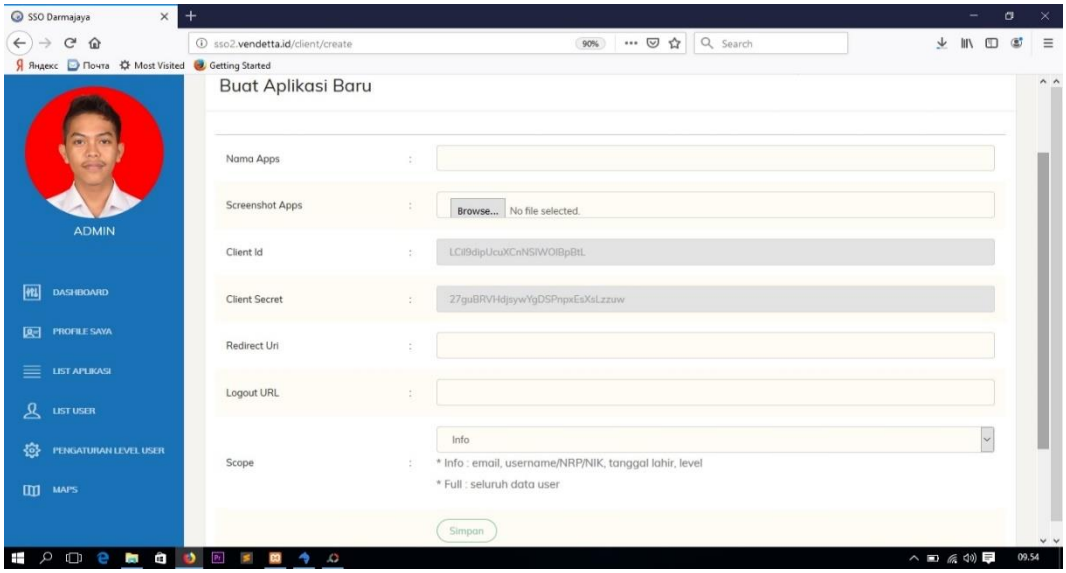
Berikut ini merupakan tampilan menu List Aplikasi pada Dashboard SSO. terdapat Client Id, Secret Id, dan callback URL. Dapat dilihat pada gambar 4.6 :



Gambar 4.19 Menu List Aplikasi

4.1.1.4.1 Tampilan Menu Tambah Aplikasi pada List Aplikasi

Berikut ini merupakan tampilan menu tambah aplikasi. Terdapat kolom yang harus diisi seperti nama aplikasi yang ingin dibuat, Redirect Url, dan Logout Url yang ada pada Database. Dapat dilihat pada gambar 4.6.1 dan 4.6.2 :

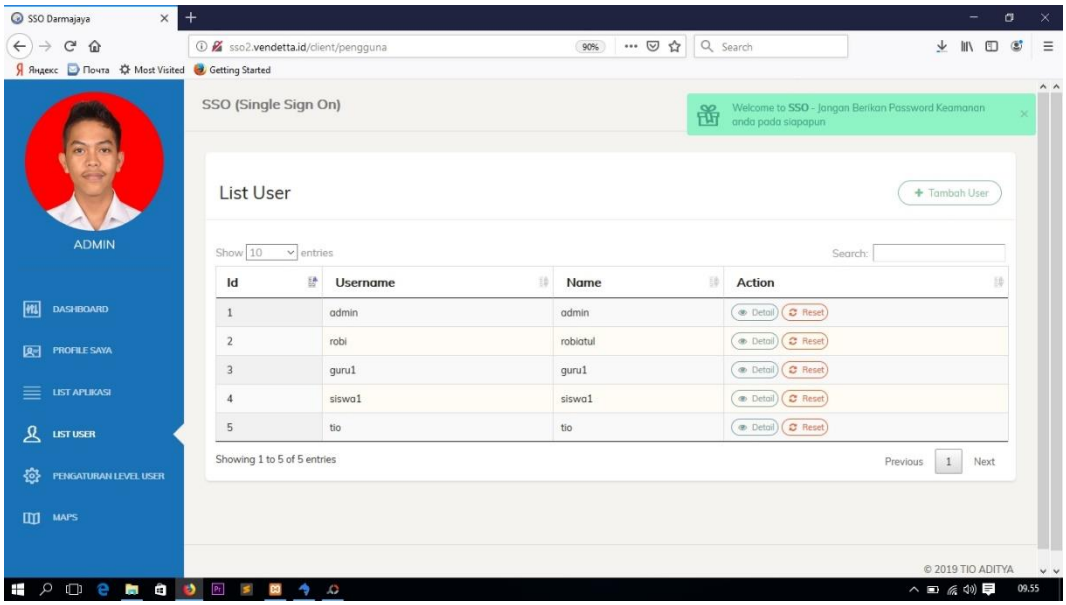


Gambar 4.19.1 Tampilan menu Tambah Aplikasi

Gambar 4.19.2 Tampilan Database Redirect Url dan Logout Url

4.1.1.5 Tampilan Menu List User

Berikut ini merupakan tampilan menu List User pada Dashboard SSO. dapat dilihat pada gambar 4.7 :

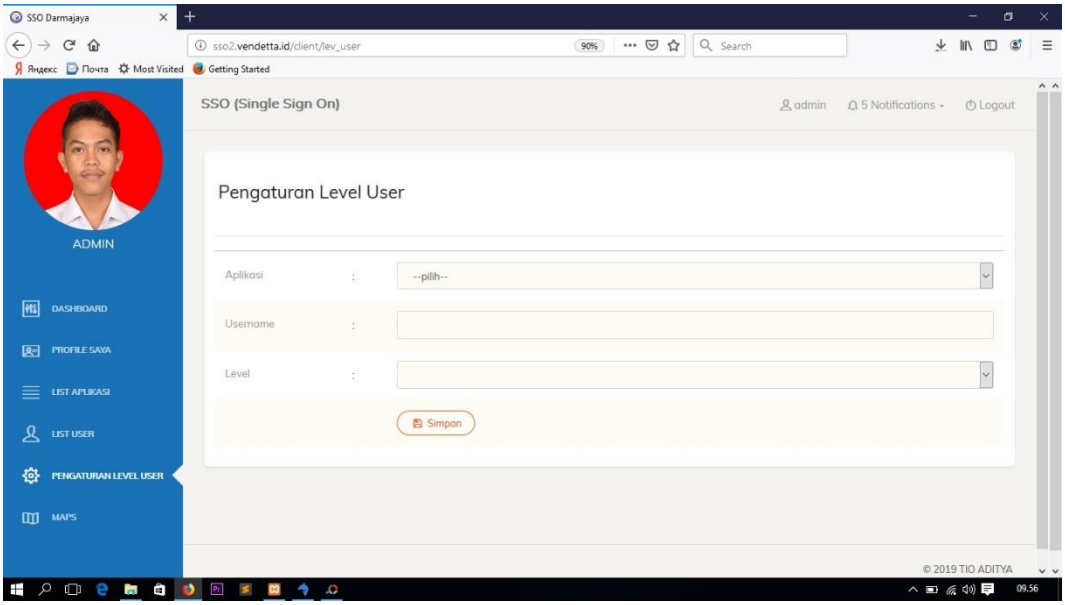


Gambar 4.20 Menu List User

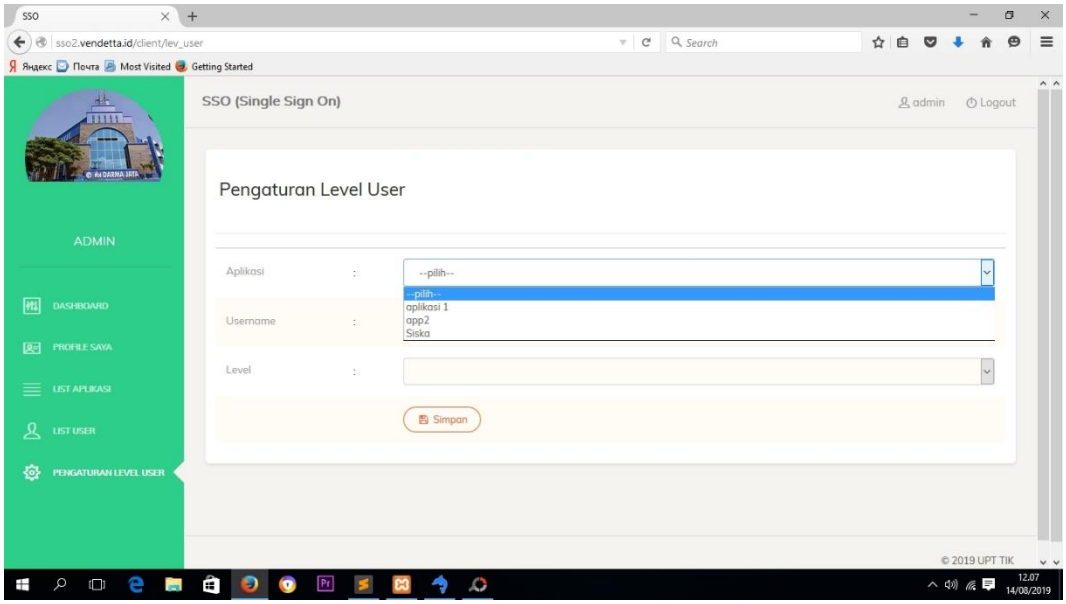
Gambar 4.20.1 Detail User

4.1.1.6 Tampilan Menu Pengaturan Level User

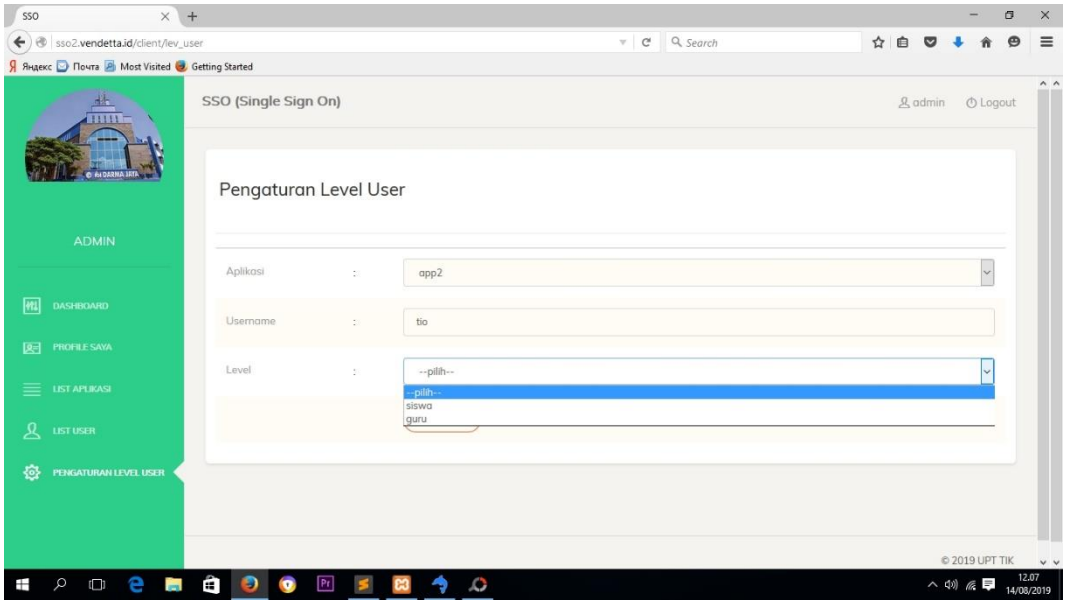
Berikut ini merupakan tampilan menu Pengaturan Level User pada Dashboard SSO. dapat dilihat pada gambar 4.8 :



Gambar 4.21 Menu Pengaturan Level User



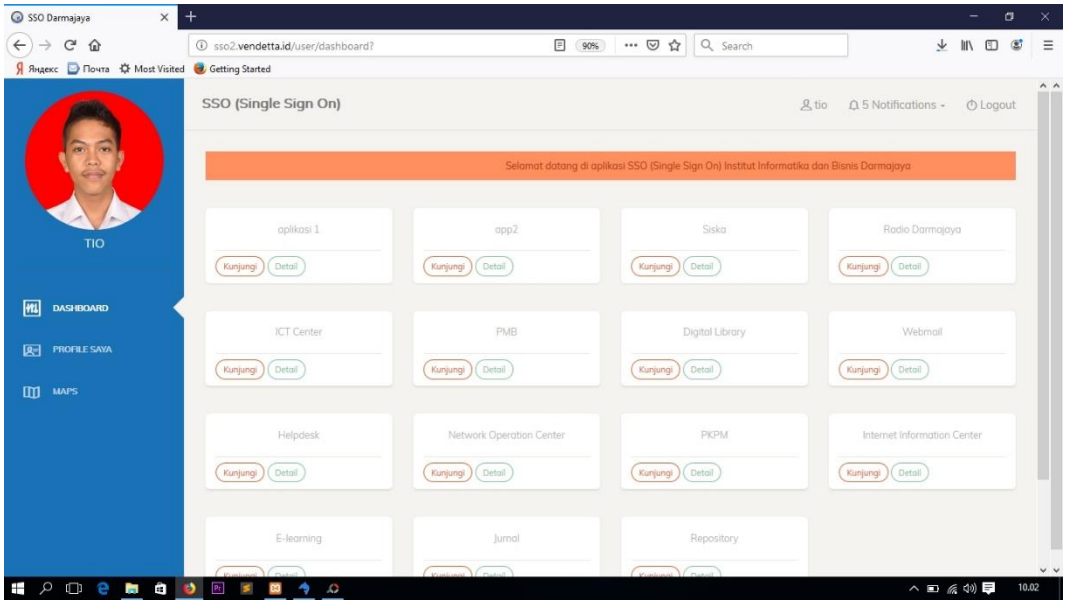
Gambar 4.21.1 Percobaan pengaturan level user



Gambar 4.21.1 Percobaan pengaturan level user

4.1.1.7 Tampilan Dashboard User

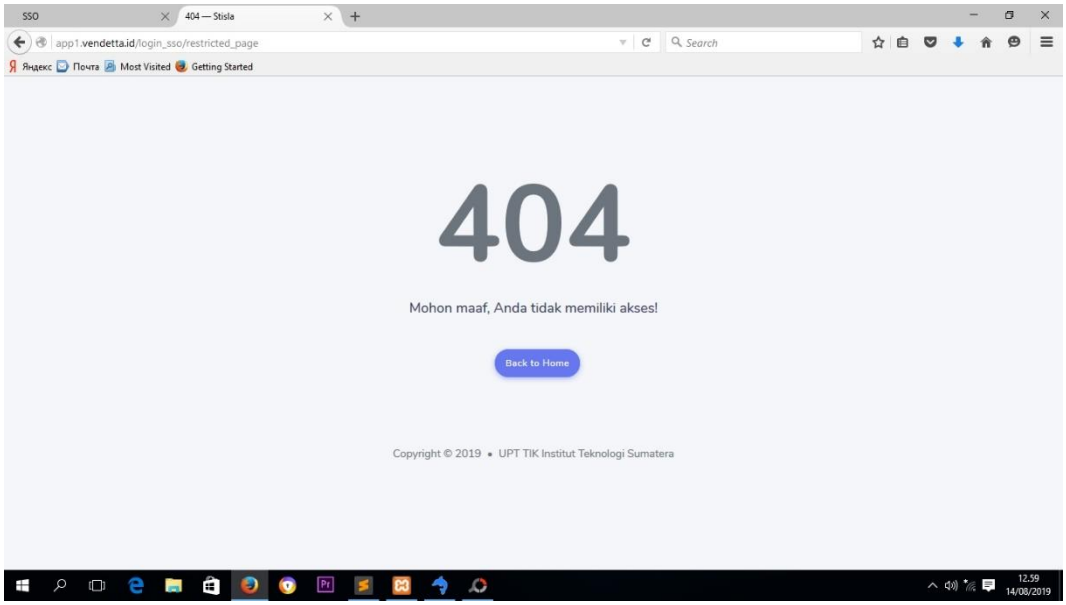
Berikut ini merupakan tampilan menu pada user yang telah terdaftar dalam database dan sudah login kedalam SSO. Dapat dilihat pada gambar 4.11 :



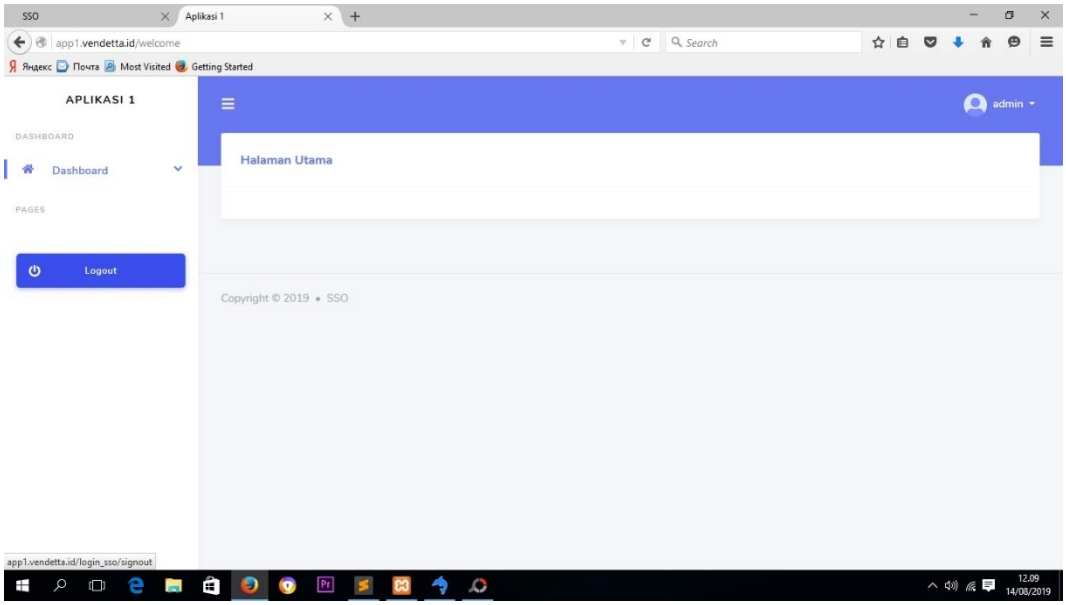
Gambar 4.22 Dashboard User

4.1.1.7.1 Tampilan Aplikasi 1 pada Dashboard User

Berikut ini merupakan tampilan Aplikasi 1 jika kita klik Kunjungi pada dashboard user yang telah terdaftar dalam database dan sudah login. Jika memiliki akses dan juga jika tidak memiliki akses. Dapat dilihat pada gambar 4.12 dan 4.13 :



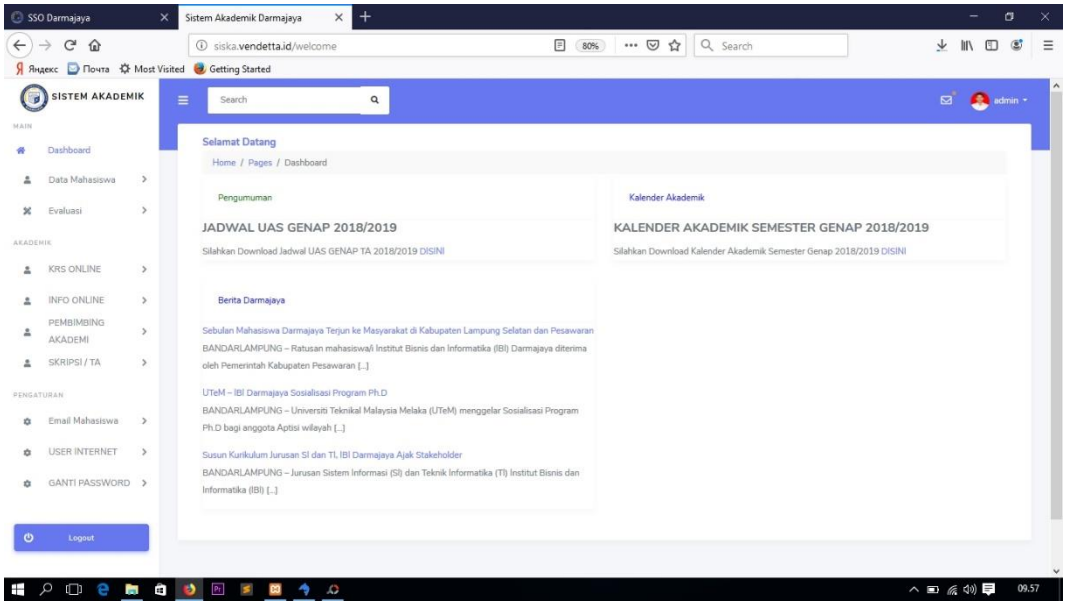
Gambar 4.23 Tampilan Aplikasi 1 jika tidak memiliki Akses



Gambar 4.24 Tampilan Aplikasi 1 jika memiliki Akses

4.1.1.7.2 Tampilan Aplikasi 2 pada Dashboard User

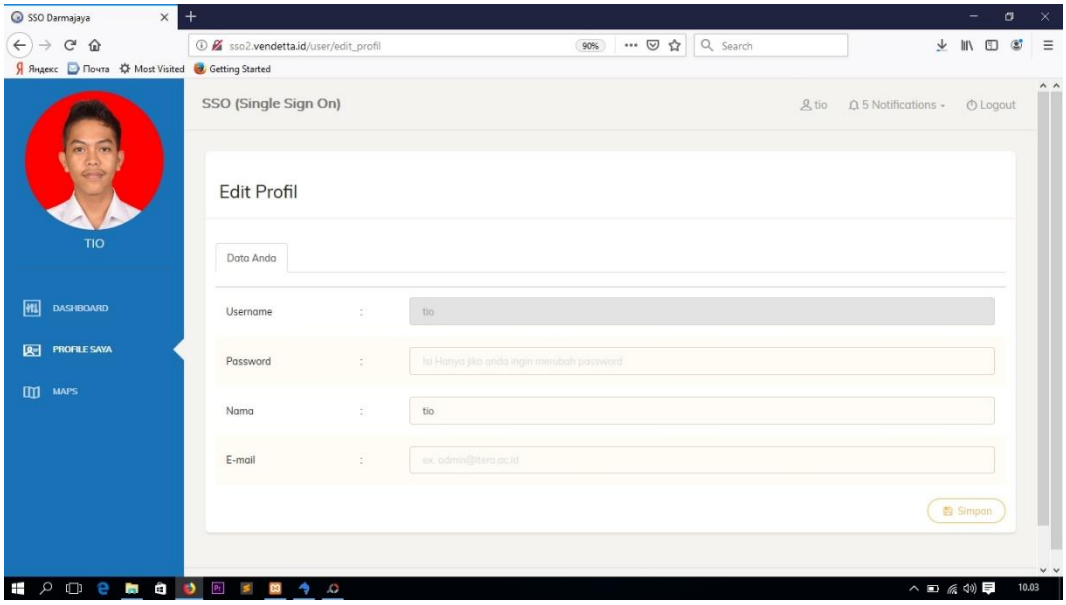
Berikut ini merupakan tampilan Aplikasi 2 pada Dashboard user. Dapat dilihat pada gambar 4.14 :



Gambar 4.25 Tampilan Aplikasi Siska di Dashboard user

4.1.1.8 Tampilan Profile Saya pada Dashboard User

Berikut ini merupakan tampilan menu profile saya pada user. Dapat dilihat pada gambar 4.15 :



Gambar 4.26 Edit Profile User

4.2 Pembahasan

4.2.1 Pengujian Sistem

Pemograman adalah kegiatan penulisan program yang nantinya dieksekusi oleh komputer berdasarkan hasil dari analisa dan juga perancangan sistem. Sebelum program akan diimplementasikan, maka program harus terbebas dari kesalahan. Pengujian sistem ini dilakukan untuk menemukan kesalahan-kesalahan yang memungkinkan terjadi.

4.2.2 Lingkungan Pengujian Sistem

Setelah tahap implementasi dilakukan tahap selanjutnya dengan pengujian dari implemntasi yang berhasil dibuat. Tahap pengujian diperlukan agar diketahui hasil dari program implementasi sistem. Program adalah kegiatan penulisan kode

program yang akan dieksekusi oleh komputer berdasarkan hasil dari analisis dan perancangan sistem.

Lingkungan pengujian ini menggunakan spesifikasi perangkat keras sebagai berikut:

1. Prosessor Intel Core i3-6006U (2.0 GHz, 3MB L3 Cache)
2. Laptop Acer Aspire E 14
3. Memori 4 GB DDR4
4. Harddisk 500GB HDD

Sedangkan lingkungan pengujian menggunakan perangkat lunak sebagai berikut:

1. Sistem Operasi Microsoft Windows 10 Professional
2. XAMPP for Windows v3.2.1 dengan *Database* SQLyog 64 Ultimate
3. *Web browser* Google Chrome dan Mozilla Firefox
4. Sublime Text 3

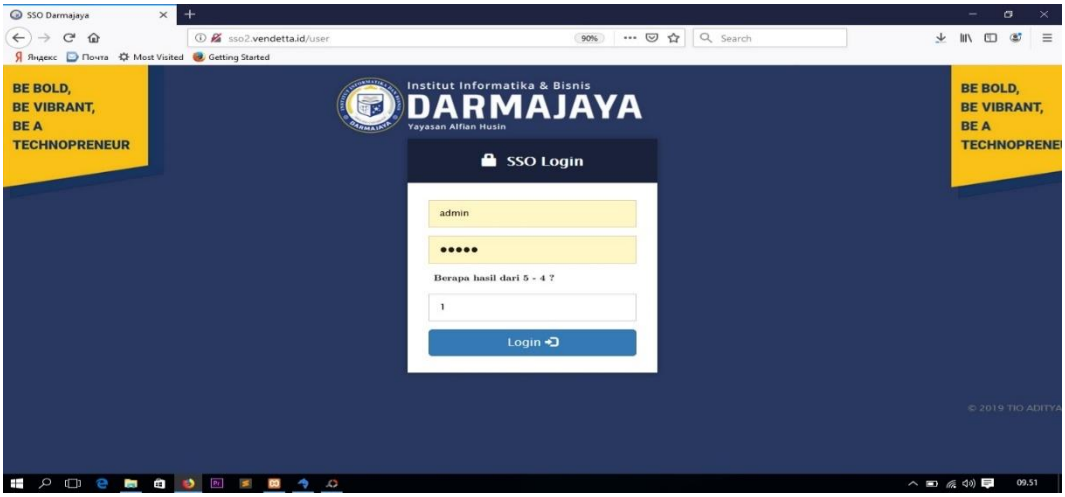
Alamat DNS yang digunakan untuk pada SSO ini menggunakan alamat *virtual host*.

4.2.3 Pengujian Sistem *Single Sign-On*

Pada pengujian aplikasi *web* sistem SSO (*Single Sign-On*), seorang pengguna mengakses salah satu dari aplikasi *web*, kemudian yang nantinya akan diarahkan ke *single sign-on server* dan pengguna memasukkan *password*-nya. Ketika pengguna berhasil masuk atau *login* maka secara otomatis seluruh aplikasi *web* yang lainnya sudah terbuka sendiri tanpa perlu memasukkan *password* kembali.

Proses pengujiannya adalah sebagai berikut :

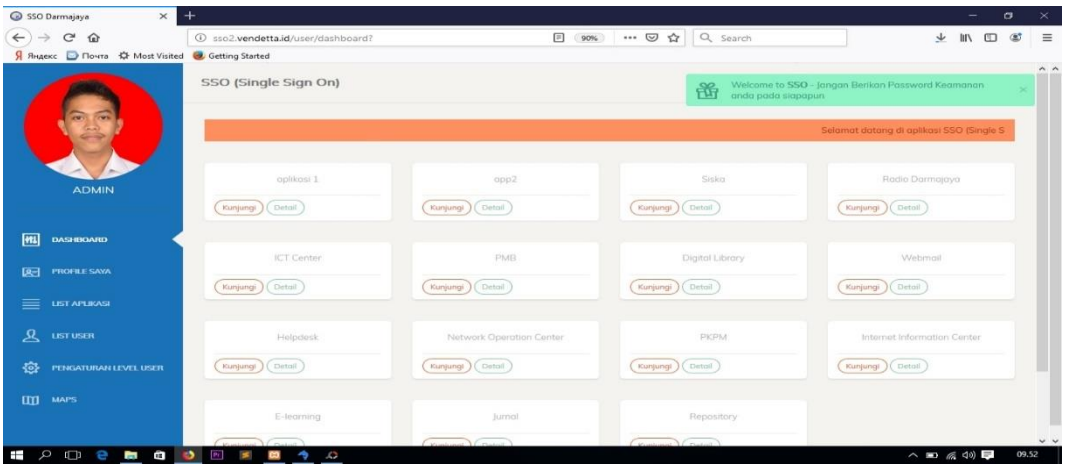
1. *User* melakukan *login* pada *server single sign-on* dengan memasukkan *username*, *password*, dan juga autentikasi penjumlahan.



Gambar 4.27 Halaman *Login* Sistem *Single Sign-On*

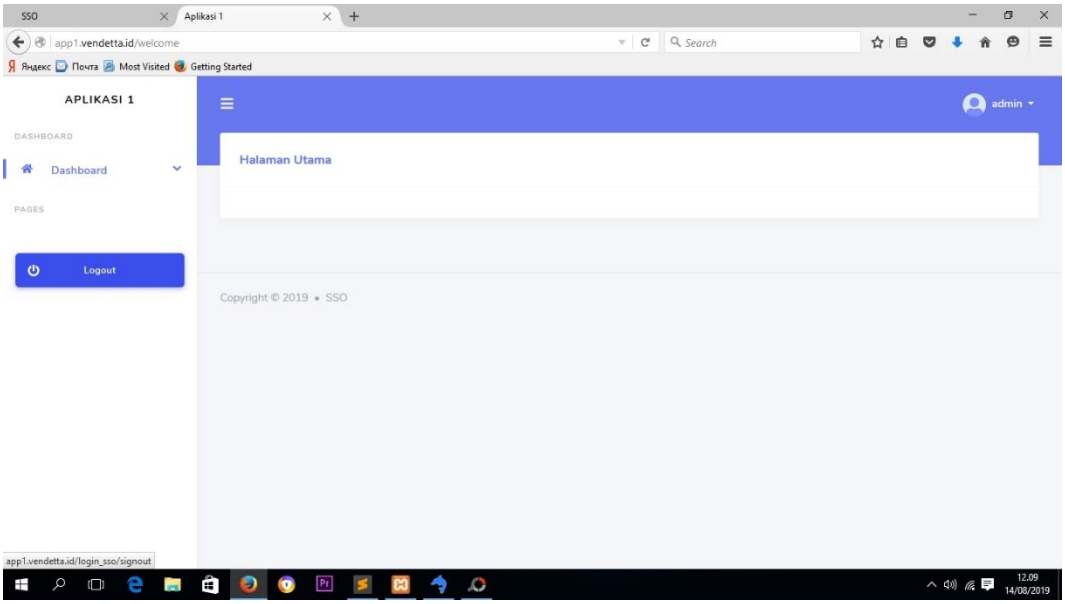
Pengujian sistem *single sign-on* dengan memasukkan *username*, *password*, serta penjumlahan angka, jika *username*, *password*, dan penjumlahannya sesuai dengan di *server* maka *login* telah berhasil, dan langsung menuju kehalaman dashboard *web portal*.

2. *User* berhasil melakukan login dan memasuki halaman dashboard *web portal*.



Gambar 4.28 Dashboard *web portal single sign-on*

3. *User*_mengakses Aplikasi 1 dan berhasil melakukan *login* tanpa memasukkan *password* kembali.



Gambar 4.29 Aplikasi *web* 1

Ketika *user* mengakses aplikasi *web* yang lain maka secara otomatis *web* yang sudah dalam keadaan *login* dan memiliki hak akses, tanpa harus melakukan *login* untuk kedua kalinya dan begitu pula selanjutnya. Begitu pula sebaliknya, ketika *user* melakukan *logout* dari salah satu situs *web* maka secara otomatis situs yang lain akan *logout* otomatis dengan sendirinya tanpa menekan tombol *logout* untuk kedua kalinya.

4.2.4 Kesimpulan Pengujian

Secara umum, pengujian ini memiliki hasil sebagai berikut :

1. Sistem s*ingle sign-on* telah dibangun dapat berjalan dengan baik, seorang *user* tidak perlu *login* untuk kedua kalinya untuk mengakses aplikasi-aplikasi yang ada di SSO. *user* cukup melakukan sekali *login* dan juga sekali *logout*.
2. Pengujian berdasarkan prosedur sistem *single sign-on* telah berhasil diujikan.
3. Autentikasi dengan menggunakan Captcha penjumlahan angka memperkuat keamanan sistem *single sign-on*.
4. Seluruh aplikasi yang diimplementasikan dapat berjalan dengan baik.

BAB V
SIMPULAN DAN SARAN

5.1 Simpulan

Beberapa hal yang dapat disimpulkan dari pelaksanaan tugas akhir ini adalah :

1. Berhasil membangun sistem SSO (*Single Sign-On*) berbasis web, dimana seorang *user* hanya perlu sekali login atau memasukkan *username* dan *password* untuk beberapa situs *web* tanpa harus memasukkannya untuk kedua kalinya.
2. Autentikasi *login* menggunakan Captcha yang merupakan salah satu solusi untuk keamanan sistem *login* terutama sistem *Single Sign-On*, dimana jika *user* salah memasukkan Captcha, maka automatis web akan me-refresh atau mengulang seperti semula (perlu memasukkan *username* dan *password* kembali).
3. SSO dapat menanggulangi kemungkinan akses *intercept* terhadap penyalahgunaan hak akses *user* SSO karena kode *sesi_id* yang dikirim bersifat dinamis dan hanya dapat digunakan satu kali otentikasi dengan batas waktu tertentu.

5.2 Saran

Saran-saran yang berkaitan dengan pelaksanaan tugas akhir ini adalah :

1. Aplikasi sistem SSO (*Single Sign-On*) ini perlu di uji pada kasus yang lebih besar dan memiliki lingkungan yang bervariasi agar diketahui seberapa besar kinerja aplikasi SSO ini. Pada tugas akhir ini, sistem SSO hanya diuji dengan jaringan *virtualhost*.
2. *Database* yang digunakan aplikasi ini masih sangat sederhana jika dibandingkan dengan aplikasi SSO yang dimiliki aplikasi lain. Sehingga perlu dilakukannya konfigurasi lebih lanjut untuk menghadapi masalah ini.
3. Untuk meningkatkan keamanan SSO ini, dapat menggunakan Autentikasi lain seperti SAMS, XAML.

DAFTAR PUSTAKA

Alkhatib Ghazi, & Rine David. (2009). *Integrated Approaches in Information Technology and Web Engineering: Advancing Organizational Knowledge Sharing.* IGI Global.

Ardagna Claudio Agostino, Frati Fulvio, & Gianini Gabriele. (2009). *Open Source in WebBased Applications : A Case Study on Single Sign-On.* Chapter VI: IGI Global.

Ariyus Dony. (2006). *Computer Security.* Penerbit Andi Yogyakarta.

Bulger Brad, Greenspan Jay, & Wall David. (2004). *MySQL/PHP Database Applications, Second Edition.* Indiana: Wiley Publishing, Inc, Indianapolis.

B.Raharjo. Belajar Otodidak Framework Codeigniter, Bandung: Informatika Bandung, 2015.

E-Book "Single Sign On, Keberos dan LDAP". Universitas Sumatera Utara. repository.usu.ac.id/bitstream/.../3/Chapter%20II.pdf. Diakses tanggal 9 Oktober 2018.

E-Book "Tinjauan Keamanan Sistem Pada Teknologi Cloud Computing". Universitas Sumatera Utara. https://www.academia.edu/5088063/Jurnal-Keamanan-Komputer Diakses tanggal 15 Juli 2019.

E-Book "Analisis Teknologi Sistem Single Sign On SSO Dengan Penerapan Central Authentication Service CAS". Universitas Guna Darma. https://www.researchgate.net/publication/308414625_ANALISIS_TEKNOLOGI_SINGLE_SIGN_ON_SSO_DENGAN_PENERAPAN_CENTRAL_AUTHENTICATION_SERVICE_CAS_PADA_ UNIVERSITAS_BINA_DARMA Diakses tanggal 14 Juli 2019.

Hursti Jani, "*Single Sign-On*.", *Department of Computer Science Helsinki University of Technology*, 1997.

Kanda, "*Integrasi Single Sign-On OpenID pada Website berbasis PHP"*, Retrieved from Kandar: http://www.kandar.info, diakses 9 Oktober 2018.

Nasir, M. (2003). *Metode Penelitian.* Jakarta: Ghalia Indonesia.

N. Heijmink, "*Secure Single Sign-On A comparision of protocols*," CCV & Radboud University Nijmegen, 2015.

Rudy, Riechie, & O. G. (2009). *Integrasi Aplikasi Menggunakan Single Sign On Berbasiskan Lightweight Directory Access Protocol (LDAP) dalam portal binus@ccess (BEE-PORTAL).* Jakarta: Universitas Bina Nusantara.

Rohi, Abdulloh. Easy & Simple Web Programming, Jakarta: PT Elex Media Komputindo, 2016.

Saputro, & Muhammad, A. Y. (2012). *Implementasi Sistem Single Sign On/Single Sign OutBerbasis Central Authentication Service Protocol Pada Jaringan Berbasis LightweightDirectory Access Protocol.* Universitas Diponegoro.

Y. N. Kunang and I. Z. Yadi, "*Sistem Single Sign on Universitas Berbasis CAS-LDAP*," Seminar Nasional Inovasi dan Tren (SNIT), no. 12, pp. 1–7, 2014.

LAMPIRAN

```
<!DOCTYPE html>

<html>

<meta charset="UTF-8">

<title>SSO </title>

<link rel="icon"
type="image/png"
sizes="96x96"
href="https://cdn2.iconfinder.com/data/icons/human-resource-1/50/13-512.png">

<meta content='width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no' name='viewport'>

<link
href="<?=base_url()?>assets/bootstrap/css/bootstrap.min.css"
rel="stylesheet" type="text/css"
/>

<link
href="<?=base_url()?>assets/fonts/fontawesome/css/font-awesome.min.css"
rel="stylesheet" type="text/css"
/>

<link
href="<?=base_url()?>assets/css/loginstyle.css" rel="stylesheet"
type="text/css" />

<script
src="<?=base_url()?>assets/js/jquery-2.2.4.min.js" ></script>

<script
src="<?=base_url()?>assets/bootstrap/js/bootstrap.min.js"></script>

<script type="text/javascript">

  $(document).ready(function(){



        $(document).on('click',
'.lupa_password', function(e){

                e.preventDefault();

  $('#modal_lupa_password').modal
();

        });



        $(document).on('submit',
'#form_lupa_password',
function(e){

                e.preventDefault();

  $('#notif_lupa_password').html('L
oading...');

                var data =
$('#form_lupa_password').serialize(
);

                $.ajax({

                        url:
'<?=base_url()?>welcome/lupa_pas
sword',

                        type: 'POST',

                        dataType:
'JSON',

                        data: data,

                        success:
function(msg){

  if(msg.status == 'ok'){

  $('#show_form_upload').hide('slo
w');

  $('#notif_lupa_password').html(m
sg.text);

  // location.reload();

                                }else{
```

```
  $('#notif_lupa_password').html
(msg.text);
                                    }
                                }
                    });
            });


            <?php
            if($this->input-
>get('token', true) != "" || $this-
>input->get('token', true) !=
NULL){
                    $this->load-
>Model('Model_user');
                    $get_data =
$this->Model_user-
>get_data(array('token' =>
$this->input->get('token', true),
'status' => '0'),
'tb_reset_password');
                    $token = @$this-
>input->get('token', true);
                    if($get_data-
>num_rows() != 0){
                            $email =
$get_data->row()->username;
            ?>

  $('#modal_reset_password').m
odal();



  $(document).on('submit',
'#form_reset_password',
function(e){

  e.preventDefault();

  $('#notif_reset_password').htm
l('Loading...');
                    var data =
$('#form_reset_password').serialize
();
                    $.ajax({
                            url:
'<?=base_url()?>welcome/reset_pas
sword',
                            type:
'POST',

  dataType: 'JSON',
                            data:
data,

  success: function(msg){

  if(msg.status == 'ok'){



  $('#show_form_reset_password').
hide('slow');



  $('#notif_reset_password').html(m
sg.text);

            // location.reload();

  }else{



  $('#notif_reset_password').html(m
sg.text);

  }
                            }
                    });
            });
            <?php
                    }
```

```
            }
            ?>
  });
</script>
<style type="text/css">
  body{
            background-image:
url("http://www.usqbc.org/reso
urces/images/various/login-
backgrounds/misty_forest2.jpg"
);
  }
  html {
     position: relative;
     min-height: 100%;
  }

</style>

<?php //echo $script_captcha; //
javascript recaptcha ?>
  <body>
  <!-- Inspired by
https://codepen.io/transportedm
an/pen/NPWRGq -->

  <!-- Remeber to put all the
content you want on top of the
slider below the slider code -->

  <div class="login-page">
            <div class="login-
content">
                  <div
class="container">
                        <div
class="row">
                              <div
class="col-md-7 col-sm-7"
style="color: #fff;">

  <blockquote>

            <h1 style="color:
#fff"><strong>Single Sign On
</strong></h1>

            <p>Selamat Datang di
Sistem Single Sign On.</p>

            <p>Jangan memberikan
akun login (nama pengguna dan
kata sandi) anda pada siapapun.
<br>Keamanan data anda terletak
pada anda sendiri.</p>

            <footer style="color:
#fff">Administrator</footer>

  </blockquote>
                              </div>
                              <div
class="col-lg-4 col-md-4 col-md-
offset-1 col-sm-5">

  <div class="login-form">

            <div class="form-title">

                  <h2><i
class="glyphicon glyphicon-
lock"></i>  <b>SSO</b>
Login</h2>

            </div>
```

```
            <div class="form-
body">

<?php if ($this->session-
>flashdata('msg')!=NULL){?>

<div class="alert alert-danger
alert-dismissible">

<button type="button"
class="close" data-
dismiss="alert" aria-
hidden="true">×</button>

<h4><i class="icon fa fa-
ban"></i> Alert!</h4>

  <?= $this->session-
>flashdata('msg'); ?>

</div>

<?php } ?>



                    <form
action="<?php echo
get_the_current_url() ?>"
method="post">

                            <div
class="form-group">



                            <input
class="form-control" data-
val="true" data-val-
required="The User name field
is required." id="user"
name="username"
placeholder="Email Pengguna"
value="" type="text" required>
                            </div>

                            <div
class="form-group">

                                <div
class="text-error">


  <span class="field-validation-
valid" data-valmsg-
for="Password" data-valmsg-
replace="true"></span>

                                </div>

                                <input
class="form-control" data-
val="true" data-val-required="The
Password field is required."
id="pwd" name="password"
placeholder="Kata Sandi"
type="password" value=""
required>

                            </div>

                            <div
class="form-group">

                                <!--
Berapa hasil dari: -->

                                <img
src="<?=base_url().'welcome/cpch'
?>" class="img-responsive"/>

            </div>

            <div class="form-group">

                                <input
class="form-control" data-
val="true" data-val-
```

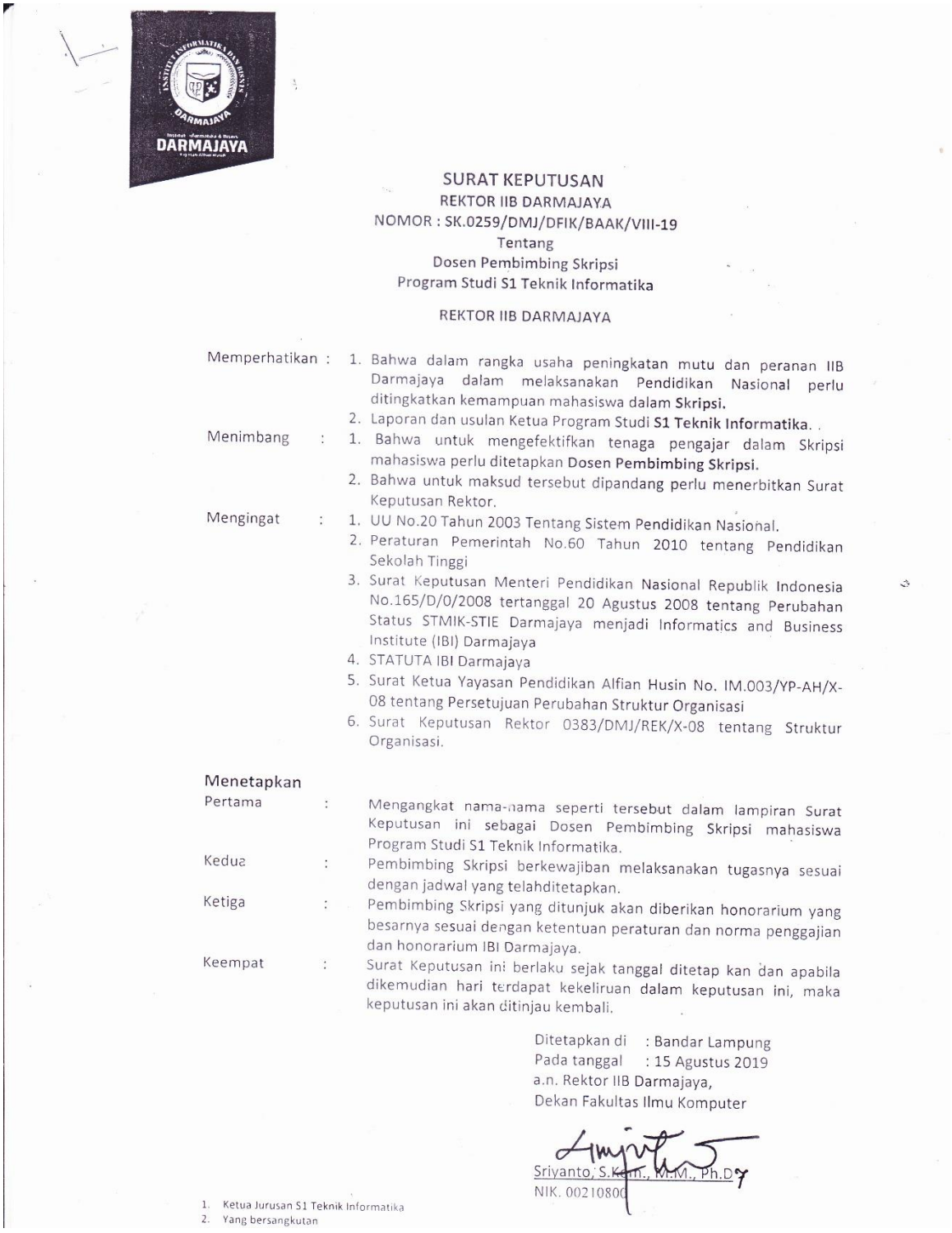
```
required="Captcha is
required." id="captcha"
name="captcha"
placeholder="Hasil" value=""
type="text" required>

                        </div>

                        <button
type="submit" name="submit"
value="submit" class="btn btn-
primary btn-lg btn-
block">Login <span
class="glyphicon glyphicon-log-
in"></span></button>

                        <!--
<button type="submit"
name="submit"
value="submit" class="btn btn-
primary btn-lg
">Register</button> -->

                        <!-- <hr/>
-->

                        <!--
<center><h4>

                        <span
style="color: red">

                        Lupa
password? klik<a href="#"
class="lupa_password"> di
sini</a>


  </span></h4>

                        </center>
-->

                    </form>

            </div>
  </div>

                        </div>

                    </div>

                </div>

            </div>

  </div>

            <!-- Modal -->

            <div
id="modal_lupa_password"
class="modal fade" role="dialog">

                <div class="modal-
dialog">


                    <!-- Modal
content-->

                    <div
class="modal-content">

                        <div
class="modal-header"
style="background-color:
#112058">


  <button type="button"
class="close" data-
dismiss="modal" style="color:
#fff">&times;</button>


  <h4 class="modal-title"
style="color: #fff"> <span
class="glyphicon glyphicon-
lock"></span> Lupa
Password</h4>

                        </div>

                        <div
class="modal-body">


  <div id="show_form_upload">


            <div class="alert alert-
```

```
danger">

                    Cek pada bagian
<strong>spam</strong> email
anda apabila tidak ada balasan
email oleh system di inbox email
anda

          </div>

          <form
id="form_lupa_password">

                    <div
class="form-group">


  <label>Email
Pengguna:</label>

                              <input
type="text"
name="email_lupa_password"
id="email_lupa_password"
class="form-control"
placeholder="Ex:
nama_depan.nim@student.itera.
ac.id" style="border-radius:
0px" required />

                    </div>

                    <div
class="form-group">

  <img
src="<?=base_url().'welcome/cp
ch'?>" class="img-
responsive"/>

</div>

<div class="form-group">

                              <input
class="form-control" data-
val="true" data-val-
required="Captcha is required."
id="captcha_reset_password"
name="captcha_reset_password"
placeholder="captcha" value=""
type="text" style="border-radius:
0px" required>

                    </div>

                    <div class="form-
group">

                              <button
type="submit" class="btn btn-
primary" style="color: #DAA520;
background-color: rgba(0,0,0,0.15);
border: 0px"><span
class="glyphicon glyphicon-
refresh"></span> Proses</button>

                    </div>

          </form>

  </div>

  <div
id="notif_lupa_password"></div>
                              </div>

                    </div>


          </div>

          </div>

          <!-- Modal Reset Password
-->

          <div
id="modal_reset_password"
class="modal fade" role="dialog">

                    <div class="modal-
dialog">
```

```
                    <!--
Modal content-->

                    <div
class="modal-content">


  <div class="modal-header"
style="background-color:
#112058">


  <button type="button"
class="close" data-
dismiss="modal" style="color:
#fff">&times;</button>


  <h4 class="modal-title"
style="color: #fff"> <span
class="glyphicon glyphicon-
lock"></span> Reset
Password</h4>


  </div>


  <div class="modal-body">


  <div
id="show_form_reset_password
">


        <form
id="form_reset_password">


                <div
class="form-group">


  <label>Email
Pengguna:</label>


                    <input
type="hidden"
name="token_reset_password"
id="token_reset_password"
class="form-control"
value="<?=$token?>">

                    <input
type="text"
name="email_reset_password"
id="email_reset_password"
class="form-control"
placeholder="Ex:
nama_depan.nim@student.itera.ac.
id" style="border-radius: 0px"
value="<?=$email?>" readonly
required />

                </div>


                <div class="form-
group">


  <label>Password Baru:</label>


                    <input
type="password"
name="password_baru_reset_pass
word"
id="password_baru_reset_passwor
d" class="form-control"
style="border-radius: 0px"
placeholder="Kata sandi baru"
required />

                </div>


                <div class="form-
group">


  <label>Ulangi Password:</label>


                    <input
type="password"
name="ulangi_password_reset_pas
sword"
id="ulangi_password_reset_passwo
rd" class="form-control"
style="border-radius: 0px"
placeholder="Ulangi kata sandi"
required />
```

```
                </div>

                <div
class="form-group">

  <label>Kode Aktivasi:</label>

                    <input
type="text"
name="kode_aktivasi"
id="kode_aktivasi"
class="form-control"
placeholder="Diisi dengan kode
aktivasi yang dikirim melalui
email" style="border-radius:
0px" required />

                </div>

                <div
class="form-group">

                    <button
type="submit" class="btn btn-
primary" style="color:
#DAA520; background-color:
rgba(0,0,0,0.15); border:
0px"><span class="glyphicon
glyphicon-refresh"></span>
Proses</button>

                </div>

            </form>

  </div>

  <div
id="notif_reset_password"></di
v>

  </div>

                    </div>
                </div>
            </body>
        </html>
```

Lampiran 1 : Surat Keputusan Penulilsan Skripsi



SURAT KEPUTUSAN
REKTOR IIB DARMAJAYA
NOMOR : SK.0259/DMJ/DFIK/BAAK/VIII-19
Tentang
Dosen Pembimbing Skripsi
Program Studi S1 Teknik Informatika

REKTOR IIB DARMAJAYA

Memperhatikan :
1. Bahwa dalam rangka usaha peningkatan mutu dan peranan IIB Darmajaya dalam melaksanakan Pendidikan Nasional perlu ditingkatkan kemampuan mahasiswa dalam **Skripsi.**
2. Laporan dan usulan Ketua Program Studi **S1 Teknik Informatika.**

Menimbang :
1. Bahwa untuk mengefektifkan tenaga pengajar dalam Skripsi mahasiswa perlu ditetapkan **Dosen Pembimbing Skripsi.**
2. Bahwa untuk maksud tersebut dipandang perlu menerbitkan Surat Keputusan Rektor.

Mengingat :
1. UU No.20 Tahun 2003 Tentang Sistem Pendidikan Nasional.
2. Peraturan Pemerintah No.60 Tahun 2010 tentang Pendidikan Sekolah Tinggi
3. Surat Keputusan Menteri Pendidikan Nasional Republik Indonesia No.165/D/0/2008 tertanggal 20 Agustus 2008 tentang Perubahan Status STMIK-STIE Darmajaya menjadi Informatics and Business Institute (IBI) Darmajaya
4. STATUTA IBI Darmajaya
5. Surat Ketua Yayasan Pendidikan Alfian Husin No. IM.003/YP-AH/X-08 tentang Persetujuan Perubahan Struktur Organisasi
6. Surat Keputusan Rektor 0383/DMJ/REK/X-08 tentang Struktur Organisasi.

Menetapkan

Pertama : Mengangkat nama-nama seperti tersebut dalam lampiran Surat Keputusan ini sebagai Dosen Pembimbing Skripsi mahasiswa Program Studi S1 Teknik Informatika.

Kedua : Pembimbing Skripsi berkewajiban melaksanakan tugasnya sesuai dengan jadwal yang telahditetapkan.

Ketiga : Pembimbing Skripsi yang ditunjuk akan diberikan honorarium yang besarnya sesuai dengan ketentuan peraturan dan norma penggajian dan honorarium IBI Darmajaya.

Keempat : Surat Keputusan ini berlaku sejak tanggal ditetap kan dan apabila dikemudian hari terdapat kekeliruan dalam keputusan ini, maka keputusan ini akan ditinjau kembali.

Ditetapkan di : Bandar Lampung
Pada tanggal : 15 Agustus 2019
a.n. Rektor IIB Darmajaya,
Dekan Fakultas Ilmu Komputer

Sriyanto, S.Kom., M.M., Ph.D
NIK. 00210800

1. Ketua Jurusan S1 Teknik Informatika
2. Yang bersangkutan

Lampiran 1 : (Lanjutan).

Lampiran : Surat Keputusan Rektor IIB Darmajaya
Nomor : SK. 0259/DMJ/DFIK/BAAK/VIII-19
Tanggal : 15 Agustus 2019
Perihal : Pembimbing Penulisan Skripsi
Program Studi Strata Satu (S1) Teknik Informatika

Judul Penulisan Sripsi dan Dosen Pembimbing
Program Studi Strata Satu (S1) Teknik Informatika

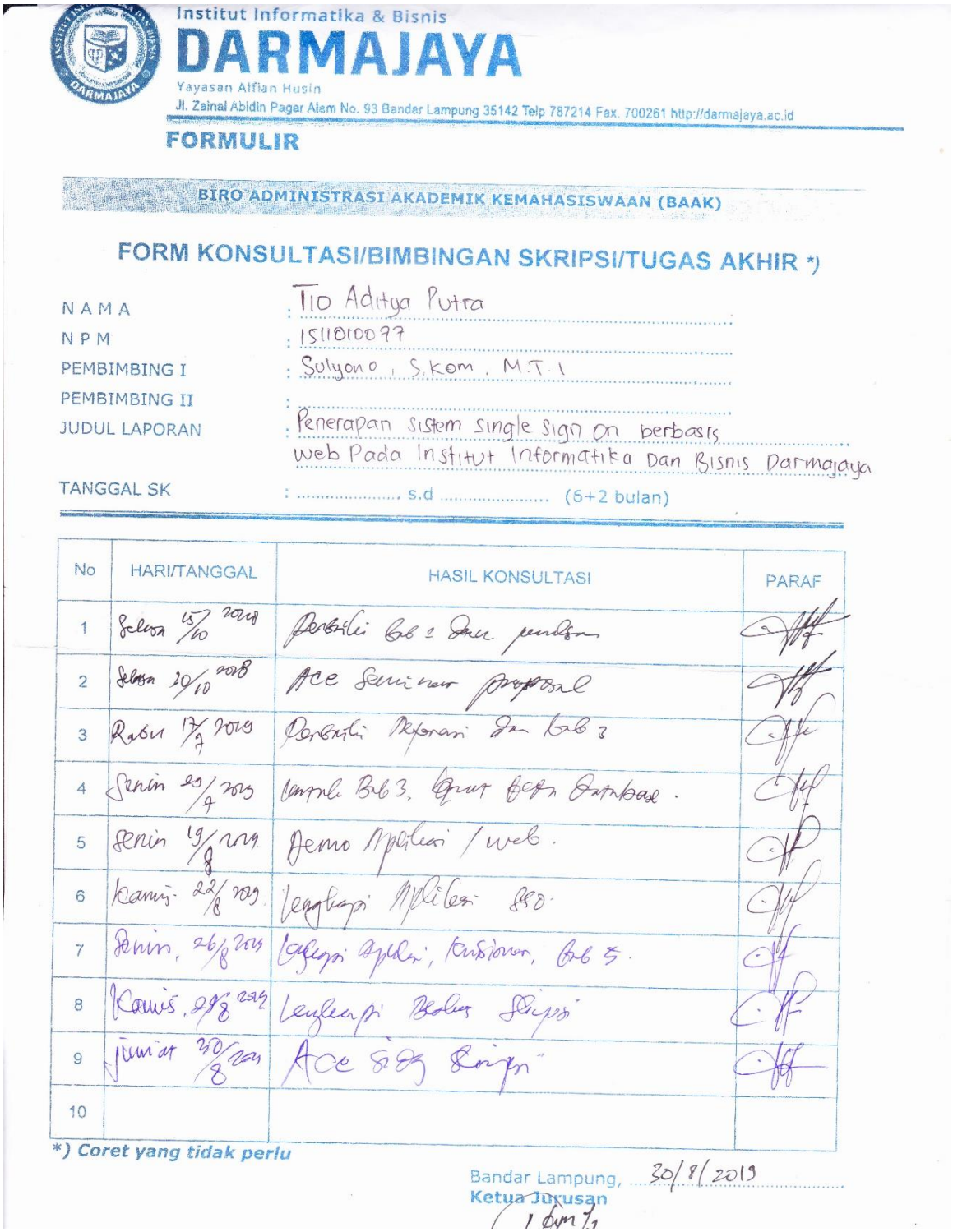
NO.	NAMA	NPM	JUDUL	PEMBIMBING
1	*Komang Dwi Purnomo	1511010056	Perancangan Film Animasi Menggunakan Teknik Stop Motion Sebagai Alternatif Sosiaisasi Tagline Darmajaya The Best	Fitria, S.T, M.Kom
2	*Irhash Ainur Rafiq	1511010068	Virtual Tour Institut Informatika dan Bisnis Darmajaya Berbasis Web	Yuni Arkhiansyah, M.Kom
3	*Tio Aditya Putra	1511010077	Penerapan Sistem Single Sign On Berbasis Web Pada Institut Informatika dan Bisnis Darmajaya	Sulyono, S.Kom, M.T.I

Keterangan : * Surat Keputusan Perpanjangan

A.n. Rektor IIB Darmajaya
Dekan Fakultas Ilmu Komputer

Sriyanto, S.Kom., M.M., Ph.D
NIK. 00210800

Lampiran 2 : Form Konsultasi/Bimbingan Skripsi **.**



Institut Informatika & Bisnis
DARMAJAYA
Yayasan Alfian Husin
Jl. Zainal Abidin Pagar Alam No. 93 Bandar Lampung 35142 Telp 787214 Fax. 700261 http://darmajaya.ac.id

FORMULIR

BIRO ADMINISTRASI AKADEMIK KEMAHASISWAAN (BAAK)

FORM KONSULTASI/BIMBINGAN SKRIPSI/TUGAS AKHIR *)

NAMA : Tio Aditya Putra
NPM : 15110100097
PEMBIMBING I : Sulyono, S.kom, M.T.I
PEMBIMBING II :
JUDUL LAPORAN : Penerapan sistem single sign on berbasis web Pada Institut Informatika Dan Bisnis Darmajaya
TANGGAL SK : ..... s.d ..... (6+2 bulan)

No	HARI/TANGGAL	HASIL KONSULTASI	PARAF
1	Selasa 15/10 2018	Perbaiki Bab 2 dan penulisan	
2	Selasa 29/10 2018	Acc Seminar proposal	
3	Rabu 17/7 2019	Perbaiki laporan dan bab 3	
4	Senin 29/7 2019	Lampir Bab 3. Lanjut Bab 4 dan Lampiran.	
5	Senin 19/8 2019	Demo Aplikasi / web.	
6	Kamis 22/8 2019	Lengkapi Aplikasi SSO.	
7	Senin, 26/8 2019	Lengkapi Aplikasi, Kuisioner, Bab 5.	
8	Kamis, 29/8 2019	Lengkapi Bahan Skripsi	
9	Jumat 30/8 2019	Acc Sidang Skripsi	
10			

*) Coret yang tidak perlu

Bandar Lampung, 30/8/2019
Ketua Jurusan

Lampiran 3 : Surat Persetujuan Sidang.

Institut Informatika & Bisnis
DARMAJAYA
Yayasan Alfian Husin
Jl. Zainal Abidin Pagar Alam No. 93 Bandar Lampung 35142 Telp 787214 Fax. 700281 http://darmajaya.ac.id

FORMULIR

BIRO ADMINISTRASI AKADEMIK KEMAHASISWAAN (BAAK)

SURAT PERSETUJUAN SIDANG SKRIPSI / TUGAS AKHIR

Yang bertanda tangan dibawah ini :

N a m a : Tio Aditya Putra

N P M : 1511010097

Program Studi : Teknik Informatika

Judul Skripsi/Tugas Akhir : Penerapan Sistem Single Sign-On Berbasis Web Pada Institut Informatika dan Bisnis Darmajaya.

Telah menyelesaikan Penulisan Skripsi /Tugas Akhir dan diperkenankan untuk mengajukan persyaratan sidang

Bandar Lampung, 20 / 8 /20

Menyetujui,
Dosen Pembimbing

(Bukhono, S.Kom.M.Ti.)
NIK. 10220304

Mengetahui,
Ketua Program Studi TI

(Zaki Jane)
NIK.

Persyaratan Sidang :

- [V] 1. Surat Persetujuan Sidang
- [V] 2. Surat Bebas Perpustakaan
- [V] 3. Rangkuman Nilai Asli (yang tidak bermasalah)
- [V] 4. Foto Copy Form Bimbingan yang telah disetujui oleh Pembimbing dan ditanda tangani oleh Ketua jurusan
- [V] 5. Kartu Seminar dan Notulen Seminar
- [ ] 6. CD berisi (Program, TA/Skripsi, Materi Sidang dalam bentuk Power Point/Slide)
- [V] 7. Photo copy KRS Semester Terakhir
- [V] 8. Photo copy Ijazah SLTA/ Photo Copy Ijasah D3 (bagi lulusan Diploma)
- [V] 9. Photo copy slip pembayaran sidang (bagi yang mengulang), photo copy slip bayaran TA/Skripsi dan juga fotocopy slip bayaran bagi yang perpanjangan SK
- [ ] 10. Photo Copy Transkrip Nilai dari PTS sebelumnya, Hasil Konversi PTS Baru, KTP, Dan Kartu Keluarga (Bagi mahasiswa konversi)
- [V] 11. Photo copy SK Pembimbing Penulisan Tugas Akhir/Skripsi dan SK Perpanjang *)
- [ ] 12. Photo copy Penulisan Tugas Akhir/ skripsi (softcover, 3 eks)
- [V] 13. Photo copy Sertifikasi Internasional (HTML5 / MOS /FORESEC /DBFA / ACA)
- [V] 14. Fotocopy Sertifikat Toefl/Surat Keterangan sudah lulus Kursus Bhs. Inggris
- [V] 15. Photo Hitam putih ukuran 3 x 4 (4lbr), kebaya(perempuan) atau Jas (Laki-laki) untuk Ijazah &Transkrip Nilai (kertas Doff bukan Printing)
- [ ] 16. Semua berkas dimasukan ke dalam stofmap **"DIAMOND 5002 atau Map Biola"** warna biru (Ilmu Komputer)
  Stofmap **"DIAMOND 5002 atau Map Biola "**warna kuning (Bisnis & Ekonomi)

Lampiran 4 : Surat Balasan Penelitian.

DARMAJAYA

Bandar Lampung, 25 Juni 2019

No : EM.0273/DMJ/WRI/VI-2019

Kepada Yth,
Dekan Fakultas Ilmu Komputer
IIB Darmajaya
di -
Tempat

Hal : Jawaban Ijin Penelitian

Dengan hormat,

Teriring salam dan doa semoga kita selalu dalam lindungan Tuhan Yang Maha Kuasa, sehingga kita dapat melaksanakan aktifitas sehari-hari dengan baik dan dapat meningkatkan kinerja demi kemajuan pendidikan di Indonesia.

Menindaklanjuti surat yang kami terima nomor :Penelitian.007/DMJ/DEKAN/BAAK/V-19 perihal Izin Penelitian, maka bersama dengan ini kami sampaikan bahwa mahasiswa atas nama :

Nama	: Tio Aditya Putra
NPM	: 1511010077
Jurusan	: S1 Teknik Informatika

Dapat melakukan penelitiannya di Institut Informatika dan Bisnis (IIB) Darmajaya pada Bagian ICT sesuai dengan waktu pelaksanaan dan judul karya ilmiah yang diajukan.

Demikian surat ini kami sampaikan. Atas perhatian dan kerjasamanya, kami ucapkan terima kasih.

Salam hormat,

an.Rektor IIB Darmajaya

Dr. RZ Abdul Aziz, MT
Wakil Rektor I
Bidang Akademik dan Riset

Tembusan :
1. Arsip