LAPORAN INDIVIDU KUKERTA

SOSIALISASI IMPLEMENTASI PROTOTYPE KEAMANAN *TWO-FACTOR AUTHENTICATION (2FA)* PADA SISTEM INFORMASI AKADEMIK (STUDI KASUS: UIN SULTAN MAULANA HASANUDDIN BANTEN)

Disusun untuk memenuhi laporan kegiatan KUKERTA

pada Program Studi Informatika

Disusun oleh:

Nama : Bayu Endru Subiyakto

NIM : 231730029

PROGRAM STUDI INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI

SULTAN MAULANA HASANUDDIN BANTEN

2026

HALAMAN PENGESAHAN

Laporan individu KUKERTA ini telah disusun oleh:

Nama	:	Bayu Endru Subiyakto
NIM	:	231730029
Program Studi	:	Informatika
Fakultas	:	Sains dan Teknologi
Judul Kegiatan	:	Sosialisasi Implementasi Prototype Keamanan *Two-Factor Authentication (2FA)* Pada Sistem Informasi Akademik (Studi kasus: UIN Sultan Maulana Hasanuddin Banten)
Tempat Kegiatan	:	Meet Online (Google Meet)
Waktu Kegiatan	:	Sabtu, 20 Juni 2026

Laporan ini telah diperiksa dan disahkan sebagai laporan pelaksanaan kegiatan KUKERTA pada Program Studi Informatika.

Tangerang, 25 Juni 2026

Dosen Pembimbing,

Ahmad Tabrani, M.T.I
NIP. 198509172018011002

Mahasiswa,

Bayu Endru Subiyakto
NIM. 231730029

Mengetahui,

Ketua Program Studi Informatika

Ahmad Tabrani, M.T.I
NIP. 198509172018011002

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Allah SWT karena atas rahmat dan karunia-Nya, penulis dapat menyelesaikan laporan individu KUKERTA yang berjudul "Sosialisasi Implementasi Prototype Keamanan *Two-Factor Authentication (2FA)* Pada Sistem Informasi Akademik (Studi kasus: UIN Sultan Maulana Hasanuddin Banten)" dengan baik. Laporan ini disusun sebagai bentuk pertanggungjawaban atas pelaksanaan kegiatan KUKERTA yang dilakukan melalui sosialisasi prototipe antarmuka keamanan SIAKAD berbasis prinsip *Human-Computer Interaction* kepada mahasiswa Program Studi Informatika UIN Sultan Maulana Hasanuddin Banten. Kegiatan ini diharapkan dapat membantu peserta memahami manfaat, alur penggunaan, serta penerapan prototipe keamanan SIAKAD yang telah dikembangkan sesuai kebutuhan pengguna.

Penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan bantuan, arahan, dan dukungan selama kegiatan berlangsung hingga penyusunan laporan ini, terutama kepada:

1. Ahmad Tabrani, M.T.I selaku Dosen Pembimbing KUKERTA yang telah memberikan bimbingan dan arahan selama pelaksanaan kegiatan.
2. Christine Cecylia Munthe, S.Kom., M.T.I selaku Pembimbing Lapangan di BRIN yang telah memberikan bimbingan teknis selama pengembangan prototipe berlangsung.
3. Mahasiswa Program Studi Informatika UIN SMH Banten selaku peserta sosialisasi yang telah berpartisipasi aktif dalam kegiatan.
4. Semua pihak yang telah membantu pelaksanaan kegiatan KUKERTA yang tidak dapat disebutkan satu per satu.

Penulis menyadari bahwa laporan ini masih memiliki kekurangan. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan agar laporan ini dapat menjadi lebih baik. Semoga laporan ini dapat memberikan manfaat bagi pembaca dan pihak-pihak yang membutuhkan.

Tangerang, 25 Juni 2026

Bayu Endru Subiyakto

DAFTAR ISI

BAB I
PENDAHULUAN

1.1 Latar Belakang

Kuliah Kerja Nyata (KUKERTA) merupakan salah satu kegiatan akademik yang bertujuan untuk memberikan pengalaman kepada mahasiswa dalam menerapkan pengetahuan dan keterampilan yang dimiliki melalui kegiatan yang bermanfaat bagi lingkungan sekitar. Dalam pelaksanaannya, kegiatan KUKERTA dapat dilakukan melalui kegiatan sosialisasi, pendampingan, edukasi, maupun pengenalan suatu program kepada sasaran tertentu.

Pada Program Studi Informatika, kegiatan KUKERTA diarahkan pada penerapan teknologi informasi yang sesuai dengan kebutuhan pengguna. Kegiatan yang dilaksanakan dalam laporan ini adalah sosialisasi prototipe antarmuka keamanan Sistem Informasi Akademik (SIAKAD) UIN Sultan Maulana Hasanuddin Banten kepada mahasiswa Program Studi Informatika. Prototipe ini dikembangkan selama kegiatan magang di Badan Riset dan Inovasi Nasional (BRIN), KST B.J. Habibie Serpong, pada Kelompok Riset *Human-Computer Interaction and Visualization (KR HCI V).*

SIAKAD UIN SMH Banten saat ini masih menggunakan mekanisme autentikasi yang sederhana, yaitu hanya mengandalkan NIM, PIN pendek, dan captcha statis tanpa adanya lapisan verifikasi tambahan seperti *Multi-Factor Authentication (MFA)* atau *One-Time Password (OTP).* Kondisi ini menunjukkan adanya celah antara kebutuhan keamanan data akademik yang semakin penting dan mekanisme autentikasi yang ada, yang berpotensi rentan terhadap ancaman keamanan.

Sebagai luaran dari kegiatan magang tersebut, penulis telah berhasil merancang prototipe antarmuka keamanan SIAKAD menggunakan Figma dengan menerapkan prinsip *Human-Computer Interaction* (*HCI*). Prototipe ini mencakup empat lapisan keamanan utama, yaitu halaman login dengan Kode Akses/PIN dan captcha, verifikasi dua langkah melalui *OTP* email maupun *Google Authenticator*, manajemen sesi aktif dengan auto timeout, serta dashboard audit log aktivitas pengguna.

Berdasarkan hal tersebut, laporan ini disusun untuk mendeskripsikan pelaksanaan kegiatan sosialisasi prototipe antarmuka keamanan SIAKAD kepada mahasiswa Program Studi Informatika UIN SMH Banten. Kegiatan ini dilaksanakan agar peserta dapat memahami fungsi, manfaat, serta cara penggunaan prototipe yang telah dikembangkan, sehingga dapat digunakan sebagai referensi pengembangan sistem keamanan SIAKAD yang lebih baik di masa mendatang.

1.2 Rumusan Masalah

Rumusan masalah dalam laporan ini adalah sebagai berikut:

- Bagaimana pelaksanaan kegiatan sosialisasi prototipe antarmuka keamanan SIAKAD kepada mahasiswa Program Studi Informatika UIN SMH Banten?
- Apa saja materi yang disampaikan dalam kegiatan sosialisasi tersebut?
- Bagaimana hasil dan dokumentasi dari pelaksanaan kegiatan sosialisasi?

1.3 Tujuan Kegiatan

Tujuan dari kegiatan ini adalah sebagai berikut:

- Menjelaskan pelaksanaan kegiatan sosialisasi prototipe antarmuka keamanan SIAKAD kepada mahasiswa Program Studi Informatika UIN SMH Banten.
- Memberikan pemahaman kepada peserta mengenai manfaat, prinsip *HCI* yang diterapkan, dan cara penggunaan prototipe keamanan SIAKAD yang disosialisasikan.
- Mendokumentasikan hasil pelaksanaan kegiatan sosialisasi sebagai bentuk laporan kegiatan KUKERTA.

1.4 Manfaat Kegiatan

Kegiatan ini diharapkan dapat memberikan manfaat bagi berbagai pihak sebagai berikut:

Bagi Mahasiswa (Penulis)

Kegiatan ini menjadi sarana untuk melatih kemampuan komunikasi, penyampaian materi, dan penerapan hasil prototipe keamanan SIAKAD kepada pengguna secara langsung. Penulis juga dapat mengasah kemampuan menyampaikan konsep teknis seperti *HCI* dan keamanan sistem kepada audiens yang beragam.

Bagi Peserta Sosialisasi

Kegiatan ini dapat membantu mahasiswa memahami kondisi keamanan SIAKAD yang ada saat ini, serta mengenal konsep dan rancangan solusi berbasis prinsip *Human-Computer Interaction* yang dapat diimplementasikan untuk meningkatkan keamanan sistem tersebut.

Bagi Program Studi Informatika

Kegiatan ini dapat menjadi dokumentasi kegiatan mahasiswa dalam menerapkan ilmu teknologi informasi, khususnya di bidang keamanan sistem dan desain antarmuka, secara langsung kepada masyarakat akademik.

BAB II
GAMBARAN UMUM KEGIATAN DAN SASARAN

2.1 Gambaran Umum Prototipe Keamanan SIAKAD

Prototipe yang disosialisasikan dalam kegiatan ini adalah rancangan antarmuka keamanan Sistem Informasi Akademik (SIAKAD) UIN Sultan Maulana Hasanuddin Banten yang dikembangkan menggunakan aplikasi Figma selama kegiatan magang di BRIN KST B.J. Habibie Serpong. Prototipe ini dirancang untuk menjawab permasalahan mekanisme keamanan SIAKAD yang masih sederhana dengan menerapkan prinsip *Human-Computer Interaction* (*HCI*) pada setiap lapisan keamanannya.

Prototipe ini terdiri dari empat lapisan keamanan utama, yaitu:

a. Halaman Login

Halaman login dirancang dengan tampilan split-layout yang memuat form login dengan NIM/Username dan Kode Akses/PIN , dilengkapi fitur "Ingat sesi login ini" dan opsi login menggunakan *Google Authenticator*. Halaman ini menerapkan prinsip *visibility of system* status dengan menampilkan informasi sistem secara jelas kepada pengguna.

b. Verifikasi Dua Langkah (2FA)

Setelah login berhasil, pengguna akan melalui proses verifikasi dua langkah yang dapat dilakukan melalui dua metode: Email *OTP* berupa kode enam digit yang dikirimkan ke alamat email terdaftar mahasiswa, atau *Google Authenticator* yang menghasilkan kode *TOTP (Time-based One-Time Password)* yang berubah setiap 30 detik. Fitur ini menerapkan prinsip error prevention and recovery.

c. Deteksi Perangkat Baru

Sistem akan mendeteksi apabila pengguna melakukan login dari perangkat yang berbeda dari biasanya dan menampilkan notifikasi verifikasi perangkat baru, termasuk informasi browser, sistem operasi, lokasi*, IP address*, dan waktu login. Pengguna dapat memilih durasi kepercayaan perangkat (1 jam atau 24 jam) atau menolak akses.

d. Dashboard Keamanan dan Riwayat Login

Pengguna dapat mengakses halaman Keamanan yang menampilkan riwayat login dari berbagai perangkat beserta status masing-masing sesi, daftar sesi aktif yang dapat diakhiri, status autentikasi *MFA,* dan daftar perangkat terpercaya. Fitur ini menerapkan prinsip *user control and freedom.*

e. Audit Log

Dashboard *Audit Log* menampilkan catatan keamanan yang lengkap, meliputi total aktivitas, jumlah login berhasil, login gagal, dan logout. Setiap entri memuat informasi waktu, jenis aktivitas, perangkat, browser, *IP address*, lokasi, dan status.

f. Halaman Logout

Halaman logout dirancang untuk memberikan konfirmasi yang jelas kepada pengguna bahwa sesi telah diakhiri dengan aman, termasuk informasi bahwa semua sesi aktif telah diakhiri, data tersimpan dengan aman, token autentikasi telah dihapus, dan cookies sesi telah dihapus.

2.2 Kebutuhan Pengguna

Berdasarkan observasi dan kajian literatur yang dilakukan selama kegiatan magang, terdapat beberapa kebutuhan pengguna yang menjadi alasan pentingnya kegiatan sosialisasi ini:

- Mahasiswa sebagai pengguna utama SIAKAD memerlukan pemahaman mengenai kondisi keamanan sistem informasi akademik yang mereka gunakan sehari-hari, termasuk potensi risiko yang ada.
- Pengguna membutuhkan informasi mengenai pentingnya mekanisme autentikasi berlapis seperti *MFA dan OTP* dalam melindungi data akademik pribadi mereka dari ancaman keamanan.
- Mahasiswa perlu mengetahui bagaimana desain antarmuka keamanan yang mempertimbangkan prinsip *HCI* dapat membuat mekanisme keamanan

menjadi lebih mudah dan nyaman digunakan tanpa mengorbankan tingkat keamanan.

- Peserta sosialisasi membutuhkan gambaran konkret melalui demonstrasi prototipe mengenai bagaimana antarmuka keamanan SIAKAD yang ideal dapat dirancang, sebagai masukan bagi pengembangan sistem ke depan.

2.3 Sasaran Kegiatan

Sasaran kegiatan sosialisasi ini adalah mahasiswa Program Studi Informatika UIN Sultan Maulana Hasanuddin Banten yang menggunakan SIAKAD sebagai sistem informasi akademik utama mereka.

Tabel 1. Sasaran Kegiatan Sosialisasi

No	Sasaran	Keterangan
1	Mahasiswa Prodi Informatika	Pengguna aktif SIAKAD UIN SMH Banten yang menjadi sasaran utama sosialisasi
2	Mahasiswa Semester 4–6	Mahasiswa yang telah berpengalaman menggunakan SIAKAD dan memahami konteks permasalahan
3	Dosen Pembimbing	Dosen pembimbing KUKERTA yang turut menyaksikan dan menilai pelaksanaan kegiatan

Sumber: Data diolah oleh penulis, 2026

BAB III
METODE PELAKSANAAN KEGIATAN

3.1 Waktu dan Tempat Pelaksanaan

Kegiatan sosialisasi dilaksanakan pada Sabtu, 20 Juni 2026, bertempat di platform Google Meet secara daring (online). Kegiatan ini dilakukan secara daring dengan sasaran peserta mahasiswa Program Studi Informatika UIN Sultan Maulana Hasanuddin Banten.

3.2 Peserta Kegiatan

Peserta kegiatan adalah mahasiswa Program Studi Informatika UIN Sultan Maulana Hasanuddin Banten. Peserta dipilih karena memiliki keterkaitan langsung dengan penggunaan SIAKAD sebagai sistem informasi akademik yang mereka gunakan sehari-hari, serta memiliki latar belakang keilmuan yang relevan di bidang teknologi informasi.

3.3 Bentuk Kegiatan

Bentuk kegiatan yang dilaksanakan adalah sosialisasi dan demonstrasi penggunaan prototipe antarmuka keamanan SIAKAD. Kegiatan dilakukan melalui penyampaian materi, demonstrasi prototipe secara langsung menggunakan Figma, penjelasan fitur-fitur keamanan, sesi tanya jawab, dan dokumentasi kegiatan.

3.4 Materi Sosialisasi

Materi yang disampaikan dalam kegiatan sosialisasi meliputi:

- Kondisi keamanan SIAKAD UIN SMH Banten saat ini: penggunaan NIM, Kode Akses/PIN , dan captcha statis tanpa lapisan verifikasi tambahan.
- Pengenalan prinsip *Human-Computer Interaction* (*HCI*) yang diterapkan dalam desain keamanan, khususnya visibility of system status, *erro*r *prevention and recovery, dan user control and freedom.*
- Pengenalan konsep usable security: integrasi keamanan yang kuat dengan kenyamanan pengguna.

- Demonstrasi prototipe antarmuka keamanan SIAKAD: alur login, verifikasi *OTP* melalui email, verifikasi menggunakan Google Authenticator, deteksi perangkat baru, dashboard keamanan, *audit log,* dan halaman logout.
- Pembahasan manfaat penerapan *Multi-Factor Authentication (MFA)* dan *activity log* dalam melindungi data akademik mahasiswa.
- Sesi tanya jawab dan diskusi mengenai pengembangan keamanan SIAKAD ke depan.

3.5 Tahapan Pelaksanaan

Tahapan pelaksanaan kegiatan terdiri dari:

- Persiapan kegiatan, meliputi penyusunan materi presentasi, pengecekan prototipe di Figma, memastikan akses Google Meet berfungsi, dan persiapan dokumentasi.
- Pelaksanaan kegiatan, meliputi pembukaan dan perkenalan, penyampaian materi sosialisasi, demonstrasi prototipe secara langsung, dan sesi tanya jawab.
- Evaluasi singkat, meliputi pencatatan masukan dari peserta, kendala yang ditemui, dan tanggapan peserta terhadap prototipe.
- Dokumentasi kegiatan, meliputi pengambilan tangkapan layar selama kegiatan berlangsung dan penyusunan lampiran laporan.

Tabel 2. Jadwal Kegiatan Sosialisasi

No	Waktu	Kegiatan	Keterangan
1	Sabtu, 20 Juni 2026 (10.00–10.10 WIB)	Pembukaan dan perkenalan	Moderator membuka acara, penulis memperkenalkan diri dan tujuan kegiatan
2	Sabtu, 20 Juni 2026 (10.10–10.45 WIB)	Penyampaian materi sosialisasi	Penulis menjelaskan kondisi keamanan SIAKAD, prinsip ***HCI*** , dan konsep usable security
3	Sabtu, 20 Juni 2026 (10.45–11.15 WIB)	Demonstrasi prototipe	Penulis mendemonstrasikan seluruh fitur prototipe

No	Waktu	Kegiatan	Keterangan
			keamanan SIAKAD di Figma secara langsung
4	Sabtu, 20 Juni 2026 (11.15–11.45 WIB)	Tanya jawab dan diskusi	Peserta mengajukan pertanyaan dan berdiskusi mengenai prototipe yang telah ditampilkan
5	Sabtu, 20 Juni 2026 (11.45–12.00 WIB)	Penutup dan dokumentasi	Kegiatan ditutup oleh moderator dan dilanjutkan dengan dokumentasi bersama

Sumber: Data diolah oleh penulis, 2026

BAB IV
HASIL DAN DOKUMENTASI KEGIATAN

4.1 Deskripsi Pelaksanaan Sosialisasi

Kegiatan sosialisasi prototipe antarmuka keamanan SIAKAD dilaksanakan pada Sabtu, 20 Juni 2026 melalui platform Google Meet secara daring. Kegiatan dihadiri oleh mahasiswa Program Studi Informatika UIN Sultan Maulana Hasanuddin Banten.

Kegiatan sosialisasi diawali dengan pembukaan dan pengenalan tujuan kegiatan oleh moderator. Setelah itu, penulis menyampaikan materi mengenai kondisi keamanan SIAKAD UIN SMH Banten saat ini, termasuk identifikasi celah keamanan pada mekanisme autentikasi yang masih sederhana. Penulis kemudian menjelaskan prinsip-prinsip *Human-Computer Interaction* yang diterapkan dalam desain prototipe, khususnya *visibility of system status*, *error prevention and recovery*, dan *user control and freedom*, serta konsep *usable security* yang menjadi landasan pengembangan.

Bagian inti kegiatan adalah demonstrasi langsung prototipe keamanan SIAKAD melalui Figma. Penulis memperagakan seluruh alur penggunaan, mulai dari halaman login, proses verifikasi dua langkah (*OTP* email dan *Google Authenticator*), deteksi perangkat baru, dashboard keamanan dan riwayat login, audit log aktivitas, hingga halaman logout yang aman. Peserta sangat antusias dan aktif mengajukan pertanyaan selama sesi demonstrasi berlangsung.

Kegiatan dilanjutkan dengan sesi tanya jawab dan diskusi yang cukup interaktif. Beberapa peserta mengajukan pertanyaan mengenai kemungkinan implementasi prototipe pada SIAKAD yang sebenarnya, perbedaan antara Email *OTP* dan *Google Authenticator* dari sisi kemudahan penggunaan, serta manfaat audit log bagi keamanan akun mahasiswa. Kegiatan ditutup dengan dokumentasi bersama dan ucapan terima kasih kepada seluruh peserta.

4.2 Hasil Kegiatan

Hasil yang diperoleh dari kegiatan sosialisasi ini adalah sebagai berikut:

Tabel 3. Hasil Pelaksanaan Kegiatan

No	Aspek	Hasil/Keterangan
1	Pemahaman peserta	Peserta memahami kondisi keamanan SIAKAD saat ini dan prinsip *HCI* yang diterapkan dalam prototipe yang disosialisasikan
2	Tanggapan peserta	Peserta merespons positif dan antusias terhadap demonstrasi prototipe, terutama pada fitur verifikasi dua langkah dan audit log
3	Pertanyaan peserta	Peserta aktif mengajukan pertanyaan mengenai implementasi teknis dan perbandingan metode autentikasi yang ditampilkan
4	Masukan peserta	Peserta memberikan masukan agar prototipe dapat dilengkapi dengan fitur notifikasi push ke aplikasi mobile untuk meningkatkan aksesibilitas verifikasi
5	Dokumentasi	Kegiatan terdokumentasi dalam bentuk tangkapan layar kegiatan sosialisasi via Google Meet

Sumber: Data diolah oleh penulis, 2026

4.3 Kendala dan Solusi

Selama pelaksanaan kegiatan sosialisasi, terdapat beberapa kendala yang ditemui beserta solusi yang diterapkan:

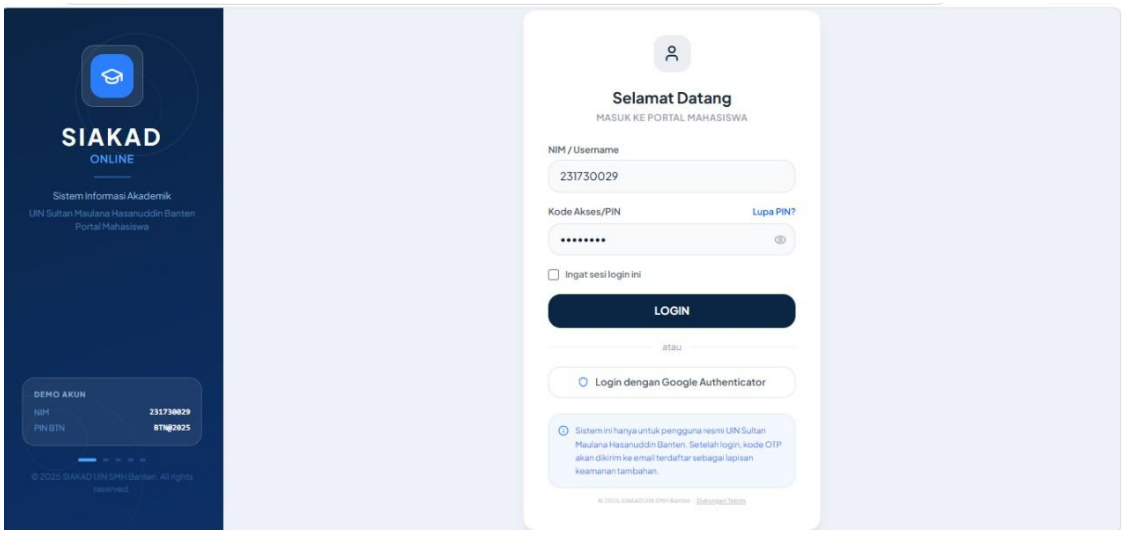
- Kendala: Koneksi internet beberapa peserta yang tidak stabil sehingga menyebabkan gangguan pada kualitas audio dan video selama kegiatan berlangsung. Solusi: Penulis mengulangi penjelasan pada bagian yang terganggu dan menyediakan rekaman layar demonstrasi prototipe yang dapat diakses kembali oleh peserta setelah kegiatan selesai.
- Kendala: Beberapa peserta belum familiar dengan konsep *HCI* dan usable security, sehingga memerlukan penjelasan tambahan sebelum masuk ke

demonstrasi prototipe. Solusi: Penulis menyesuaikan penyampaian materi dengan menggunakan analogi dan contoh sehari-hari yang mudah dipahami oleh peserta.

- Kendala: Waktu yang tersedia terbatas sehingga tidak semua pertanyaan peserta dapat dijawab secara mendalam selama sesi tanya jawab. Solusi: Penulis menyediakan sesi tindak lanjut melalui grup diskusi untuk menjawab pertanyaan yang belum sempat terjawab.

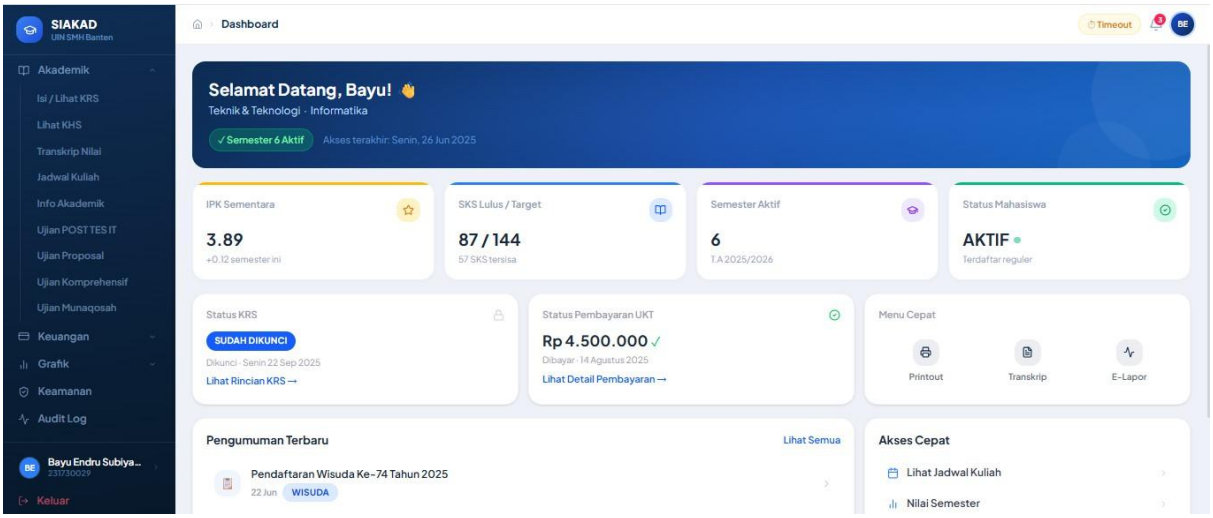
4.4 Dokumentasi Kegiatan

Berikut adalah dokumentasi prototipe antarmuka keamanan SIAKAD yang ditampilkan selama kegiatan sosialisasi:



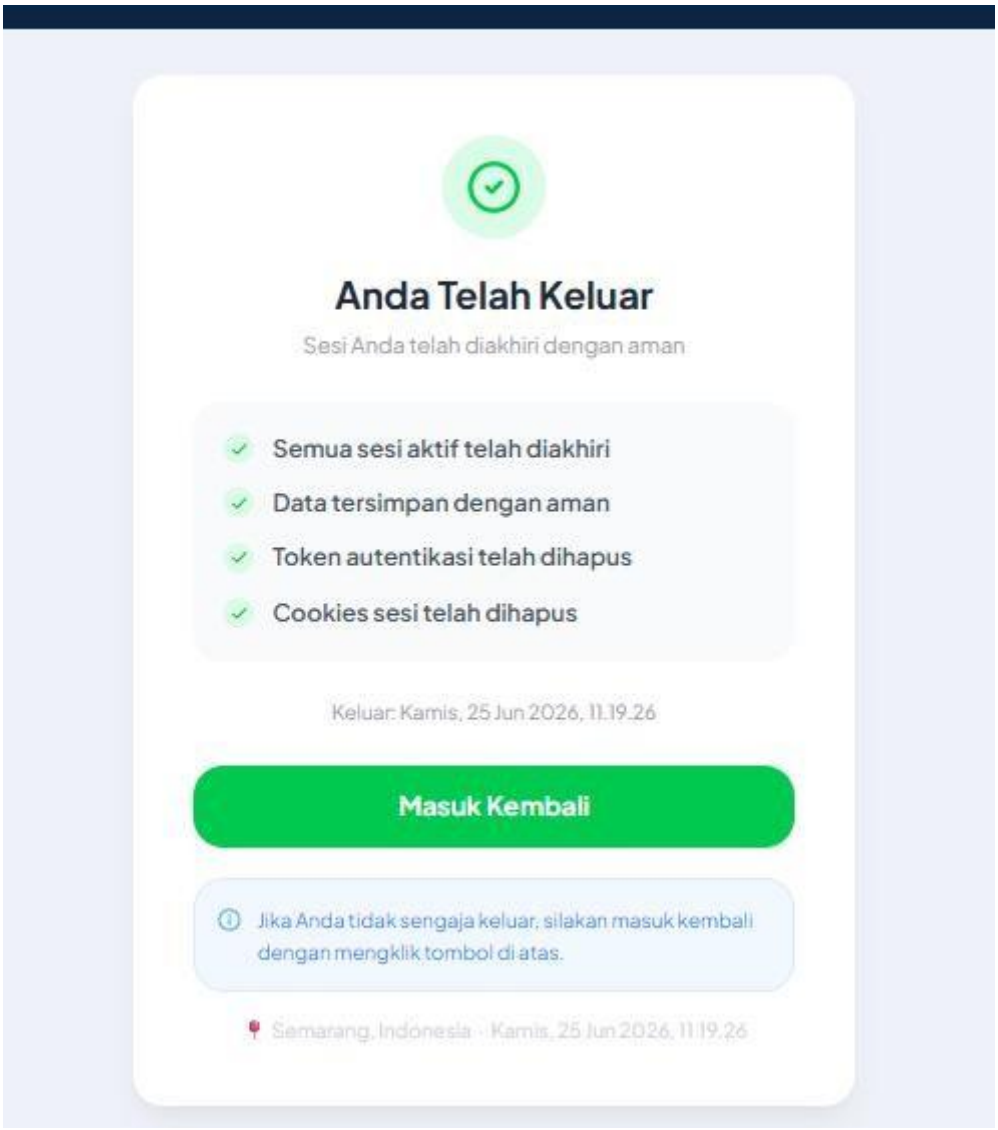
Gambar 1. Halaman Login SIAKAD dengan Kode Akses/PIN dan Opsi Google Authenticator

Sumber: Dokumentasi Penulis, 2026



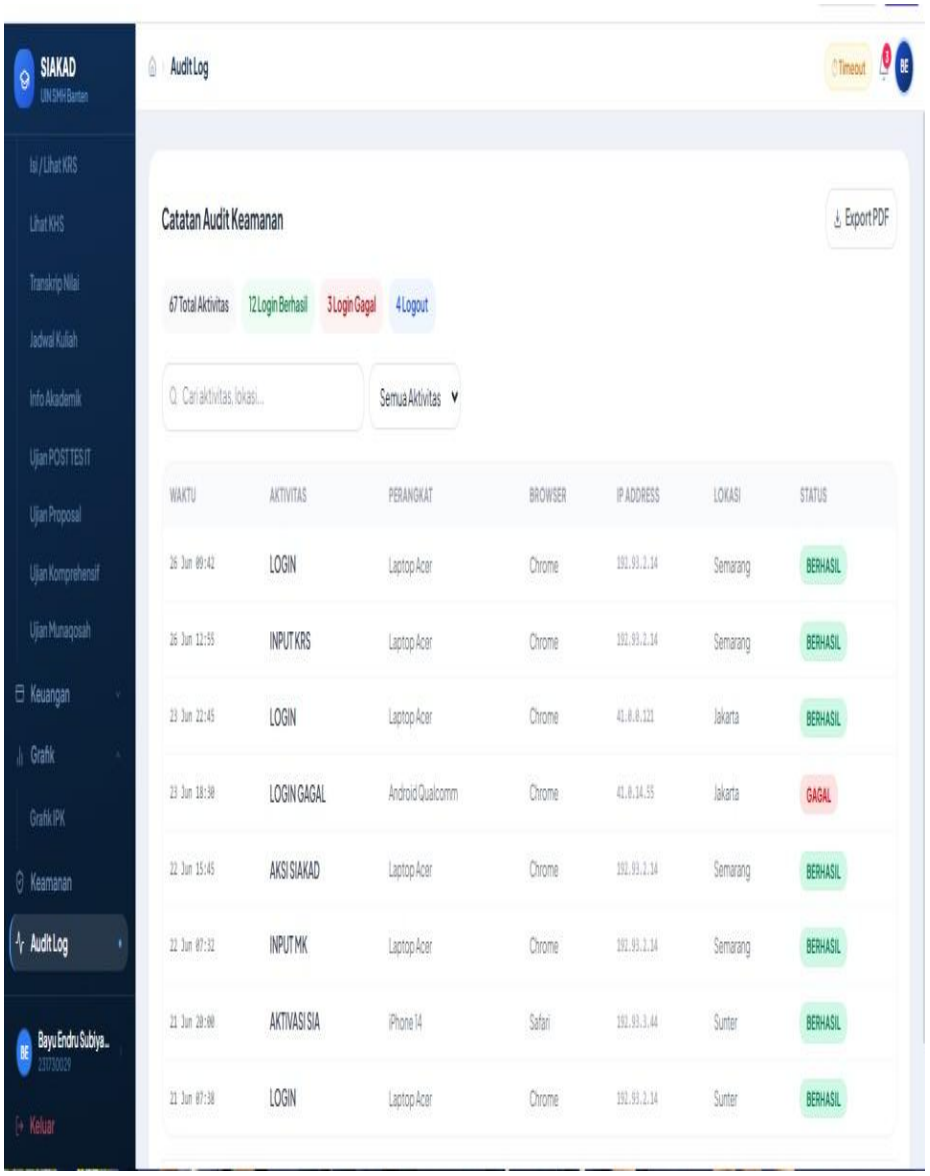
Gambar 2. Dashboard Utama SIAKAD Setelah Login Berhasil

Sumber: Dokumentasi Penulis, 2026



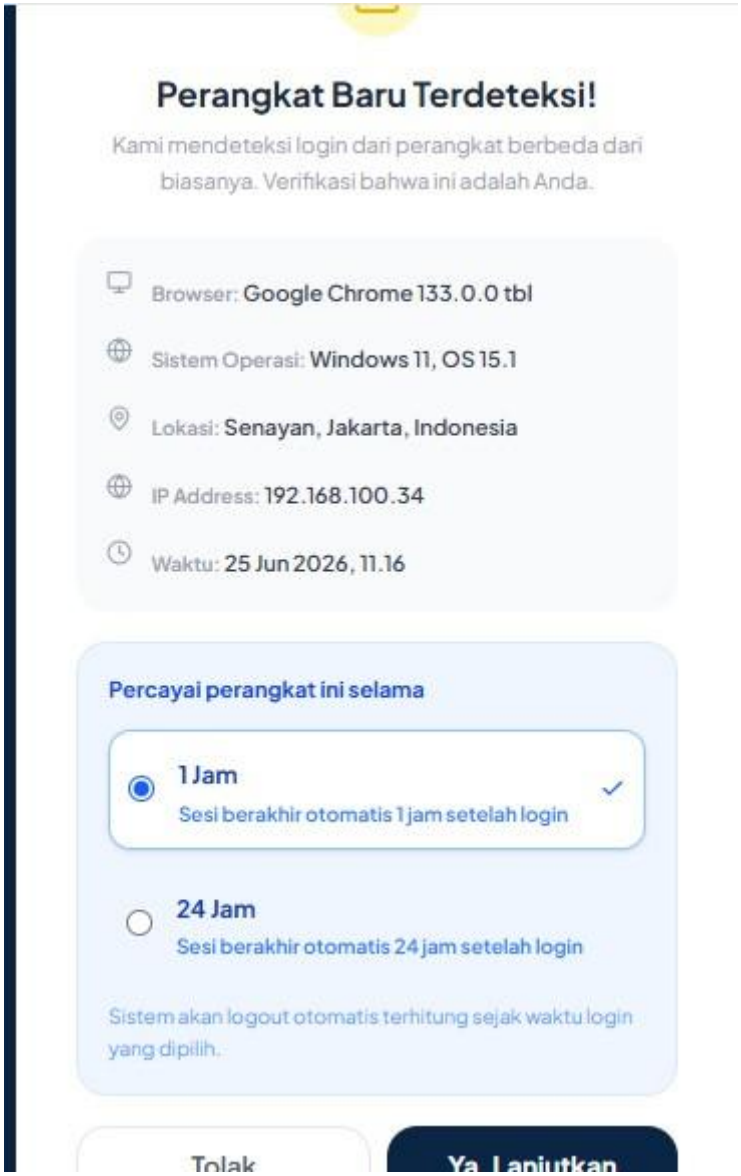
Gambar 3. Verifikasi Dua Langkah — Email OTP

Sumber: Dokumentasi Penulis, 2026



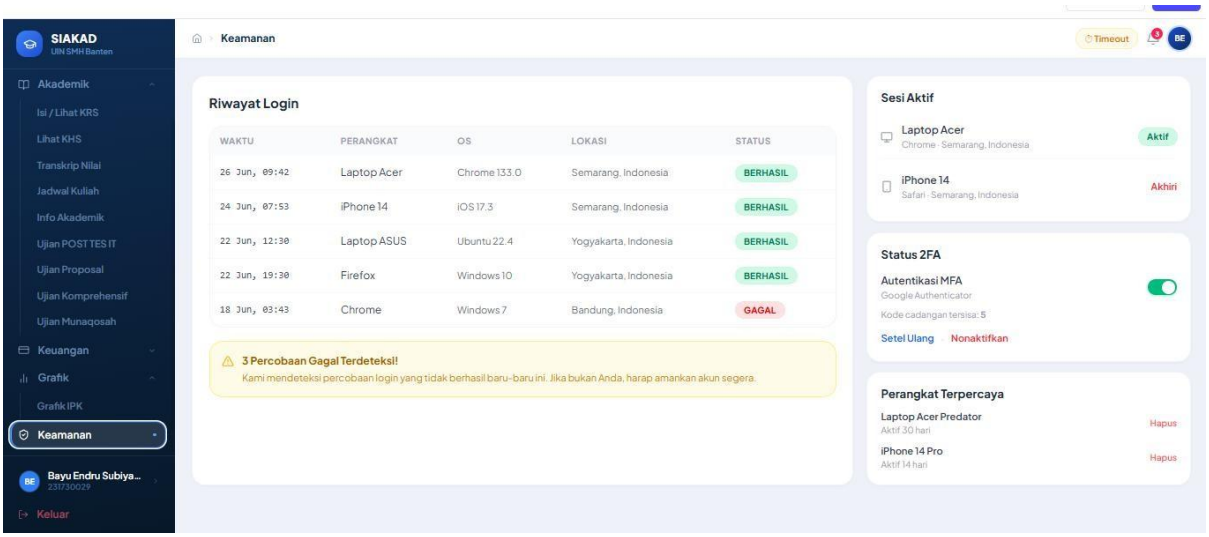
Gambar 4. Verifikasi Dua Langkah — Google Authenticator

Sumber: Dokumentasi Penulis, 2026



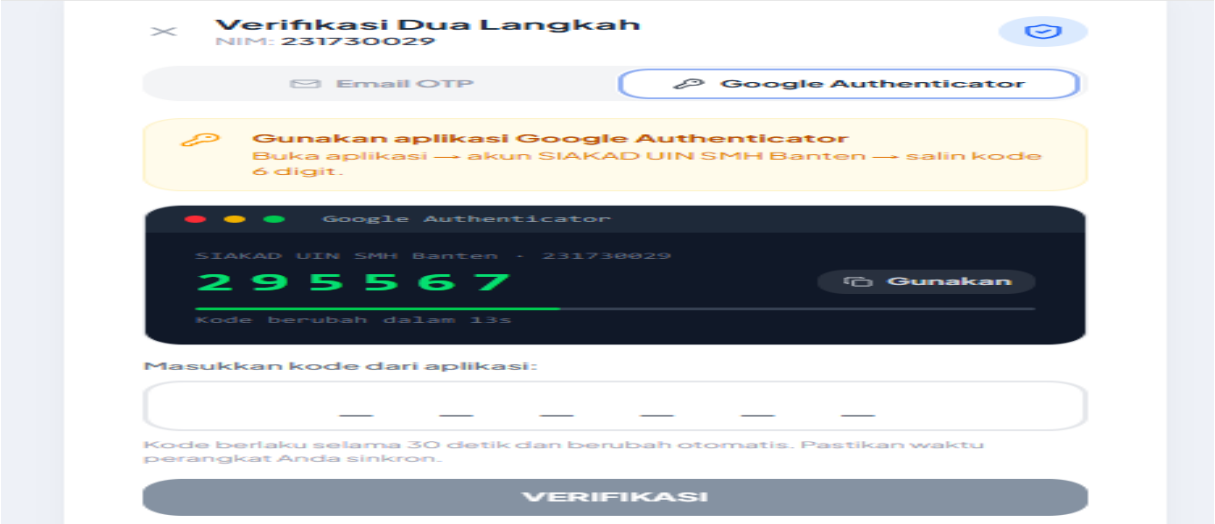
Gambar 5. Deteksi Perangkat Baru dan Pilihan Durasi Kepercayaan Perangkat

Sumber: Dokumentasi Penulis, 2026



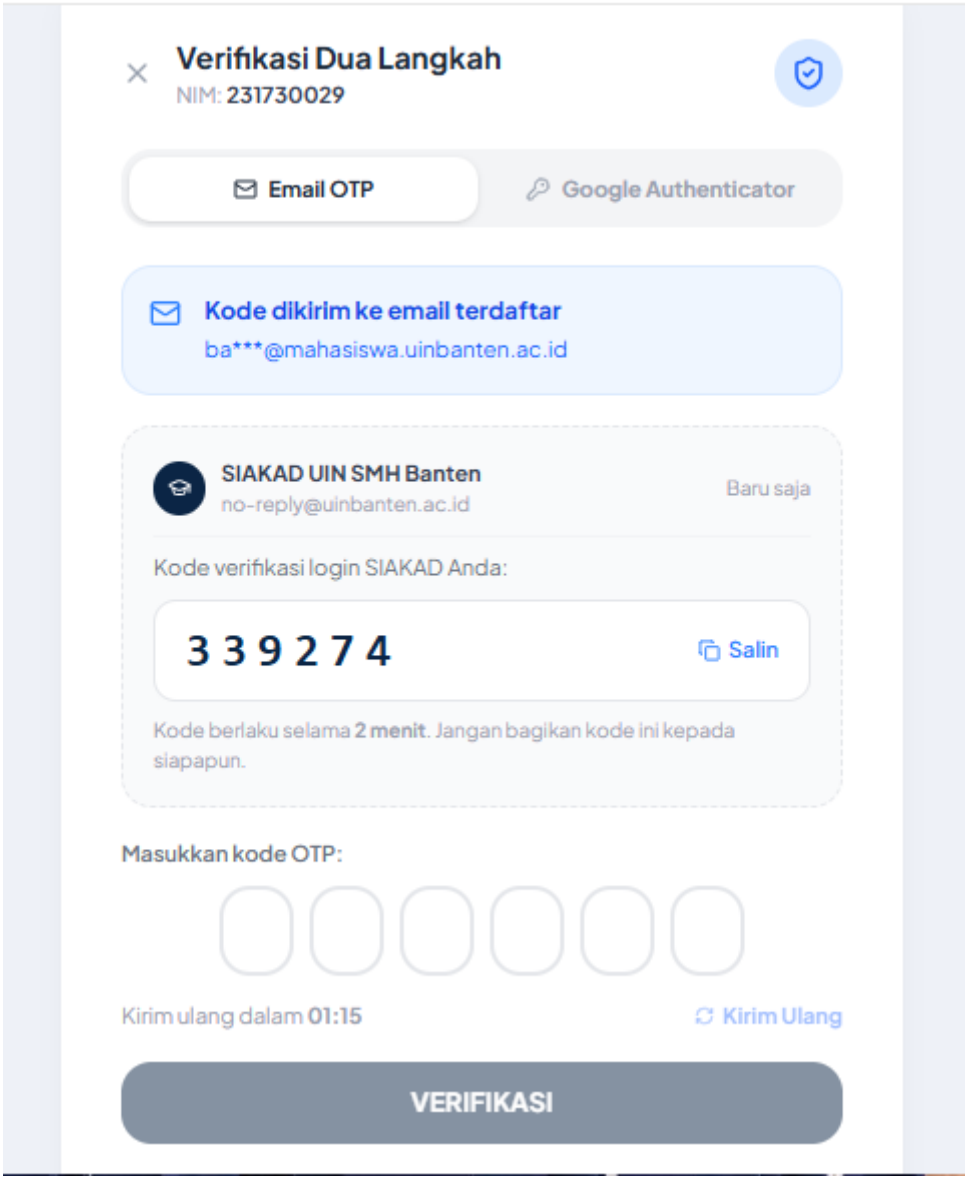
Gambar 6. Halaman Keamanan: Riwayat Login, Sesi Aktif, Status 2FA, dan Perangkat Terpercaya

Sumber: Dokumentasi Penulis, 2026



Gambar 7. Dashboard Audit Log Keamanan SIAKAD

Sumber: Dokumentasi Penulis, 2026



Gambar 8. Halaman Konfirmasi Logout yang Aman

Sumber: Dokumentasi Penulis, 2026

BAB V
PENUTUP

5.1 Kesimpulan

Berdasarkan pelaksanaan kegiatan sosialisasi prototipe antarmuka keamanan SIAKAD, dapat disimpulkan bahwa kegiatan berjalan dengan baik dan sesuai dengan tujuan yang telah direncanakan. Kegiatan dilaksanakan secara daring melalui Google Meet pada Sabtu, 20 Juni 2026, dengan peserta mahasiswa Program Studi Informatika UIN Sultan Maulana Hasanuddin Banten.

Peserta memperoleh penjelasan mengenai kondisi keamanan SIAKAD UIN SMH Banten saat ini beserta celah keamanan yang ada, prinsip *Human-Computer Interaction* yang diterapkan dalam perancangan keamanan sistem informasi, serta demonstrasi langsung prototipe antarmuka keamanan SIAKAD yang mencakup halaman login, verifikasi dua langkah (Email *OTP* dan *Google Authenticator*), deteksi perangkat baru, dashboard keamanan dan riwayat login, audit log aktivitas pengguna, dan halaman logout yang aman.

Respons peserta sangat positif, ditandai dengan antusiasme dalam mengikuti demonstrasi dan aktifnya sesi tanya jawab. Dokumentasi kegiatan juga telah disusun sebagai bukti pelaksanaan kegiatan KUKERTA. Kegiatan sosialisasi ini diharapkan dapat memberikan kontribusi berupa peningkatan kesadaran mahasiswa terhadap pentingnya keamanan sistem informasi akademik yang mempertimbangkan kenyamanan pengguna.

5.2 Saran

Berdasarkan pengalaman pelaksanaan kegiatan sosialisasi, terdapat beberapa saran yang ingin disampaikan:

Bagi Mahasiswa

Mahasiswa yang akan melaksanakan kegiatan serupa disarankan untuk mempersiapkan materi sosialisasi dengan bahasa yang mudah dipahami oleh audiens

yang beragam latar belakangnya, serta menyediakan media demonstrasi yang interaktif agar peserta lebih mudah memahami konsep yang disampaikan.

Bagi Peserta Sosialisasi

Peserta disarankan untuk lebih aktif memanfaatkan fitur keamanan yang tersedia pada sistem informasi yang mereka gunakan, serta meningkatkan kesadaran terhadap pentingnya menjaga keamanan akun akademik, termasuk dengan tidak membagikan PIN atau kode *OTP* kepada pihak lain.

Bagi Pengelola SIAKAD UIN SMH Banten

Pengelola SIAKAD disarankan untuk mempertimbangkan penambahan mekanisme keamanan seperti verifikasi dua langkah dan *activity log* pada sistem yang digunakan, dengan tetap memperhatikan kemudahan penggunaan bagi mahasiswa sebagaimana yang telah dirancang dalam prototipe yang dikembangkan. Prototipe yang dihasilkan dari penelitian ini dapat dijadikan referensi awal dalam pengembangan sistem keamanan SIAKAD yang lebih komprehensif.

Bagi Program Studi Informatika

Program Studi Informatika disarankan untuk terus mendorong mahasiswa agar melaksanakan kegiatan KUKERTA yang berkaitan erat dengan bidang keilmuan, sehingga luaran yang dihasilkan dapat memberikan kontribusi nyata bagi pengembangan teknologi informasi di lingkungan kampus.

DAFTAR PUSTAKA

[1] J. Nielsen, Usability Engineering. San Francisco, CA, USA: Morgan Kaufmann, 1994.

[2] J. Nielsen, "10 Usability Heuristics for User Interface Design," Nielsen Norman Group, 2020. [Online]. Available: https://www.nngroup.com/articles/ten-usability-heuristics/

[3] L. F. Cranor and S. Garfinkel, Security and Usability: Designing Secure Systems That People Can Use. Sebastopol, CA, USA: O'Reilly Media, 2005.

[4] A. Adams and M. A. Sasse, "Users Are Not the Enemy," Communications of the ACM, vol. 42, no. 12, pp. 40–46, 1999.

[5] S. Das, L. A. Dabbish and J. I. Hong, "A Typology of Perceived Triggers for End-User Security and Privacy Behaviors," in Symposium on Usable Privacy and Security (SOUPS), 2019.

[6] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen and Y. Koucheryavy, "Multi-Factor Authentication: A Survey," Cryptography, vol. 2, no. 1, pp. 1–31, 2018.

[7] S. N. Lyastani, M. Schilling, S. Fahl, M. Backes and S. Bugiel, "Better Managed than Memorized? Studying the Impact of Managers on Password Strength and Reuse," in USENIX Security Symposium, 2018.

[8] R. Biddle, S. Chiasson and P. C. van Oorschot, "Graphical Passwords: Learning from the First Twelve Years," ACM Computing Surveys, vol. 44, no. 4, pp. 1–41, 2012.

[9] D. Florêncio and C. Herley, "A Large-Scale Study of Web Password Habits," in World Wide Web Conference (WWW), 2007.

[10] A. Dix, J. Finlay, G. Abowd and R. Beale, Human-Computer Interaction. Harlow, U.K.: Pearson Education, 2004.

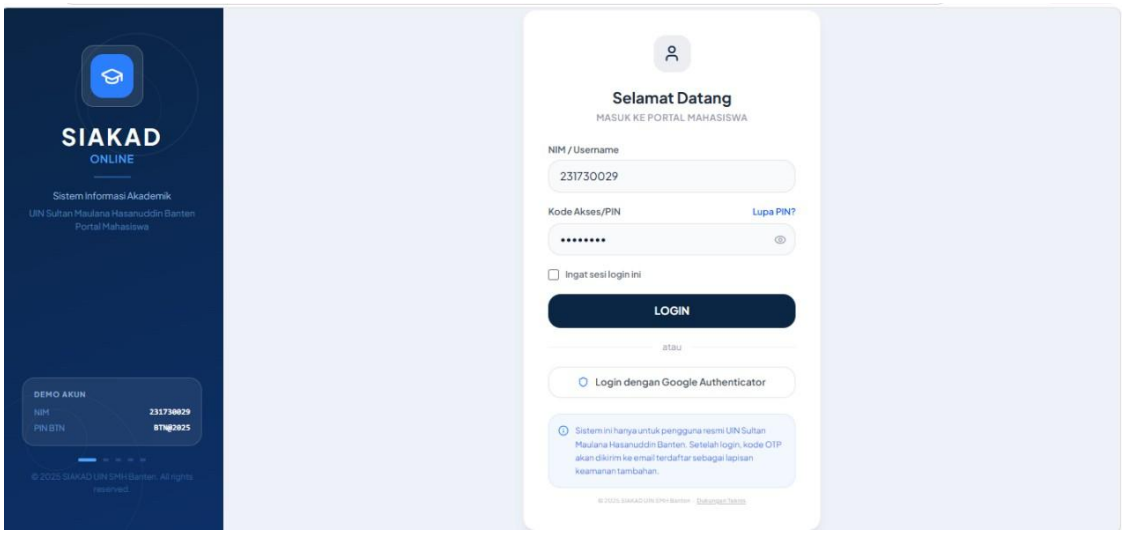
[11] B. R. d. I. Nasional, "Profil Pusat Riset Sains Data dan Informasi (PRSDI)," Jakarta, 2024.

[12] Sugiyono, Metode Penelitian Kuantitatif, Kualitatif, dan R&D. Bandung: Alfabeta, 2019.

LAMPIRAN

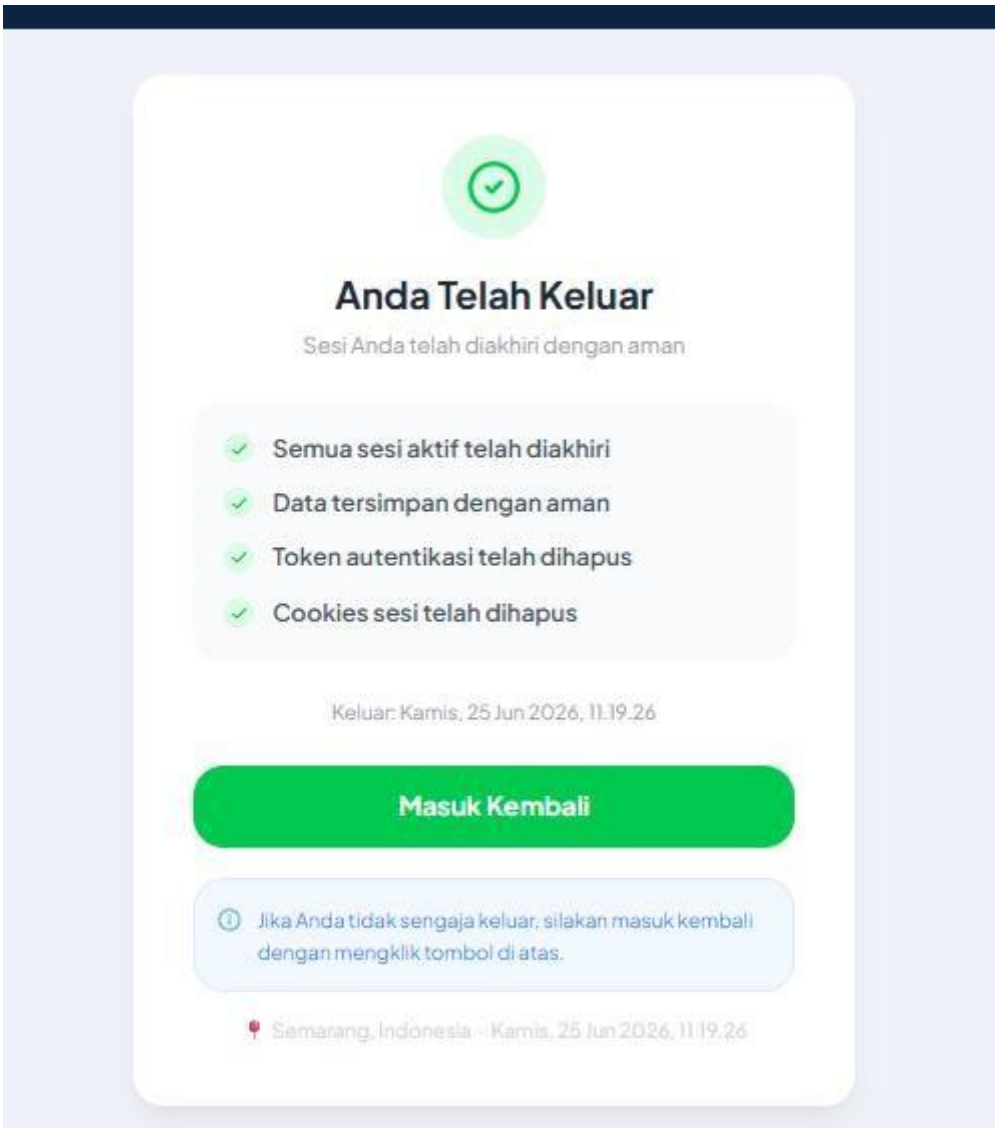
Lampiran 1. Dokumentasi Prototipe Antarmuka Keamanan SIAKAD

Berikut adalah tangkapan layar lengkap prototipe antarmuka keamanan SIAKAD UIN SMH Banten yang didemonstrasikan selama kegiatan sosialisasi KUKERTA:



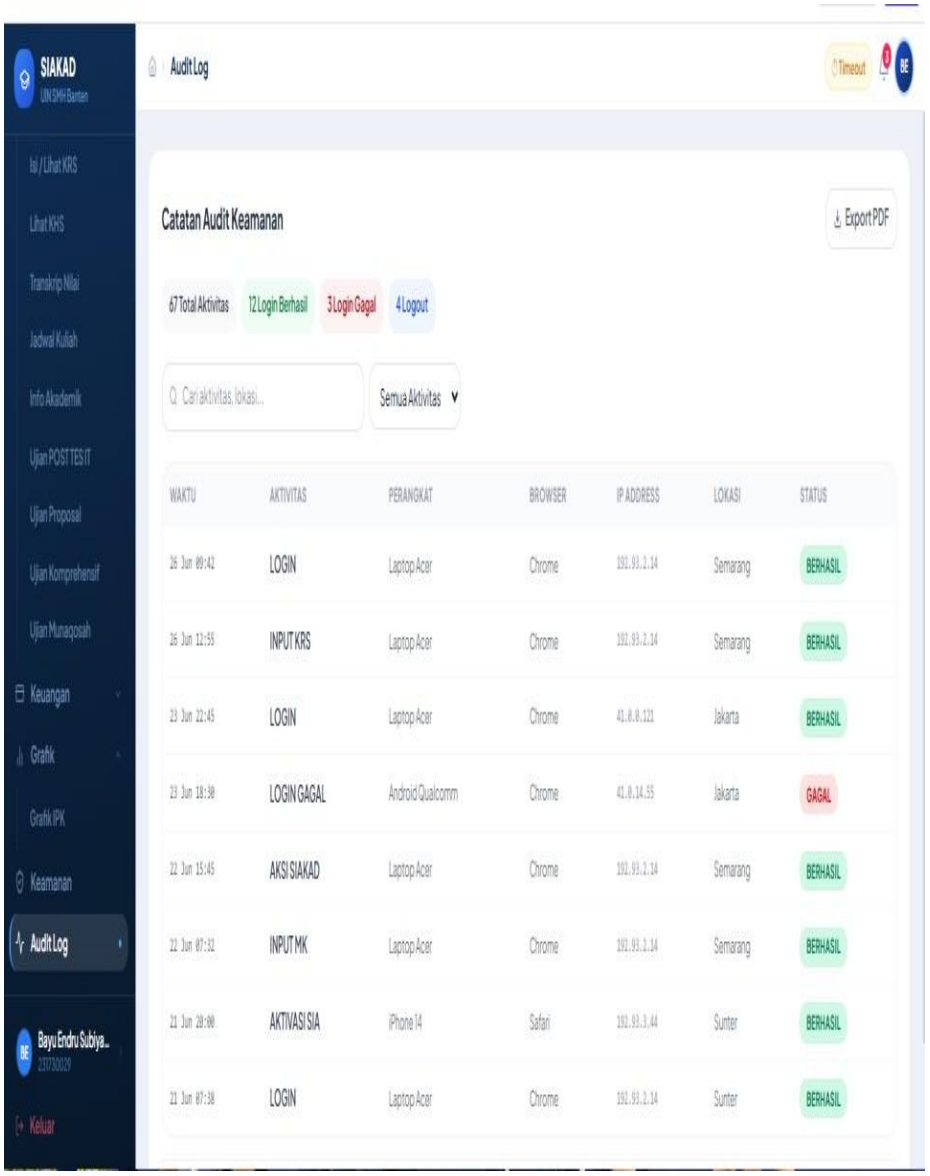
Gambar L.1. Halaman Login SIAKAD

Sumber: Dokumentasi Penulis, 2026



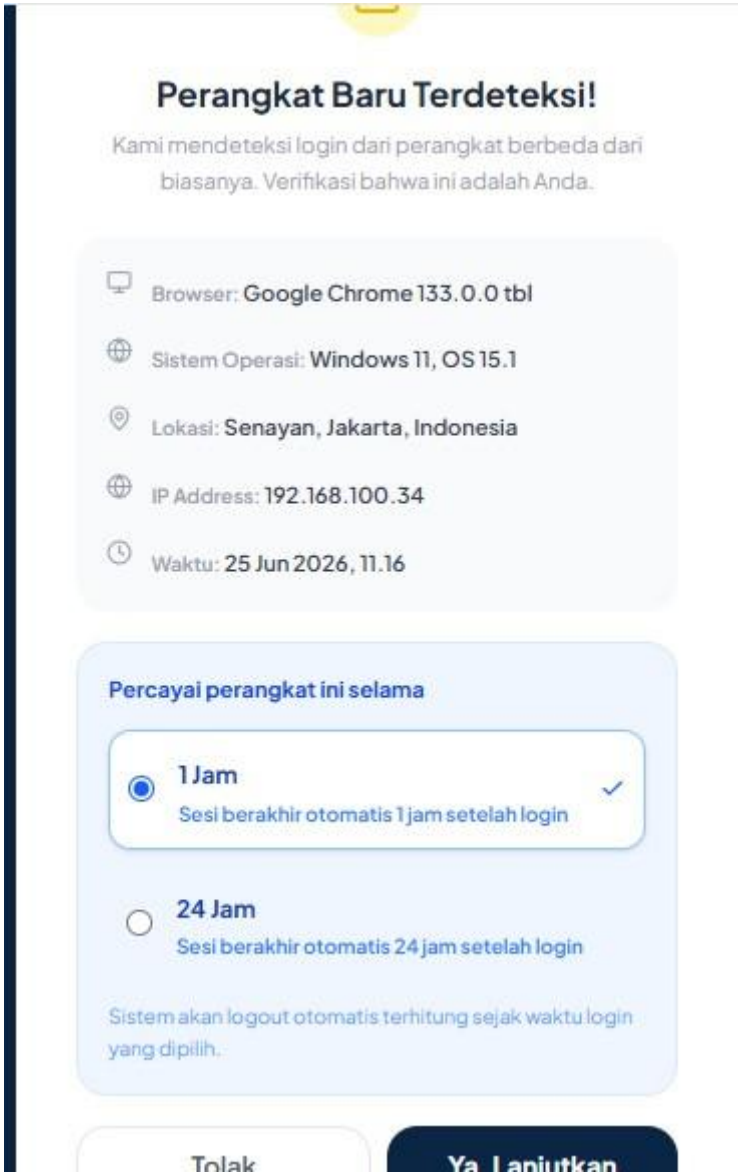
Gambar L.2. Verifikasi Dua Langkah — Email OTP

Sumber: Dokumentasi Penulis, 2026



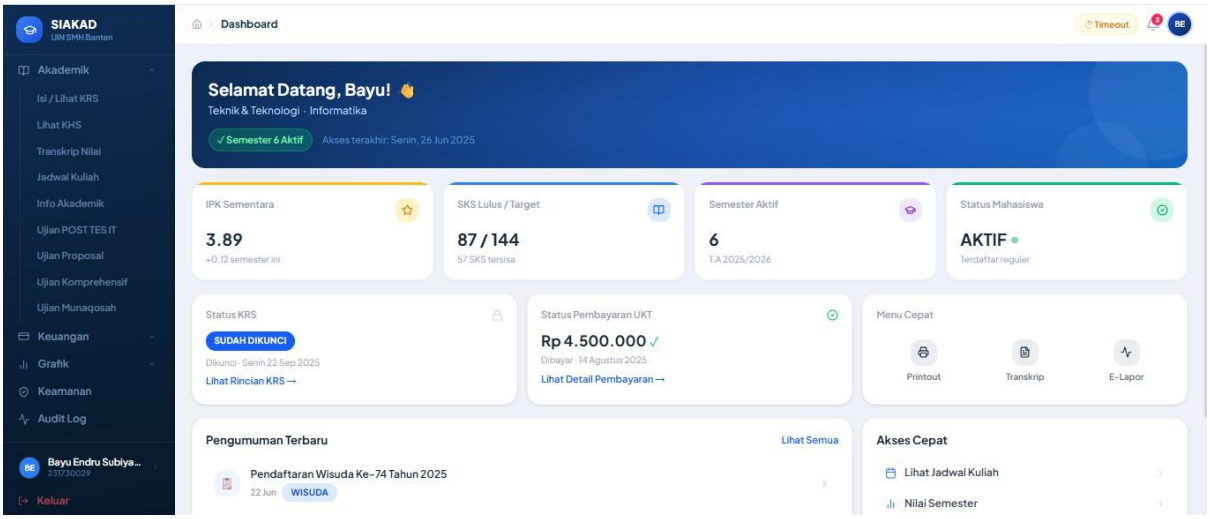
Gambar L.3. Verifikasi Dua Langkah — Google Authenticator

Sumber: Dokumentasi Penulis, 2026



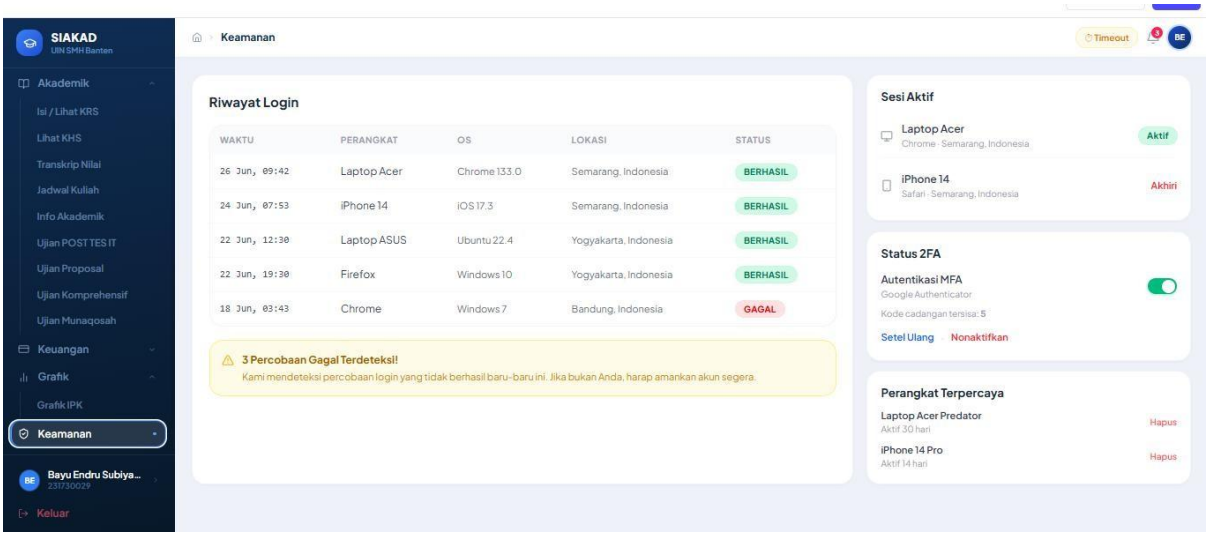
Gambar L.4. Deteksi Perangkat Baru

Sumber: Dokumentasi Penulis, 2026



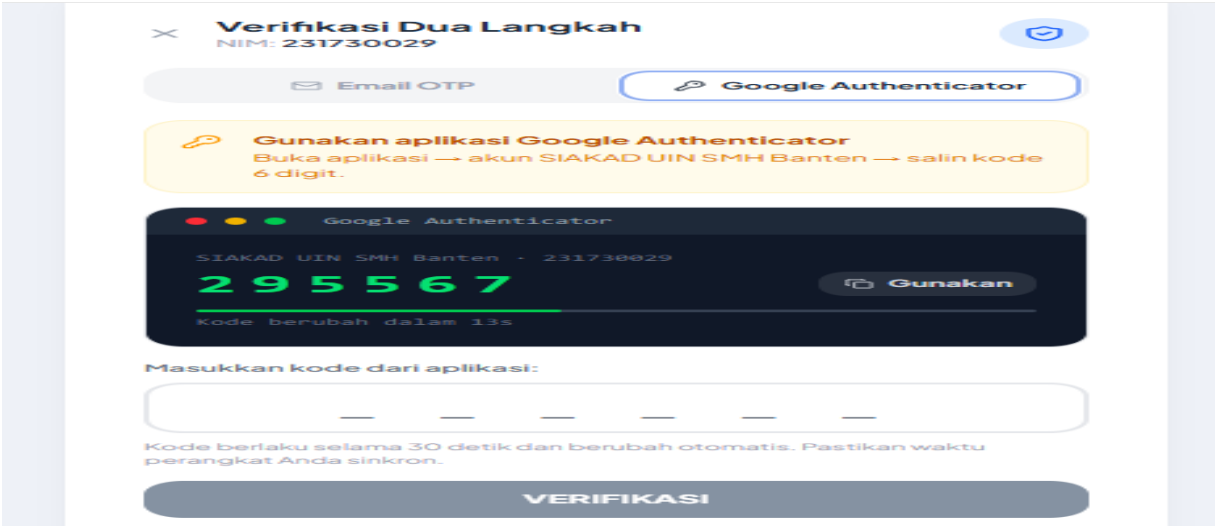
Gambar L.5. Dashboard Utama SIAKAD

Sumber: Dokumentasi Penulis, 2026



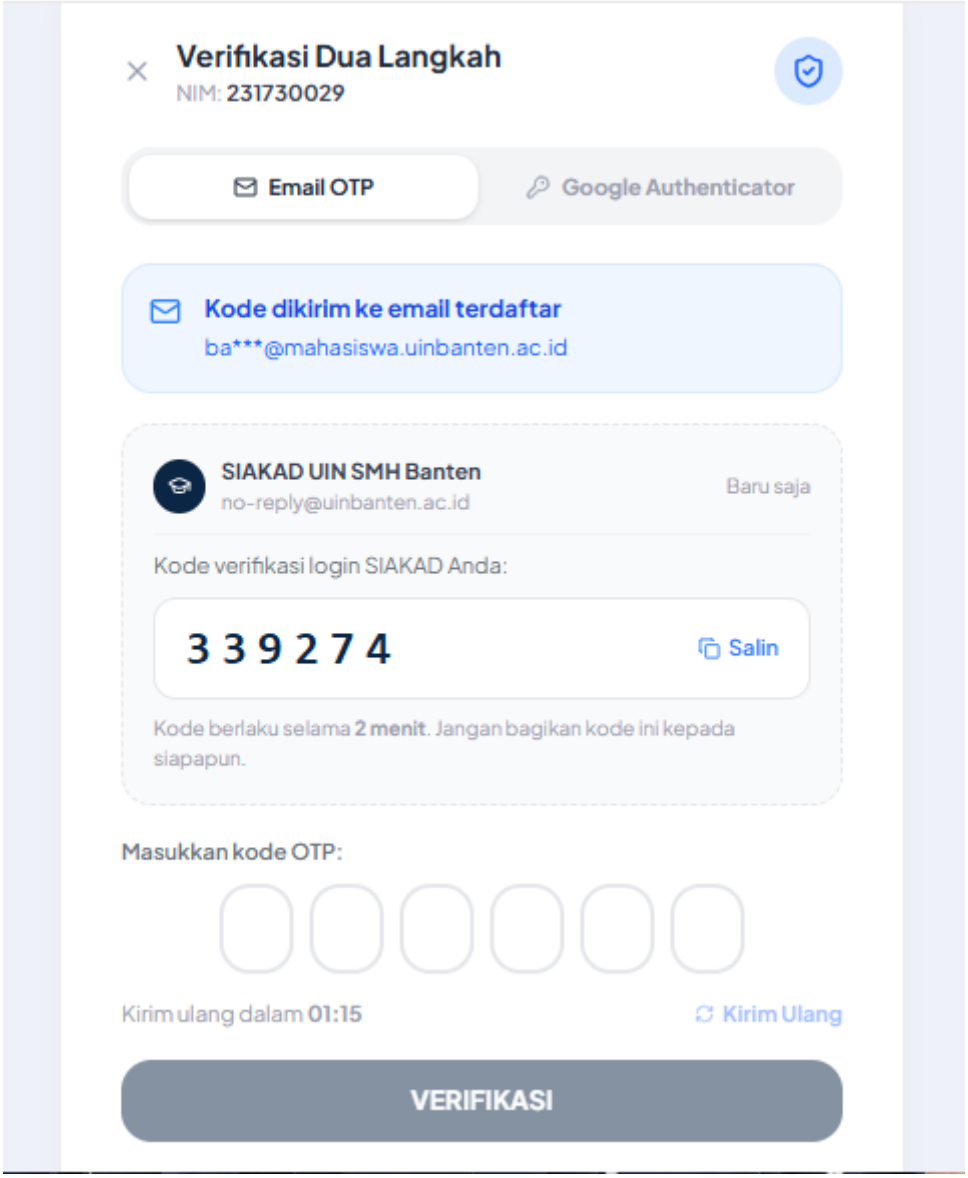
Gambar L.6. Halaman Keamanan dan Manajemen Sesi

Sumber: Dokumentasi Penulis, 2026



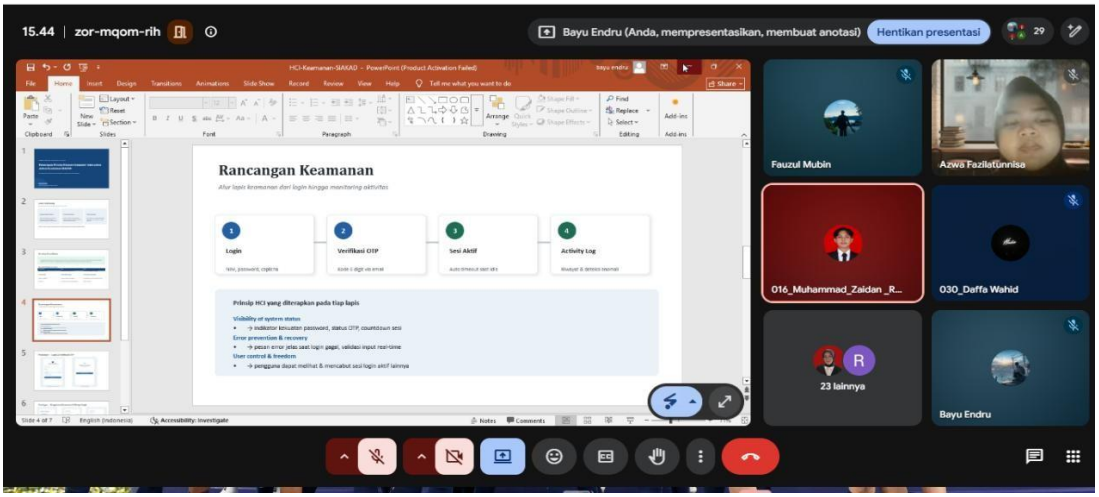
Gambar L.7. Dashboard Audit Log Keamanan

Sumber: Dokumentasi Penulis, 2026

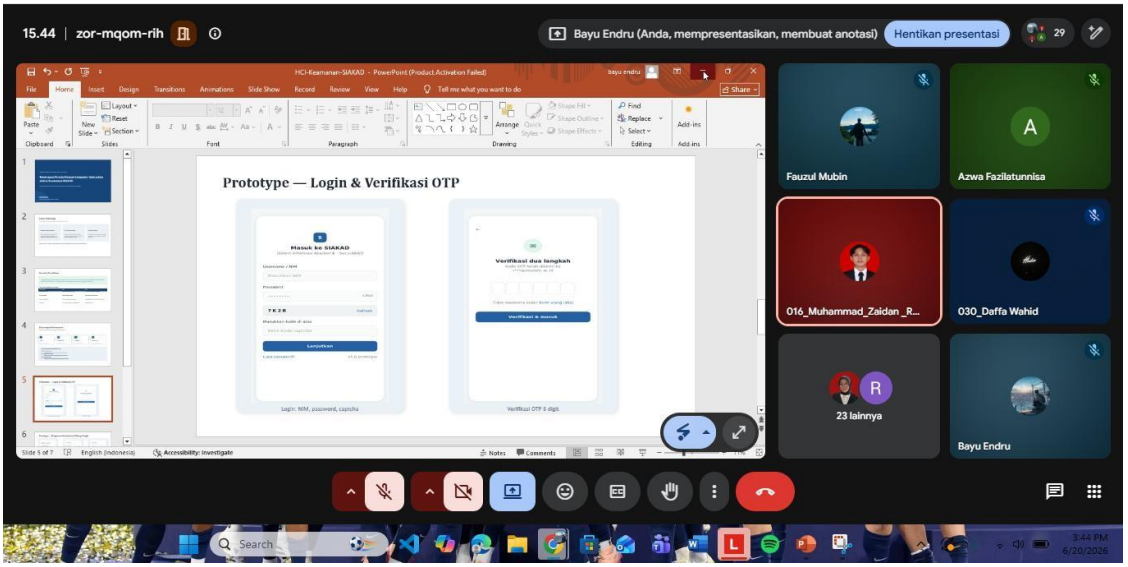


Gambar L.8. Halaman Logout yang Aman

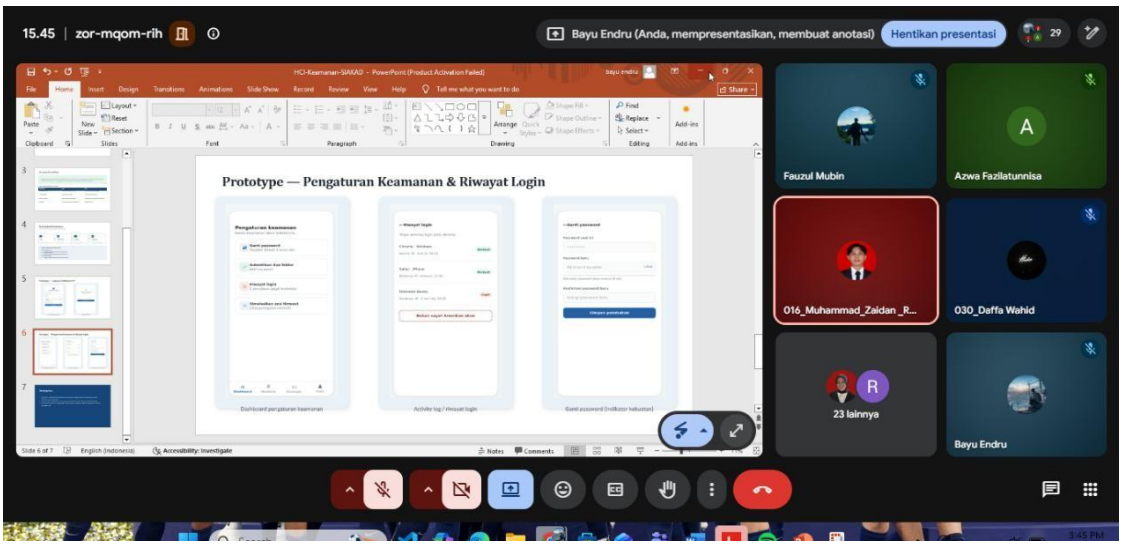
Sumber: Dokumentasi Penulis, 2026



Gambar L.9. Dokumentasi Sosialisai



Gambar L.10. Dokumentasi Sosialisai



Gambar L.11. Dokumentasi Sosialisai