BAB IV
HASIL PENELITIAN DAN PEMBAHASAN

4.1 Hasil Penelitian

Hasil penelitian ini berfokus pada penerapan bagian implementasi pada tahapan ke tiga dari metode waterfall yang berisikan metode Penetration Testing Execution Standard (PTES) yang mencakup tahapan *Exploitation, Post-Exploitation,* dan *Reporting*. Berdasarkan analisis kerentanan yang telah dilakukan pada BAB 3, beberapa kelemahan dalam sistem keamanan website desa telah diidentifikasi dan akan dieksplorasi lebih lanjut dalam tahapan ini.

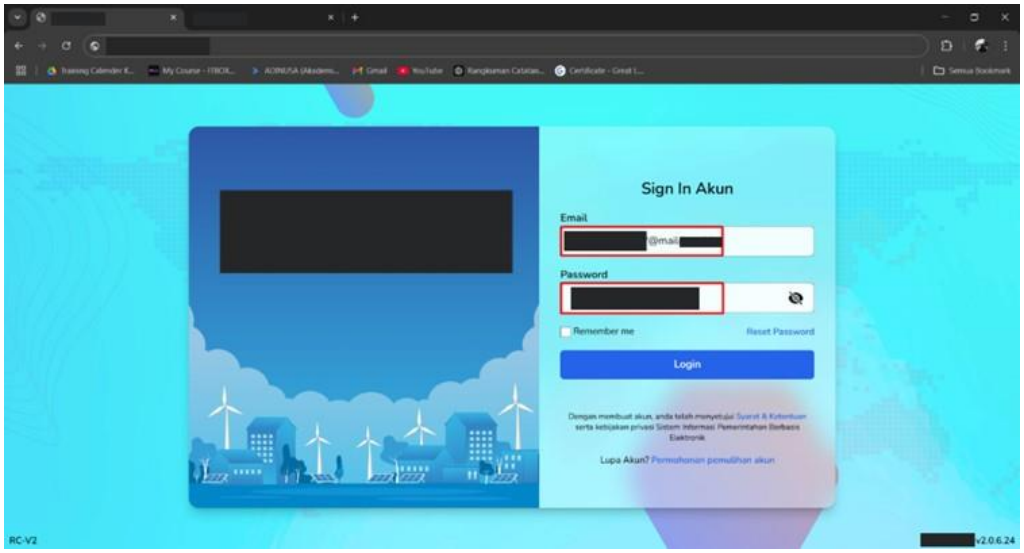
4.2 Implementation

4.2.1 Exploitation

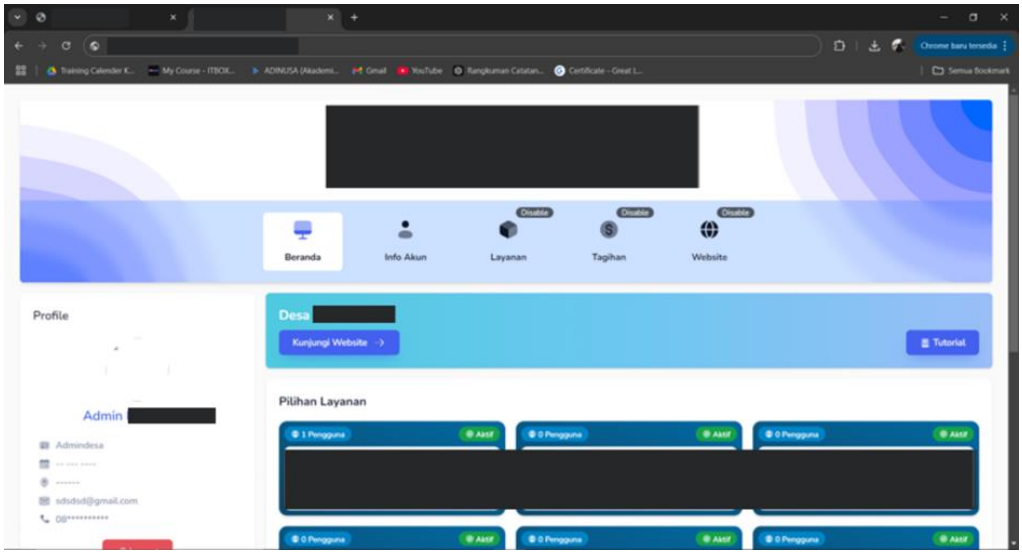
Pada tahap ini, eksploitasi dilakukan terhadap kerentanan yang telah diidentifikasi pada langkah 3.5 Vulnerability Analysis. Beberapa langkah Exploitation yang diambil meliputi Pengujian Ketiadaan MFA, Ketiadaan Pembatasan Login, serta Pengujian Brute Force pada Mockup yang akan dijelaskan lebih detail berikut ini:

1. Pengujian Ketiadaan Multi-Factor Authentication (MFA)

Pada gambar 4.2.1 pengujian dilakukan dengan menggunakan akun yang diberikan akses oleh pihak desa (XYZ) untuk mencoba login ke sistem. Sesuai dengan temuan pada tahap 3.3 Intelligence Gathering, dalam pengujian yang dilakukan ini tidak ditemukan adanya lapisan verifikasi tambahan sehingga setelah dimasukkannya username dan password akan diarahkan langsung ke dashboard Admin seperti yang di tunjukkan pada gambar 4.2.2, yang menunjukkan bahwa sistem rentan terhadap akses tidak sah. Tanpa adanya MFA, penyerang dapat dengan mudah mendapatkan akses ke akun admin hanya dengan menggunakan kredensial yang valid.



Gambar 4.2.1 Proses Login Pada Website Desa



Gambar 4.2.2 Dashboard Admin Setelah Berhasil Login

2. Ketiadaan Pembatasan Login

Penguji melakukan percobaan login menggunakan username yang ditemukan pada halaman Pendaftaran, yaitu dengan format pengelola<nama>@mailxxxx.id. Selain itu, penguji juga menggunakan pola password yang telah diidentifikasi sebelumnya, seperti pengelola<nama>@456.

Dengan melakukan beberapa percobaan login menggunakan temuan pola username dan password yang ada, serta beberapa kombinasi password yang sengaja dimasukkan secara tidak sesuai dengan pola, penguji menemukan bahwa sistem tidak memiliki mekanisme pembatasan jumlah percobaan login yang gagal. Hal ini memungkinkan penyerang untuk mencoba kombinasi password secara berulang tanpa adanya konsekuensi, yang meningkatkan risiko terjadinya serangan brute force. Temuan hasil percobaan login ini dirangkum lebih lanjut pada Tabel 4.2.1 dibawah ini.

Tabel 4.2.1 Tabel Percobaan Login

No.	Username	Password	Status
1.	nama1234567891@mailxxxx.id	pengeloladesajambu@456	Berhasil
2.	nama1234567892@mailxxxx.id	pengeloladesamangga@456	Berhasil
3.	nama1234567893@mailxxxx.id	pengeloladesakedondong@456	Berhasil
4.	nama1234567894@mailxxxx.id	pengeloladesaapel@456	Berhasil
5.	nama1234567895@mailxxxx.id	pengeloladesajeruk@456	Berhasil
6.	nama1234567891@mailxxxx.id	salahpassword1@456	Gagal
7.	nama1234567892@mailxxxx.id	salahpassword2@456	Gagal
8.	nama1234567893@mailxxxx.id	salahpassword3@456	Gagal
9.	nama1234567894@mailxxxx.id	salahpassword4@456	Gagal
10.	nama1234567895@mailxxxx.id	salahpassword5@456	Gagal

3. Pengujian Hydra pada Mockup

Pengujian dilakukan dengan menggunakan *hydra* untuk menguji ketahanan sistem terhadap serangan yang mencoba menebak kombinasi username dan password secara otomatis. Serangan ini ditujukan kepada mockup yang telah dibuat, dengan menggunakan data hasil observasi yang telah dikumpulkan. Username dan password yang digunakan dimasukkan ke dalam file username.txt dan passwords.txt untuk mengetahui keberhasilan dari proses

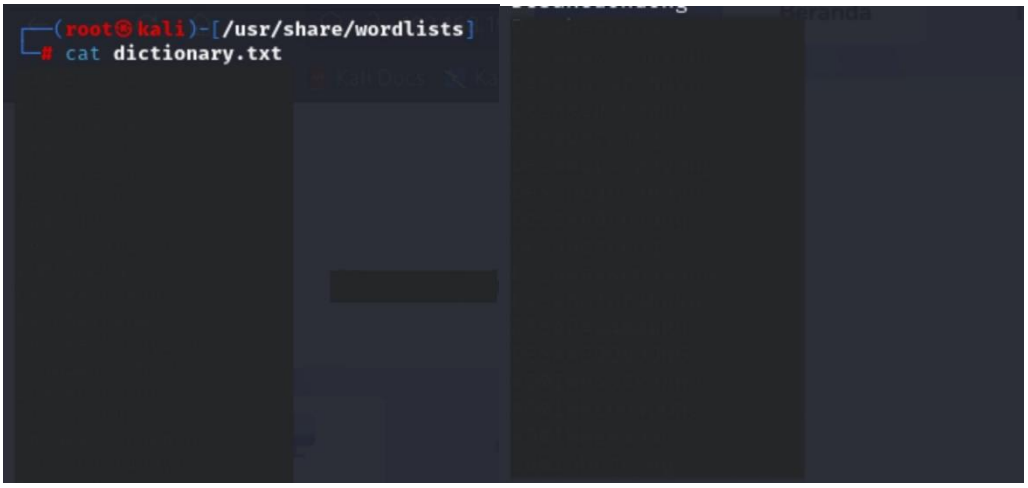
login. Gambar 4.2.3 adalah sampel wordlist untuk bagian username yang diperoleh dari tahapan 3.3 *Intelligence Gathering* yakni 3.3.1 Observasi Halaman Pendaftaran. Sedangkan gambar 4.2.4 dan gambar 4.2.5 merupakan wordlist untuk percobaan penyerangan otomatisasi pada *hydra.*yang mana wordlist hybrid.txt merupakan sampel password yang diperoleh dari identifikasi pada tahapan 3.3.2 Temuan Pola Password.

Langkah-langkah exploitation yang dilakukan dibawah ini dilakukan dengan menggunakan OS Kali Linux dengan:

1. **Membuat Wordlist Data Username dan Password**

   Pada gambar 4.2.3, 4.2.4, dan 4.2.5 merupakan hasil dari pembuatan wordlist untuk keperluan melakukan pengujian dengan hydra.

Gambar 4.2.3 wordlist username.txt



Gambar 4.2.4 wordlist dictionary.txt

Gambar 4.2.5 wordlist hybrid.txt

2. Memasukkan perintah Hydra

Pengujian dilakukan dengan menggunakan perintah Hydra sebagai berikut yang dapat melakukan pengisian username dan password secara otomatis kedalam halaman yang dituju untuk mencoba keberhasilan login. Gambar 4.2.6 dan 4.2.7 merupakan perintah yang digunakan untuk menggunakan hydra.

Gambar 4.2.6 Perintah Hydra (Dictionary Attack)

Gambar 4.2.7 Perintah Hydra (Hybrid Attack)

Gambar 4.2.6 dan 4.2.7 merupakan perintah hydra yang dituliskan pada terminal untuk melakukan serangan otomatisasi oleh hydra baik dictionary attack maupun hybrid attack. Hybrid attack merupakan perpaduan serangan antara insider attack (perolehan password pada saat masa Praktik Kerja) dan dictionary attack yang diidentifikasinya pola password hasil insider attack

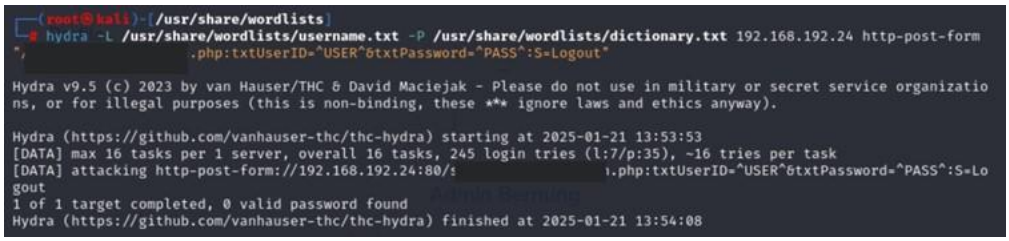
tersebut. Adapun penjelasan mengenai perintah menjalankan hydra, akan dijelaskan berikut ini:

Penjelasan:

- **-L /usr/share/wordlists/username.txt**:
  File yang berisi daftar username yang akan dicoba.
- **-P /usr/share/wordlists/dictionary.txt**:
  atau **-P /usr/share/wordlists/hybrid.txt**
  File yang berisi daftar password yang akan dicoba.
- **192.168.192.24**:
  Alamat IP dari target yang akan diuji.
- **https-post-form**:
  Menunjukkan bahwa metode yang digunakan adalah POST dengan form HTML.
- **"/WebsiteDesa1/sso/auth.php:txtUserID=^USER^&txtPassword =^PASS^:S=Logout"**:
  URL endpoint untuk login, di mana ^USER^ dan ^PASS^ akan digantikan dengan username dan password dari daftar yang dicoba.

3. Hasil Pengujian

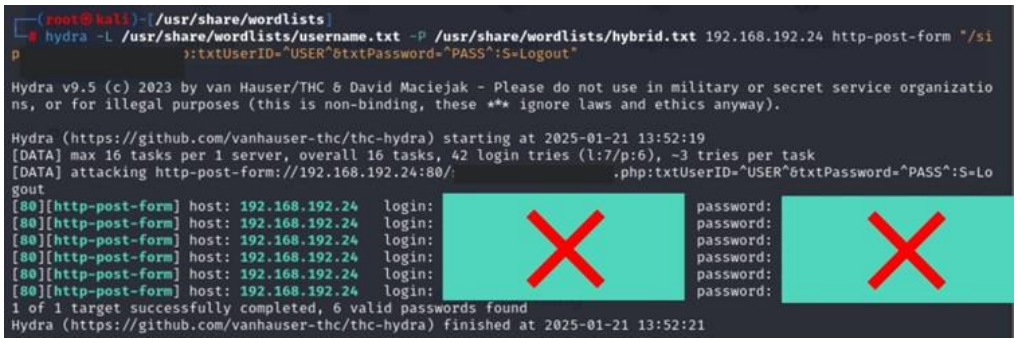
Setelah perintah yang dimasukkan berhasil dijalankan, maka berikut ini adalah hasil dari pengujian yang dilakukan menggunakan Hydra:



Gambar 4.2.8 Hasil Hydra (Dictionary Attack)

Gambar 4.2.8 menunjukkan bahwa serangan Dictionary Attack belum mampu untuk melakukan pembobolan pada sistem keamanan login MockUp. Hal ini

disebabkan isi dari wordlist password pada gambar 4.2.4 dictionary.txt tidak memiliki kata yang cocok dengan password yang ada pada sistem. Untuk itu maka akan dibuktikan dengan melanjutkan pengamatan pada hasil pengujian dengan *hybrid Attack* (penggabungan *Insider Attack* dan *Dictionary Attack*) yang berada pada gambar 4.2.9 berikut ini.



Gambar 4.2.9 Hasil Hydra (Hybrid Attack)

Gambar 4.2.9 menunjukkan bahwa Hasil pengujian *Hybrid Attack* dengan menggunakan *Hydra* menunjukkan bahwa sistem memiliki kerentanan yang signifikan terhadap serangan ini. Dari total 42 percobaan login yang dilakukan, *Hydra* berhasil menemukan 6 kombinasi username dan password yang valid. Untuk pengujian lebih lanjut, dilakukan percobaan serangan Dictionary Attack dan Hybrid Attack sebanyak 10 kali seperti yang ditampilkan pada tabel 4.2.2 berikut.

Tabel 4.2.2 Percobaan Pengujian Hydra

No.	Jenis Pengujian	Waktu Percobaan	Hasil
1.	Dictionary Attack	00:00:15	0 Valid Password Found
2.	Hybrid Attack	00:00:02	6 Valid Password Found
3.	Dictionary Attack	00:00:14	0 Valid Password Found
4.	Hybrid Attack	00:00:03	6 Valid Password Found
5.	Dictionary Attack	00:00:15	0 Valid Password Found
6.	Hybrid Attack	00:00:03	6 Valid Password Found
7.	Dictionary Attack	00:00:15	0 Valid Password Found
8.	Hybrid Attack	00:00:04	6 Valid Password Found
9.	Dictionary Attack	00:00:15	0 Valid Password Found
10.	Hybrid Attack	00:00:03	6 Valid Password Found

Berdasarkan tabel 4.2.2, terlihat bahwa dari 10 percobaan, serangan *Hybrid Attack* berhasil menemukan kombinasi username dan password yang valid sebanyak 6 kali, sementara *Dictionary Attack* tidak berhasil sama sekali. Ini menunjukkan bahwa metode serangan hybrid lebih efektif dibandingkan dengan metode dictionary pada pengujian ini.

Secara keseluruhan, hasil pengujian ini menegaskan bahwa sistem rentan terhadap serangan brute force. Diperlukan evaluasi lebih lanjut terhadap kebijakan keamanan yang diterapkan untuk meningkatkan perlindungan terhadap serangan semacam ini. Beberapa poin penting dari hasil pengujian ini adalah:

1. **Keberhasilan Akses**: Enam akun admin berhasil diakses menggunakan kombinasi username dan password yang telah disiapkan. Ini menunjukkan bahwa password yang digunakan tidak cukup kuat untuk menahan serangan brute force, dan pola yang digunakan dalam pembuatan password mungkin terlalu mudah ditebak.

2. **Efisiensi Serangan**: Dengan menggunakan wordlist yang berisi username dan password, Hydra mampu menyelesaikan serangan dalam waktu singkat, menunjukkan bahwa sistem tidak memiliki mekanisme yang efektif untuk mendeteksi atau mencegah serangan brute force.
3. **Keterbatasan Keamanan**: Keberhasilan serangan ini menandakan bahwa sistem tidak membatasi jumlah percobaan login yang gagal, yang memungkinkan penyerang untuk terus mencoba kombinasi tanpa adanya konsekuensi. Hal ini menciptakan celah yang dapat dimanfaatkan oleh penyerang untuk mendapatkan akses tidak sah.

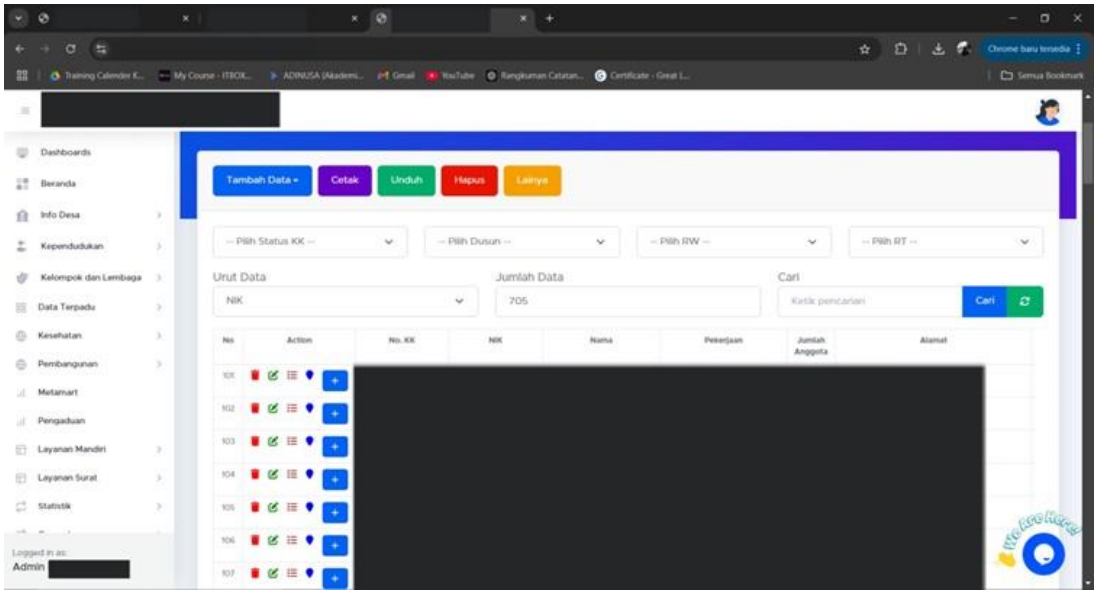
Secara keseluruhan, hasil pengujian ini menegaskan bahwa sistem Website Desa rentan terhadap serangan brute force, dan menunjukkan perlunya evaluasi lebih lanjut terhadap kebijakan keamanan yang diterapkan.

4.2.2 Post-Exploitation

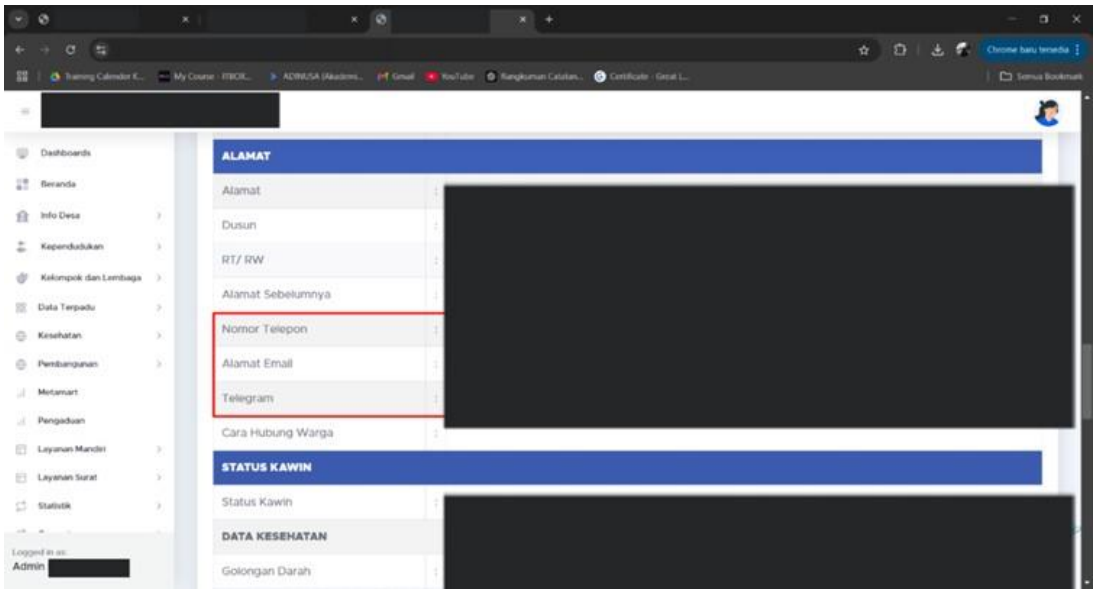
Setelah berhasil mengeksploitasi sistem, penguji menganalisis tingkat akses yang diperoleh dan potensi risiko yang dihadapi. Tahap ini juga mencakup pengumpulan informasi tambahan yang dapat digunakan untuk menilai lebih lanjut dampak dari serangan dan untuk membantu dalam mitigasi.

Beberapa temuan penting dari tahap ini meliputi:

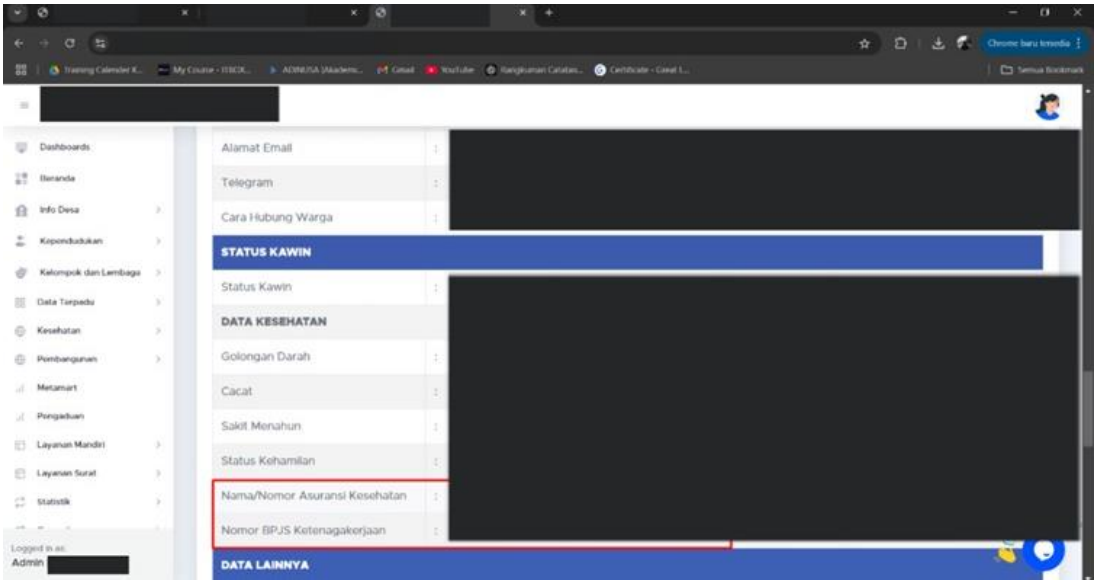
1. **Akses Data Sensitif:** Penyerang yang berhasil masuk ke akun admin dapat mengakses data sensitif masyarakat, termasuk data dalam Kartu Keluarga (KK) yang terdapat pada gambar 4.3.1. Selain itu, Informasi lain yang diperoleh juga mencakup nomor telepon, alamat email, dan nomor BPJS yang terdapat pada gambar 4.3.2 dan 4.3.3. Akses terhadap data ini dapat mengakibatkan pelanggaran privasi dan penyalahgunaan informasi pribadi.



Gambar 4.2.10 Halaman Data Kartu Keluarga Masyarakat

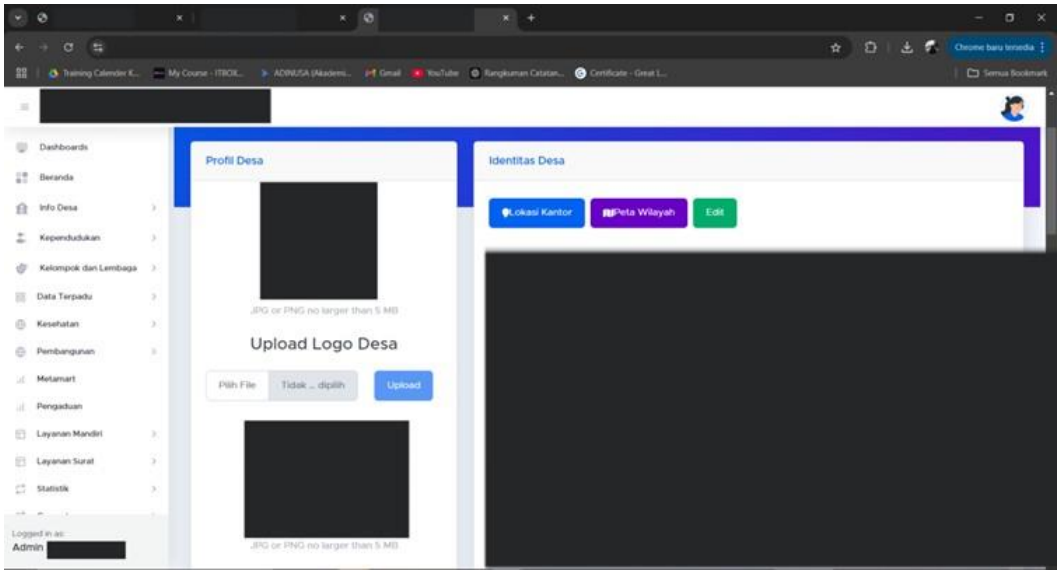


Gambar 4.2.11 Halaman Detail Data Penduduk 1

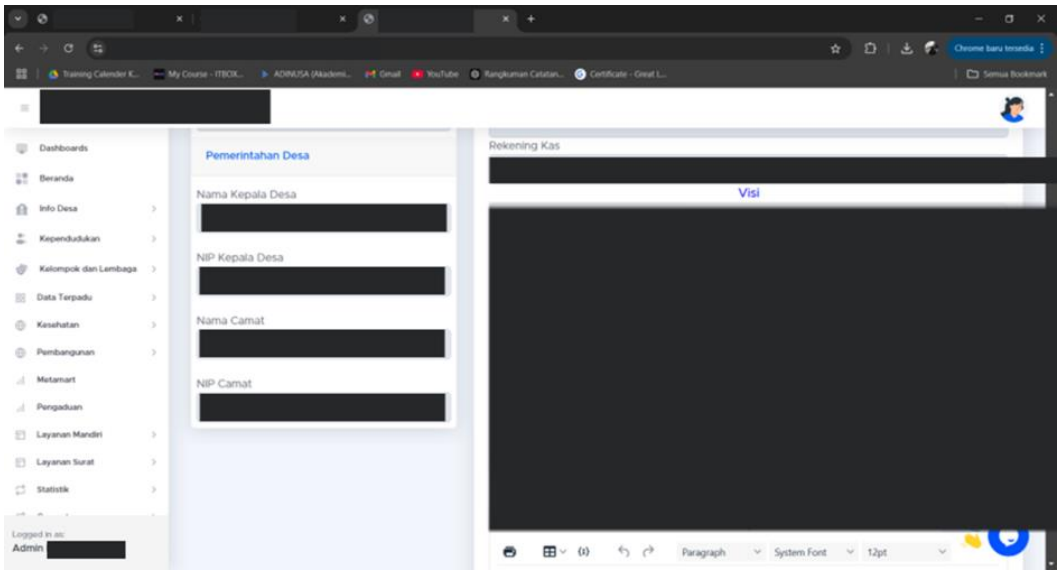


Gambar 4.2.12 Halaman Detail Data Penduduk 2

2. **Kemampuan untuk Mengubah Data:** Seperti yang ditampilkan pada gambar 4.3.4 dan 4.3.5 Penyerang dapat melakukan perubahan pada berbagai data yang ada dalam sistem, seperti slogan desa, kode pos, alamat kantor, rekening desa, visi dan misi desa, serta gambar logo dan kantor desa. Kemampuan ini memberikan penyerang kontrol penuh atas informasi yang ditampilkan kepada publik, yang dapat merusak reputasi desa dan menimbulkan kebingungan di kalangan masyarakat.



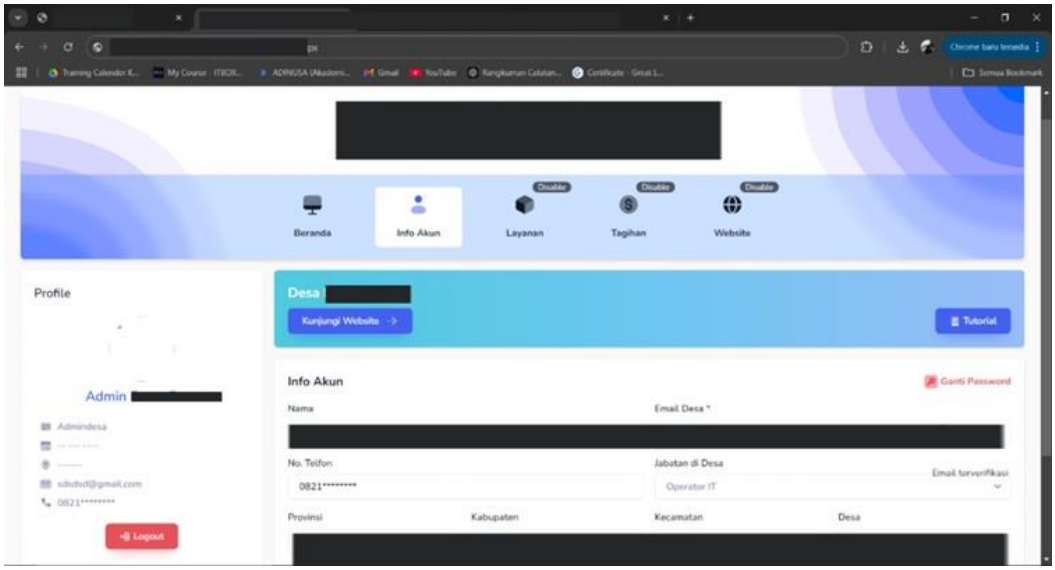
Gambar 4.2.13 Halaman Identitas Desa 1



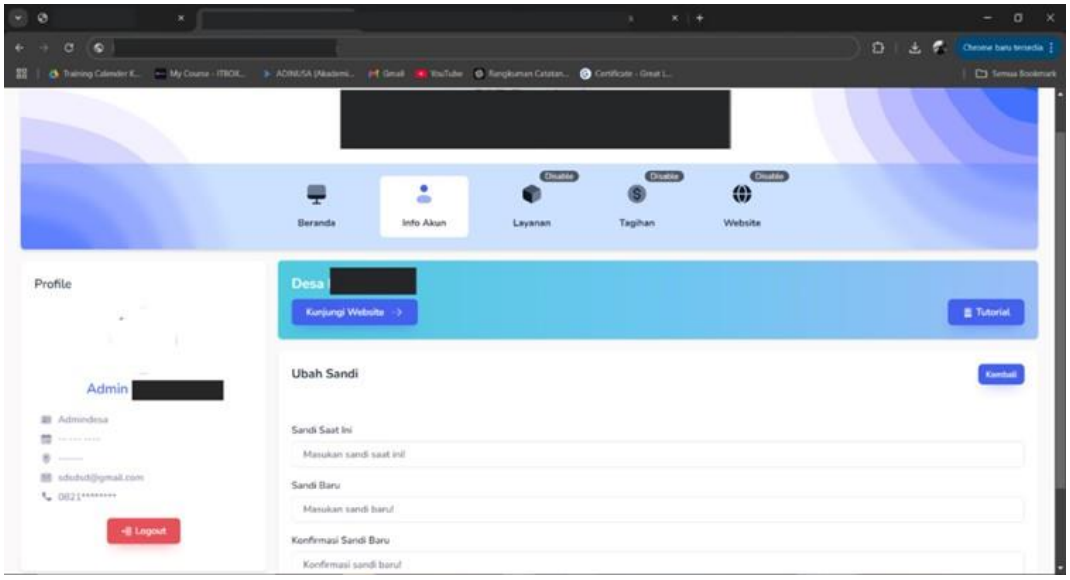
Gambar 4.2.14 Halaman Identitas Desa 2

3. **Pengelolaan Akun Admin:** Penyerang memiliki kemampuan untuk mengelola akun admin, termasuk mengganti password akun admin tersebut. Dengan kemampuan ini, penyerang dapat mengunci pemilik sah dari akses ke akun admin, sehingga mereka dapat mempertahankan kontrol penuh atas sistem. Selain itu, penyerang juga dapat mengubah data akun admin lainnya, yang memungkinkan

mereka untuk menyembunyikan jejak akses mereka dan menghindari deteksi. Halaman tersebut dapat dilihat pada gambar 4.3.6 dan 4.3.7 berikut ini.

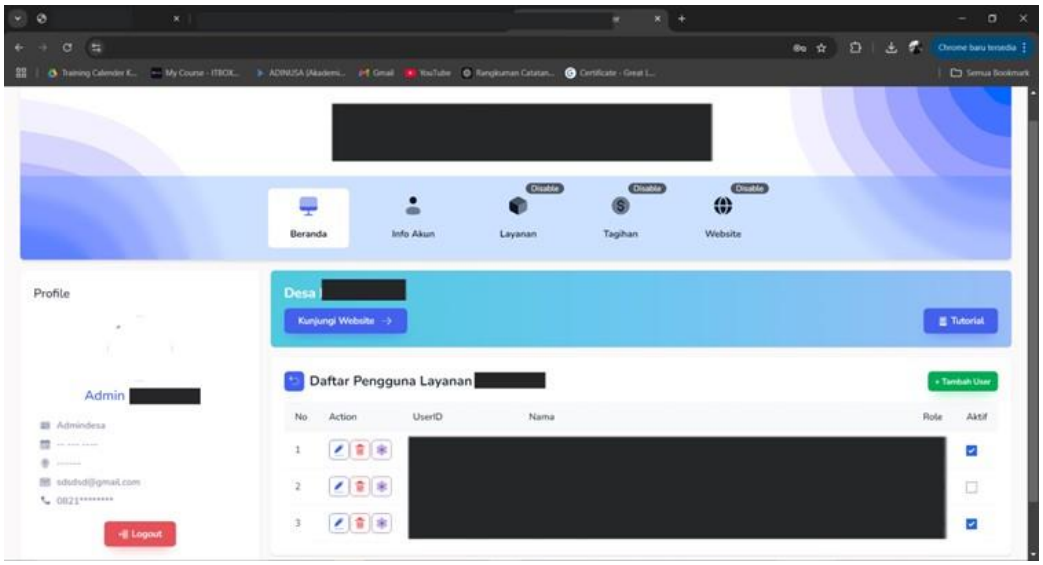


Gambar 4.2.15 Halaman Pengelolaan Data Akun Admin

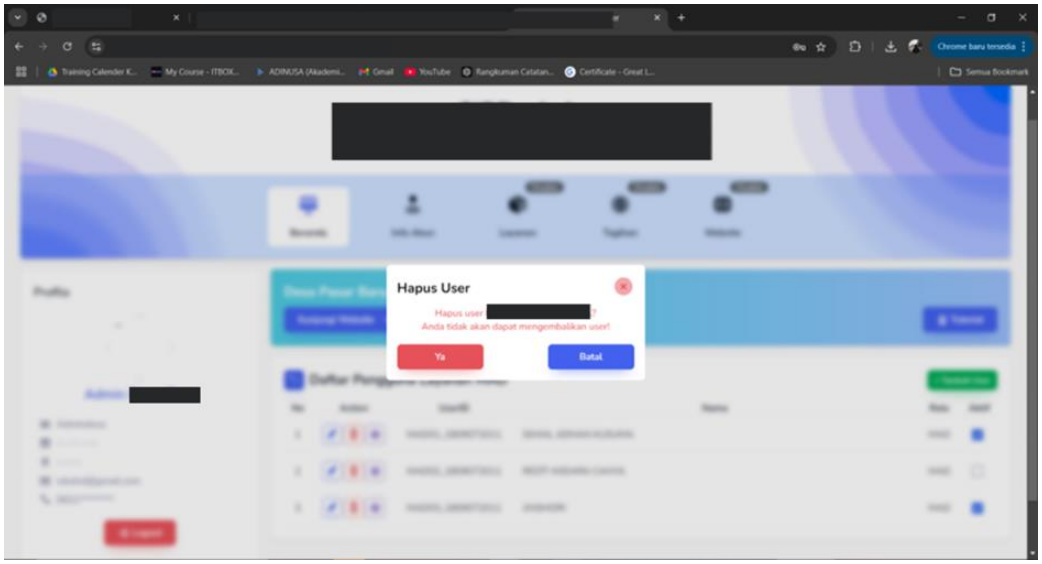


Gambar 4.2.16 Halaman Pengelolaan Password Akun Admin

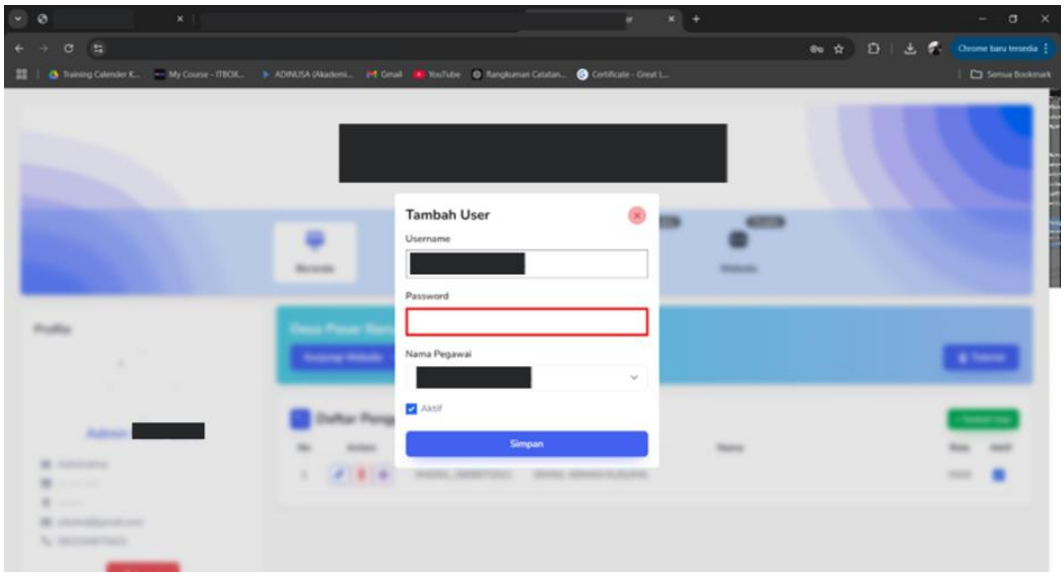
4. **Pengelolaan Akun Aparat Desa:** Selain akun admin, penyerang juga dapat mengelola akun level aparat desa yang di tampilkan pada gambar 4.3.8, termasuk menghapus akun aparat desa (gambar 4.3.9) dan mengubah password aparat (gambar 4.3.10). Hal ini dapat mengakibatkan hilangnya akses aparat desa yang sah ke sistem, serta menciptakan kekacauan dalam pengelolaan data dan informasi desa.



Gambar 4.2.17 Halaman Pengelolaan Akun Aparat Desa



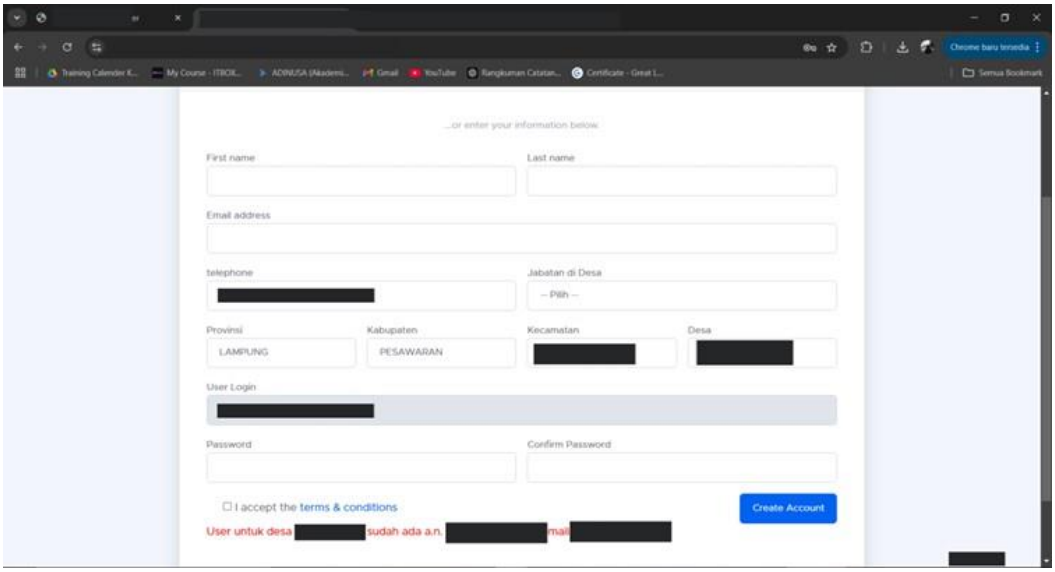
Gambar 4.2.18 Tampilan Proses Penghapusan Akun Aparat Desa



Gambar 4.2.19 Tampilan Proses Edit Akun Aparat Desa

5. **Halaman Pendaftaran Mandiri untuk Akun Admin:** Berdasarkan wawancara dengan operator desa pada tahap 3.2 *Pre-Engagement Interactions*, diketahui bahwa akun admin desa diberikan langsung kepada operator desa (username dan password). Hal ini berarti operator admin desa tidak perlu melakukan pendaftaran secara mandiri untuk memiliki akun admin desa. Dengan demikian, pembuatan akun hanya dilakukan oleh Super Admin.

Oleh karena itu, tombol atau halaman "Pendaftaran" pada gambar 4.3.11 sebaiknya tidak ditampilkan atau tidak dapat diakses oleh pihak lain, terutama karena halaman tersebut memiliki kerentanan yang memungkinkan penyerang untuk menampilkan username masing-masing desa.



Gambar 4.2.20 Halaman Pendaftaran Akun Admin Desa

Dengan adanya temuan-temuan tersebut, berikut ini adalah potensi risiko yang dihadapi:

1. **Pelanggaran Privasi:** Akses terhadap data sensitif masyarakat dapat mengakibatkan pelanggaran privasi yang serius, yang dapat digunakan untuk tujuan penipuan atau pencurian identitas.
2. **Manipulasi Informasi:** Kemampuan untuk mengubah data penting dapat menyebabkan penyebaran informasi yang salah, yang dapat merusak reputasi desa dan menimbulkan ketidakpercayaan di kalangan masyarakat.
3. **Kehilangan Kontrol Sistem:** Dengan kemampuan untuk mengganti password akun admin dan mengelola akun aparat desa, penyerang dapat

menghapus atau mengubah akses ke sistem, yang dapat mengakibatkan kehilangan kontrol atas data dan fungsi penting dalam sistem.

4. **Risiko Keamanan Jangka Panjang:** Jika penyerang berhasil mengubah password dan menghapus jejak akses mereka, mereka dapat mempertahankan akses ke sistem dalam jangka waktu yang lama, meningkatkan risiko serangan lebih lanjut di masa depan.

Secara keseluruhan, hasil dari tahap post-exploitation menunjukkan bahwa sistem memiliki kerentanan yang signifikan yang dapat dimanfaatkan oleh penyerang untuk merusak integritas dan kerahasiaan data yang dikelola.

4.2.3 Reporting

1. **Pendahuluan**

   Laporan ini disusun berdasarkan pengujian keamanan sistem yang dilakukan menggunakan metode PTES (Penetration Testing Execution Standard). Pengujian ini bertujuan untuk mengidentifikasi dan mengevaluasi kerentanan keamanan pada sistem serta memberikan rekomendasi untuk mitigasi risiko. Fokus utama pengujian adalah halaman Pendaftaran, login, dan fitur administrasi pada sistem desa digital (xxy.websitedesa.com).

2. **Temuan**

   Berdasarkan pengujian yang dilakukan, berikut adalah rangkuman temuan utama:

   1. **Kerentanan Format Username dan Password Default**: Format username dan password default yang mudah ditebak, meningkatkan risiko serangan brute force dan dictionary attack.
   2. **Ketiadaan Multi-Factor Authentication (MFA)**: Sistem login tidak memiliki lapisan verifikasi tambahan untuk meningkatkan keamanan akses.

3. **Fitur Reset Password Tidak Berfungsi**: Mengakibatkan pengguna tidak dapat memulihkan akses ke akun jika lupa password.
4. **Tidak Ada Pembatasan Percobaan Login**: Membuka peluang serangan brute force.
5. **Kebocoran Data Sensitif**: Data Username Admin Desa, data masyarakat, termasuk informasi pribadi seperti nomor BPJS, dapat diakses oleh pihak tidak berwenang.
6. **Kemampuan Penyerang untuk Mengubah dan Mengelola Data**: Termasuk data akun admin dan aparat desa.

3. Dampak Potensial

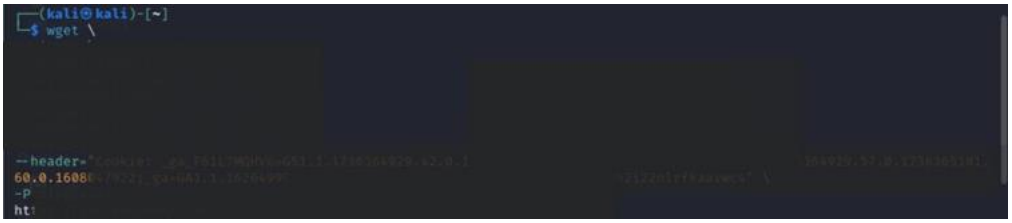
1. **Pelanggaran Privasi**: Data sensitif masyarakat dapat disalahgunakan untuk penipuan atau pencurian identitas.
2. **Gangguan Operasional**: Manipulasi data penting yang mengakibatkan ketidakpercayaan masyarakat.
3. **Kehilangan Kendali Sistem**: Penyerang dapat mengunci pengguna sah dari akses ke sistem.
4. **Kerusakan Reputasi**: Lemahnya keamanan sistem dapat merusak citra desa.

4. Rekomendasi Mitigasi

Sebelum menyajikan rekomendasi mitigasi, perlu dicatat bahwa rekomendasi pengembangan sistem keamanan ini telah dilengkapi dengan pembuatan website berbasis PHP menggunakan Visual Studio Code, XAMPP, MySQL, PHPMailer, Twilio, dan WGET. WGET digunakan untuk memperoleh file frontend dari website asli, yang memungkinkan pembuatan mockup dengan tampilan yang sama persis seperti website aslinya tanpa menggunakan program asli.

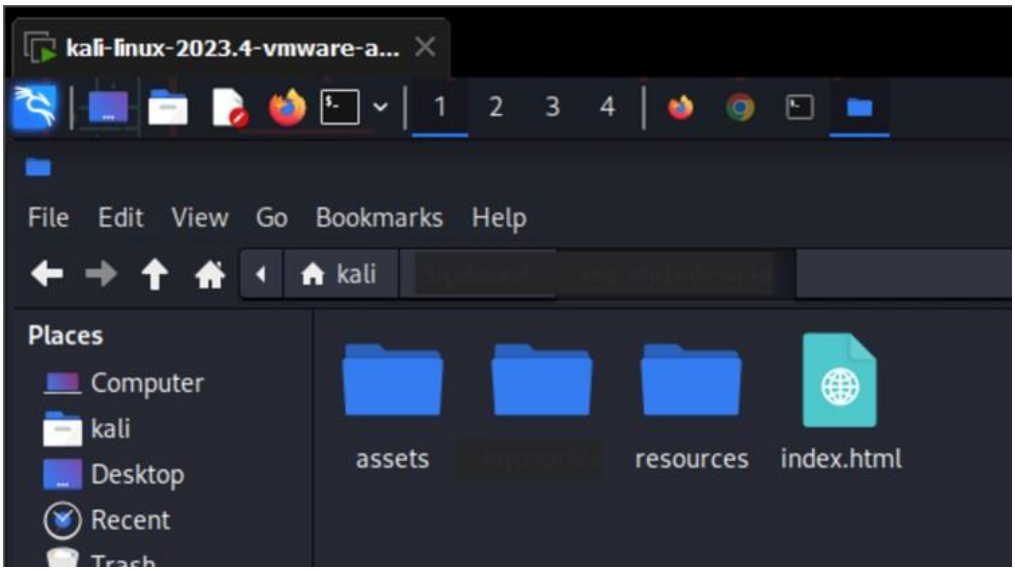
Sistem keamanan yang telah dikembangkan menggunakan mockup ini diharapkan dapat memudahkan proses mitigasi dan implementasi oleh developer website desa pada website aslinya. Masing-masing rekomendasi mitigasi akan dilampirkan dengan flowchart dan hasil dari mitigasi yang telah dilakukan pada mockup yang telah dibuat.

Berikut ini gambar 4.4.1 adalah perintah yang dituliskan untuk penggunaan WGET dalam memperoleh file *front-end.*



Gambar 4.2.21 Perintah WGET unruk memperoleh file FrontEnd

Setelah perintah WGET berhasil dijalankan, maka akan didapatkan file *front-end* yang akan digunakan dalam pembuatan mockup dan rekomendasi mitigasi.



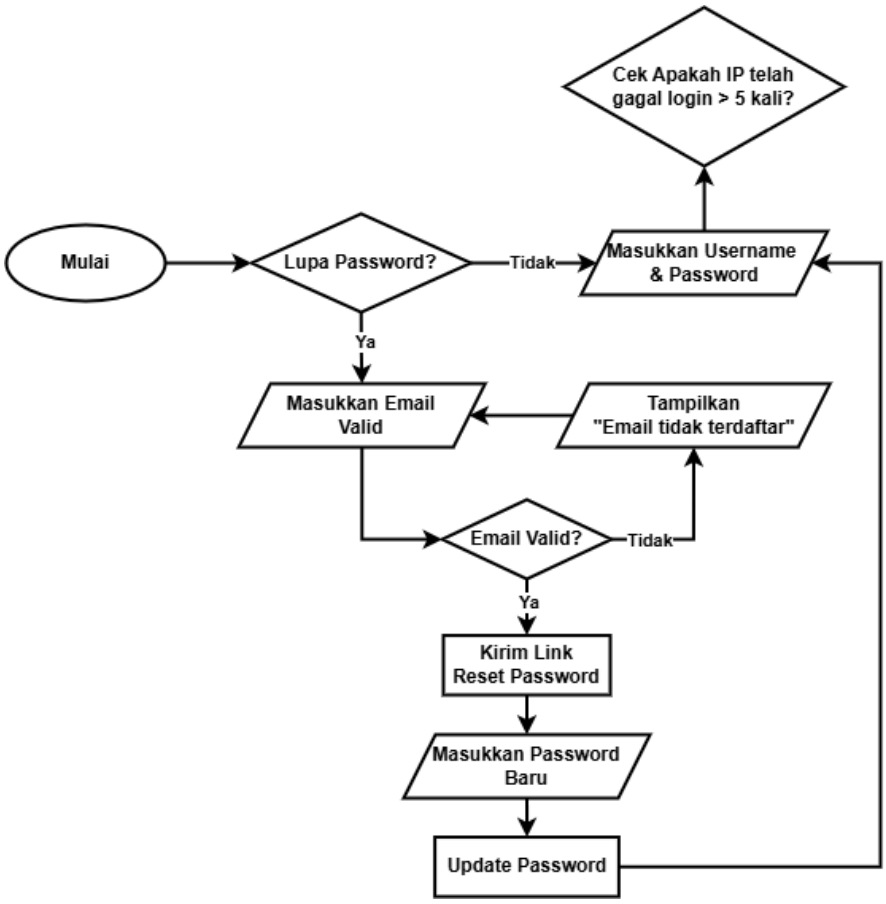
Gambar 4.2.22 File Hasil dari perintah WGET

Rekomendasi mitigasi akan dimulai dari A hingga D berikut ini.

A. Perbaikan Sistem Autentikasi

1. Perbaiki fitur "Reset Password" agar dapat digunakan untuk pemulihan akses.

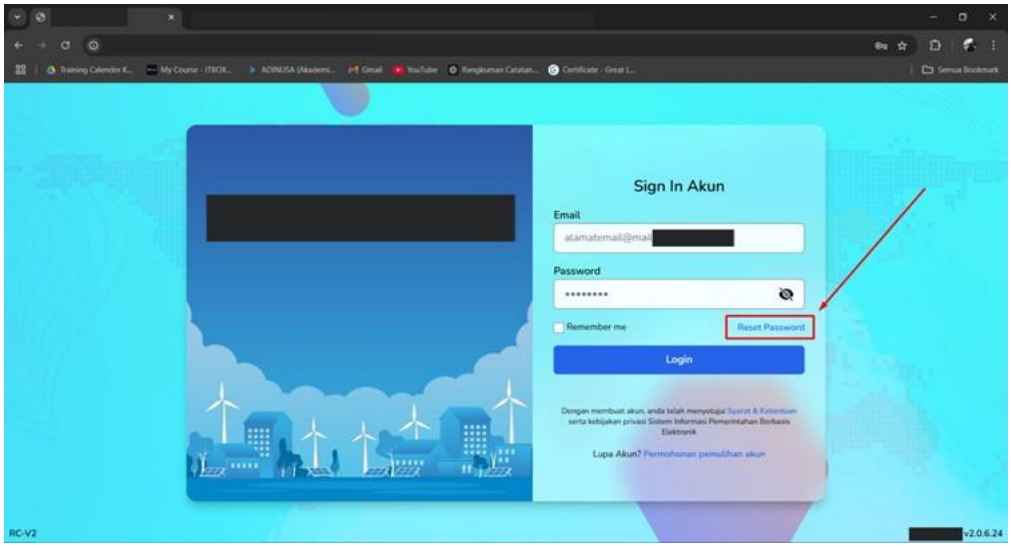
Perbaikan Sistem Autentikasi dimulai dari perbaikan pada fitur “Reset Password” yang mana fitur ini diperbaiki karena terdapat potensi “Account Lockout Risk” yang diidentifikasi pada tahapan 3.4 Threat Modeling.



Gambar 4.2.23 Flowchart fitur Reset Password

Penjelasan mengenai Flowchart pada gambar 4.4.3 tersebut adalah sebagai berikut:

a. **Mulai:** Proses dimulai.
b. **Lupa Password?:** Pengguna ditanya apakah mereka lupa password. Jika ya, lanjut ke langkah berikutnya; jika tidak, pengguna diminta untuk memasukkan username dan password.



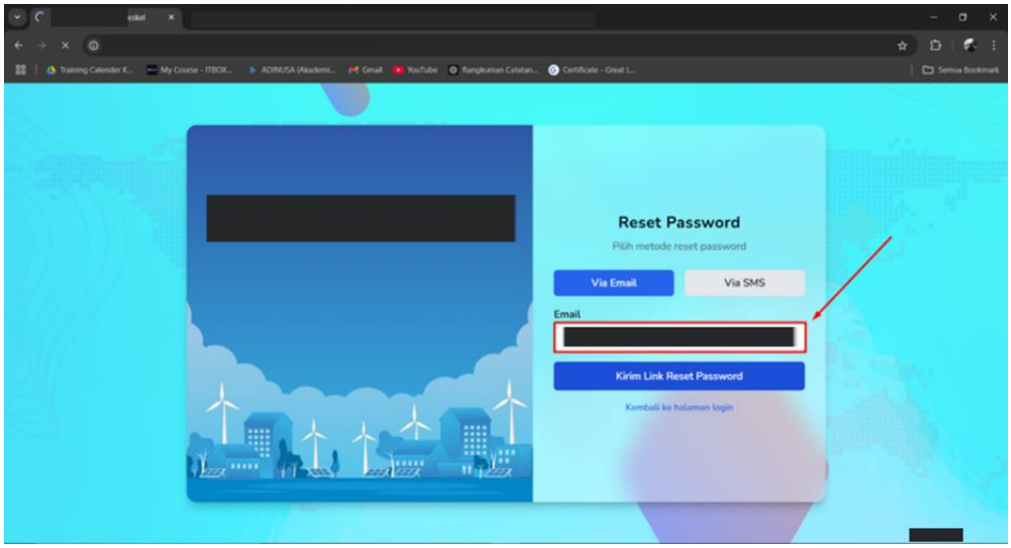
Gambar 4.2.24 Proses Reset Password 1 (Tombol Reset Pasword)

Gambar 4.4.4 merupakan gambar halaman login user yang didalamnya terdapat tombol Reset Password yang sebelumnya tidak berfungsi atau tidak dapat digunakan. Pada mitigasi ini tombol tersebut difungsikan untuk mengarahkan user ke halaman Reset Password seperti pada gambar 4.4.5.

c. **Masukkan Email Valid:** Pengguna diminta untuk memasukkan alamat email yang terdaftar.

Berikutnya, pada gambar 4.4.5 yakni halaman reset password terdapat kolom untuk memasukkan email, yang mana apabila user memasukkan email yang terdaftar maka akan ditampilkan pesan keberhasilan mengirim link reset password seperti pada gambar 4.4.6 dan juga

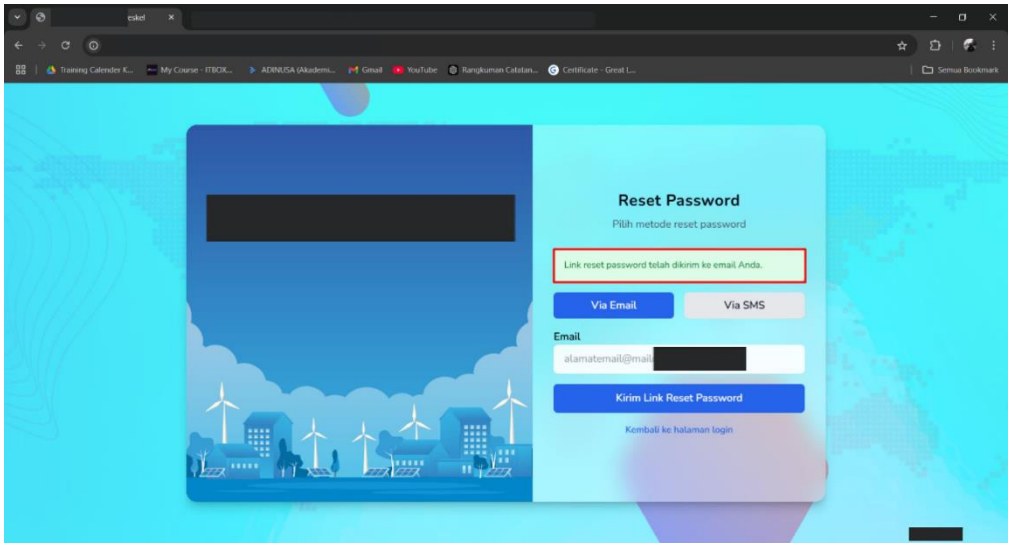
gambar 4.4.8 yakni pengguna yang menerima email reset password kemudian apabila email tidak terdaftar maka akan ditampilkan pesan gagal seperti yang di tampilkan pada gambar 4.4.7



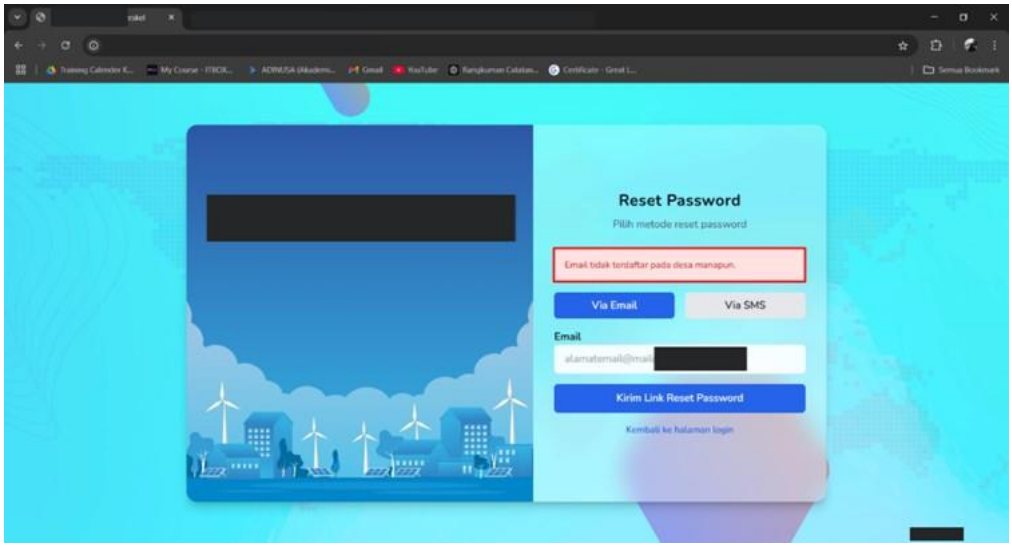
Gambar 4.2.25 Proses Reset Password 2 (Masukkan Email Valid)

d. **Email Valid?:** Sistem memeriksa apakah email yang dimasukkan valid.

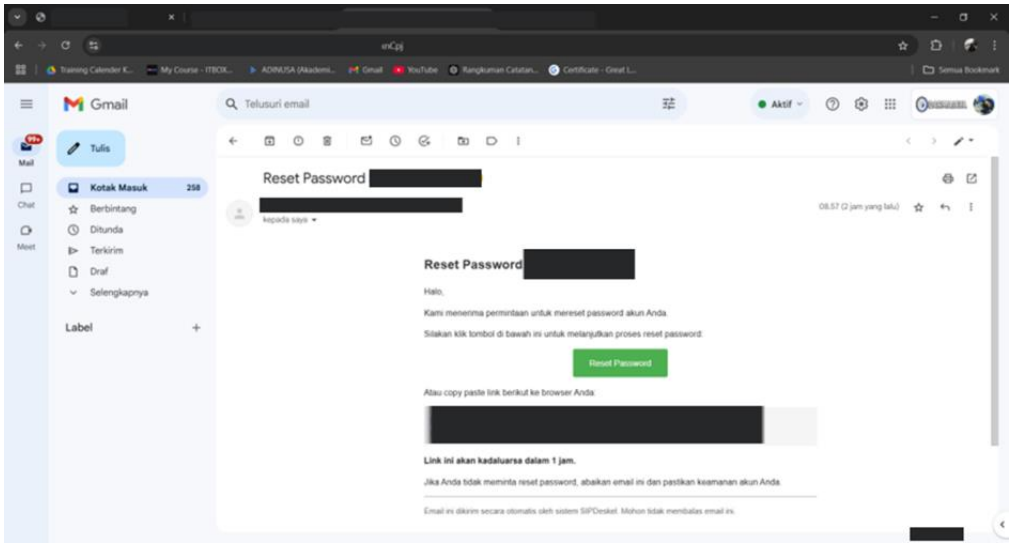
   Jika email tidak valid, sistem menampilkan pesan "Email tidak terdaftar". Tetapi jika email valid, sistem mengirimkan link untuk mereset password.



Gambar 4.2.26 Proses Reset Password 3 (Email Valid)



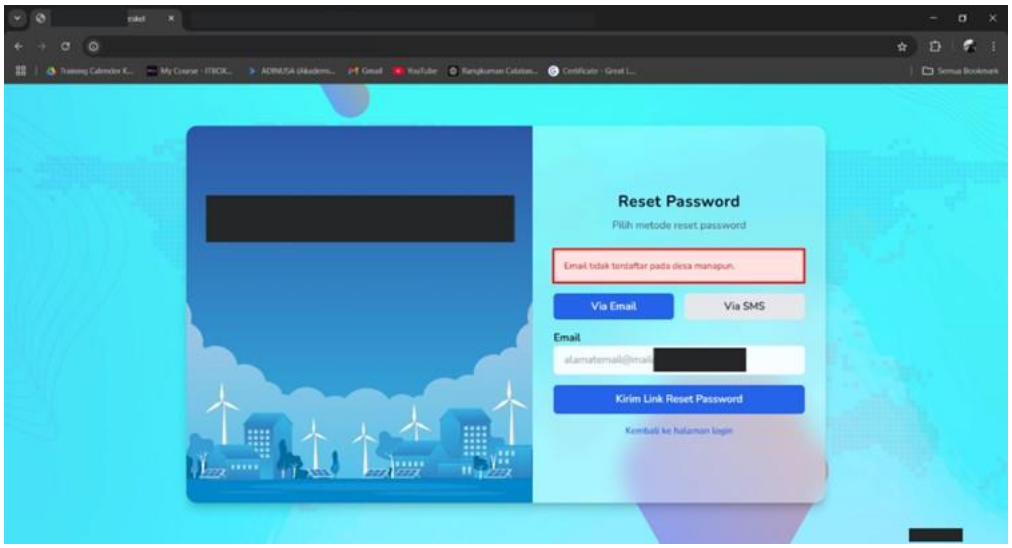
Gambar 4.2.27 Proses Reset Password 4 (Email Tidak Valid)



Gambar 4.2.28 Proses Reset Password 5 (Email terkirim)

e. **Masukkan Password Baru:** Pengguna diminta untuk memasukkan password baru.

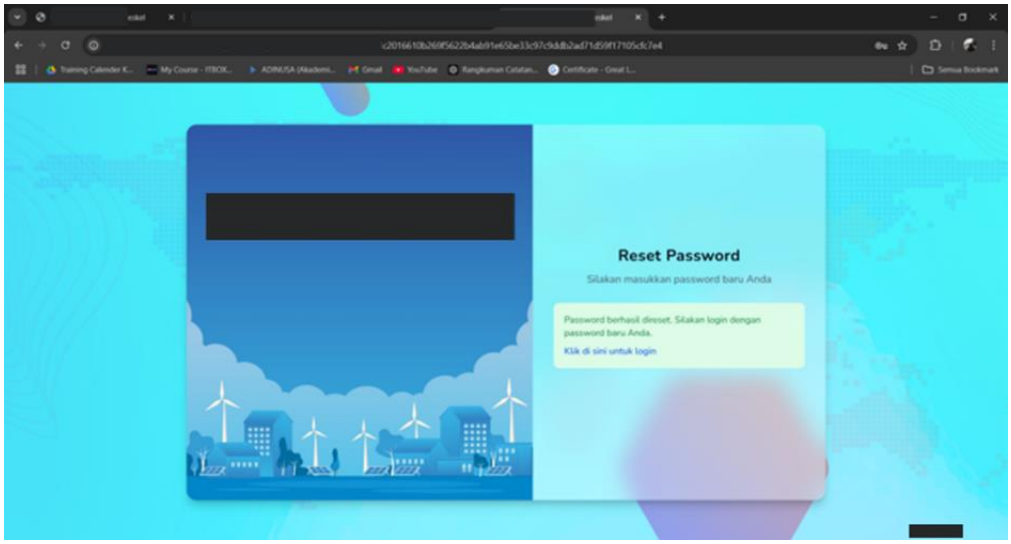
Link atau tombol yang dikirimkan ke email user dan dibuka oleh user, maka user akan diminta untuk memasukkan password baru dan konfirmasi password seperti pada gambar 4.4.9



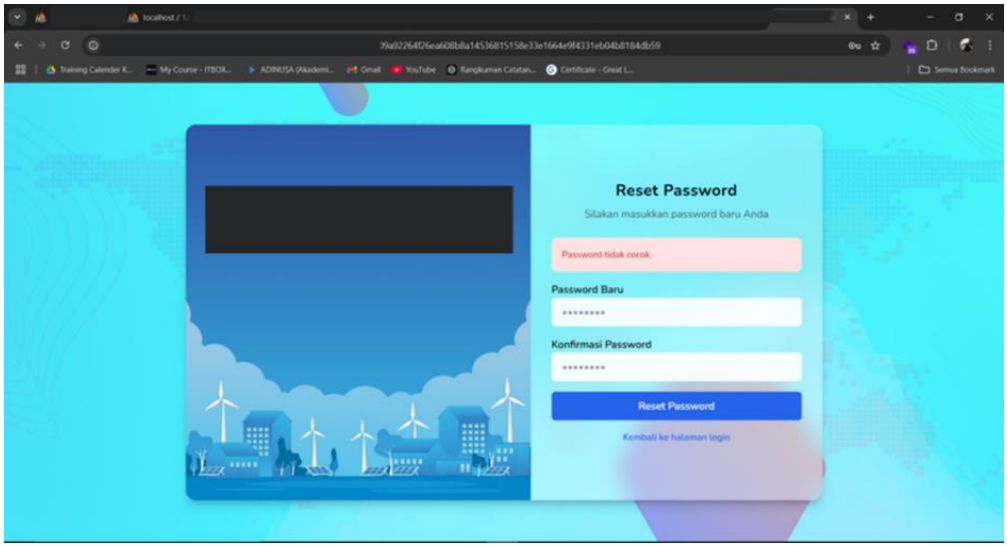
Gambar 4.2.29 Proses Reset Password 6 (Masukkan Password Baru)

f. Update Password: Password baru diperbarui dalam sistem.

Apabila Password berhasil diubah maka akan ditampilkan pesan seperti pada gambar 4.4.10. kemudian apabila password belum sesuai dengan ketentuan atau passsword tidak sesuai maka akan ditampilkan pesan gagal seperti pada gambar 4.4.11.



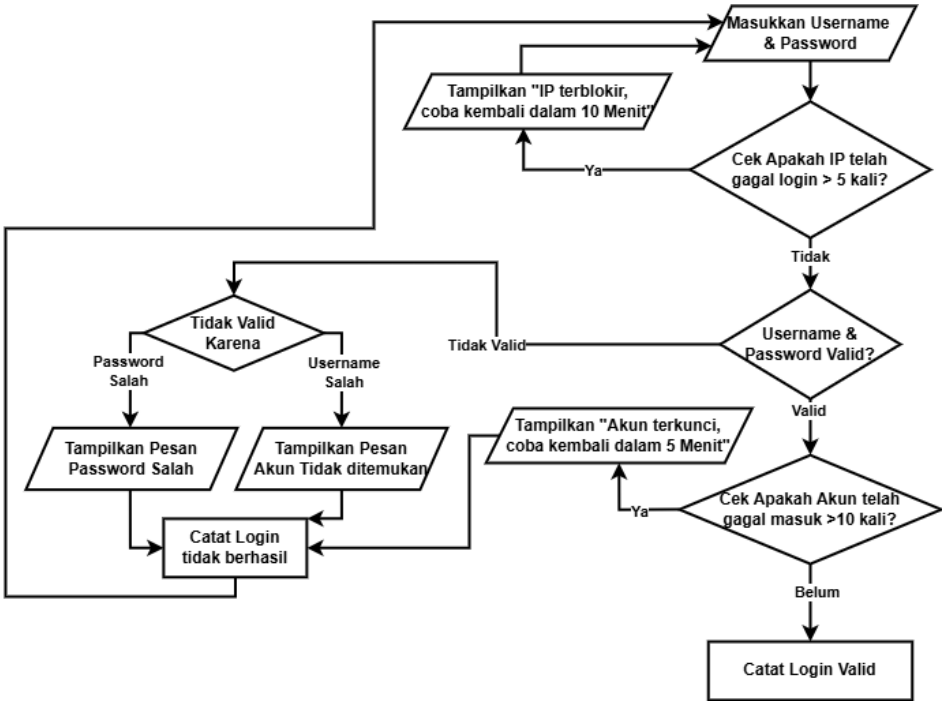
Gambar 4.2.30 Proses Reset Password 7 (Password diperbarui)



Gambar 4.2.31 Proses Reset Password 8 (Gagal)

2. **Implementasikan Login Attempt Throttling untuk membatasi jumlah percobaan login yang gagal.**

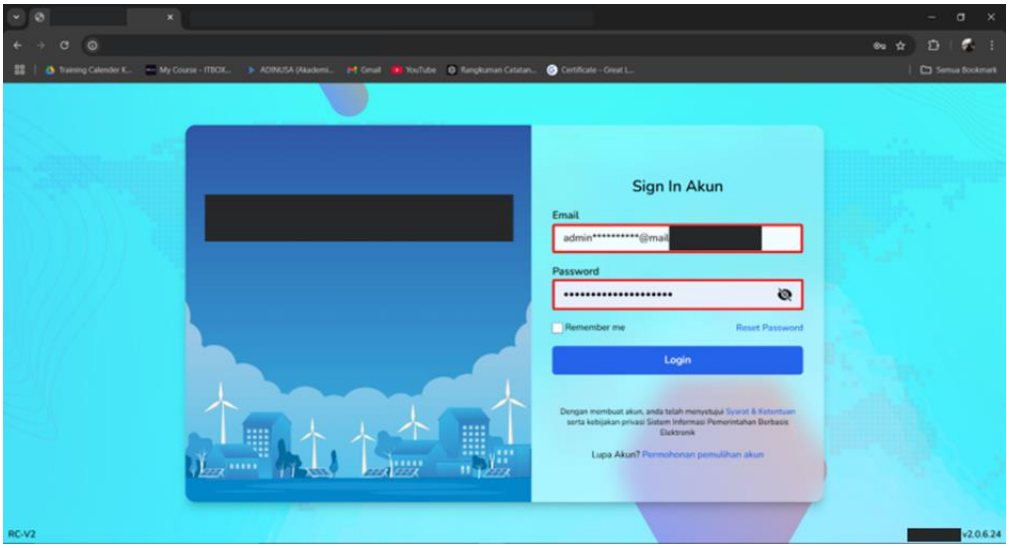
   Kemudian yang kedua yakni Implementasi Login Attempt Throttling. Hal ini untuk mitigasi potensi serangan *bruteforce* yang berpotensi melumpuhkan server website seperti yang terdapat pada tahap Pre-Engagement Interactions.



Gambar 4.2.32 Flowchart Login Attempt Throttling

a. **Input Username & Password**: Pengguna memasukkan kredensial login.

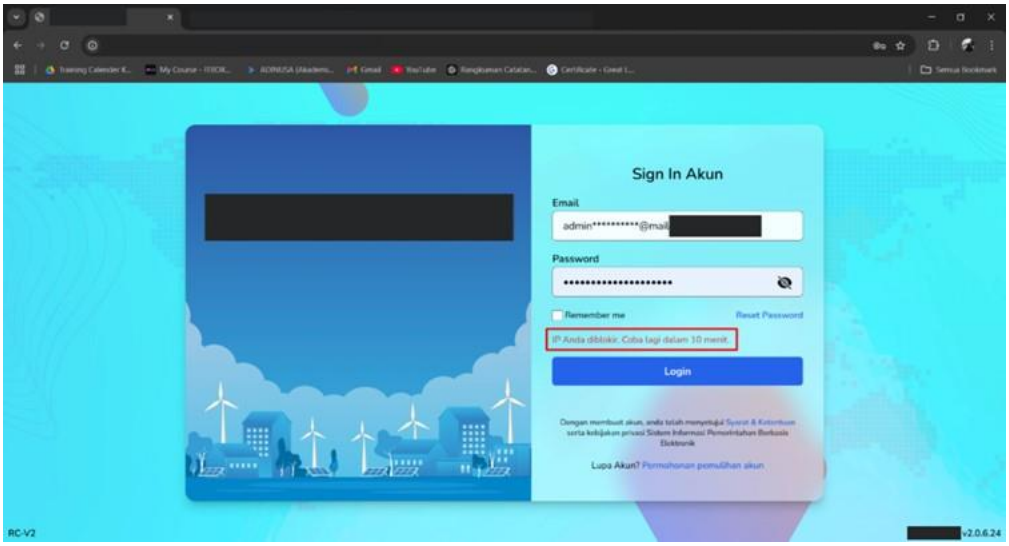
Proses Login Attempt Throttling dimulai dari halaman Login Website untuk melakukan input Username/Email dan juga Password seperti pada gambar 4.4.13 berikut ini.



Gambar 4.2.33 Proses Login Attempt Throttling 1 (Input Username & Password)

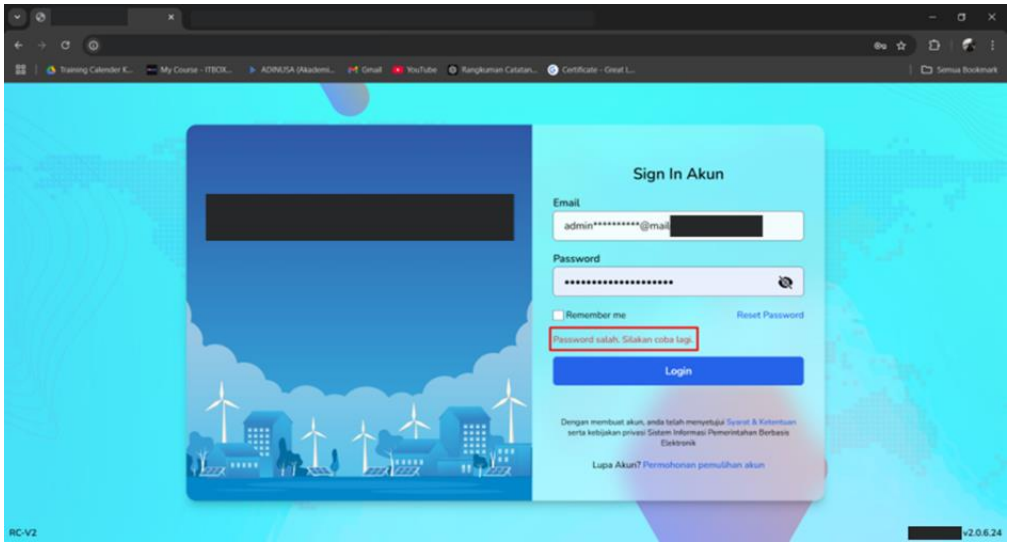
b. **Cek IP Address**: Jika IP sudah melakukan lebih dari 5 kali gagal login, maka pengguna diblokir selama 10 menit.

Proses Pengecekan IP Addres dilakukan pada sistem sehingga apabila sistem mendeteksi IP telah gagal login lebih dari 5 akan di tampilkan seperti pada gambar 4.4.14 berikut ini.



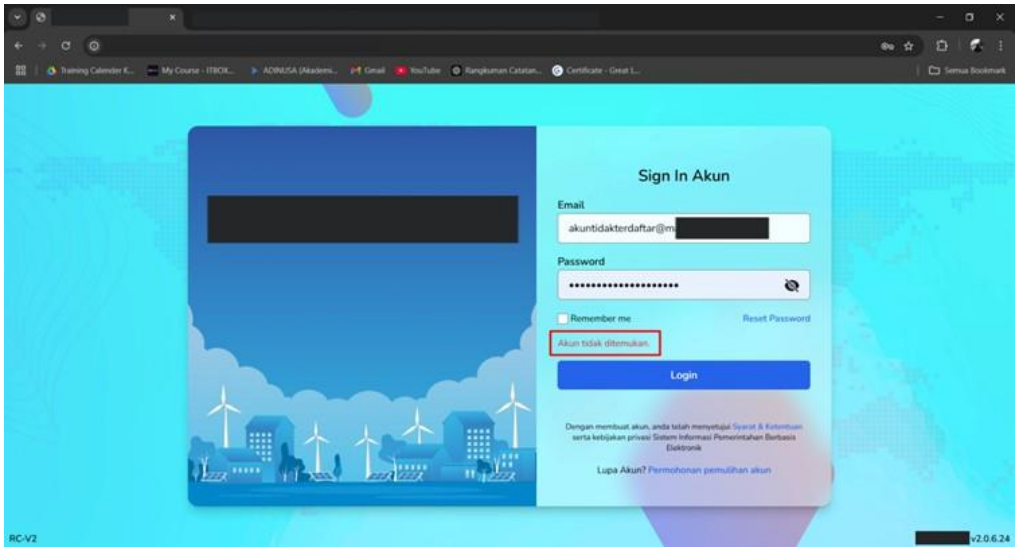
Gambar 4.2.34 Proses Login Attempt Throttling 2 (IP Terblokir)

c. **Validasi Kredensial**: Pada gambar 4.4.15 dan 4.4.16 sistem memeriksa apakah username dan password valid. Jika valid, lanjut ke langkah berikutnya. Dan jika tidak valid: **Password salah**: Tampilkan pesan "Password Salah."



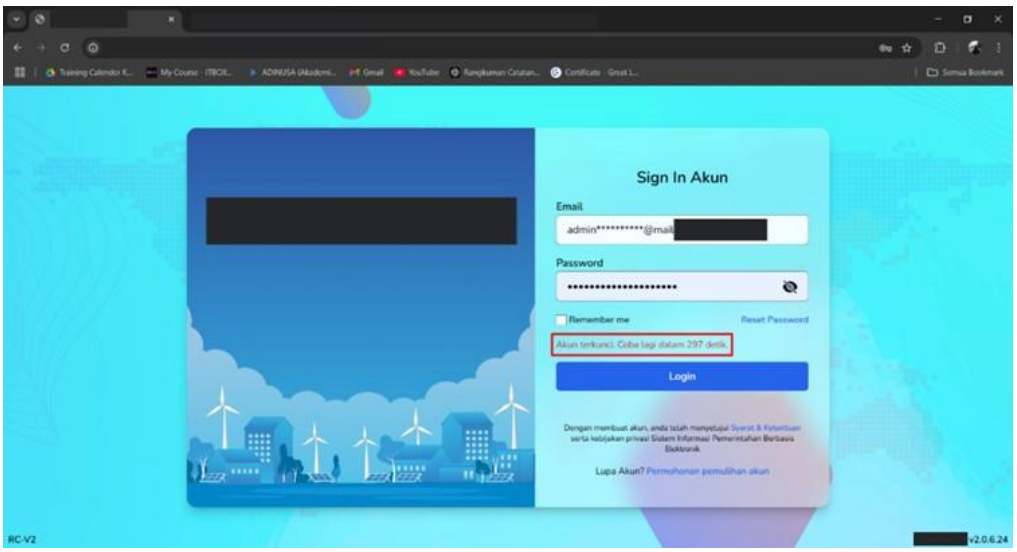
Gambar 4.2.35 Proses Login Attempt Throttling 3 (Password Salah)

Username salah: Tampilkan pesan "Akun Tidak Ditemukan." Catat bahwa login gagal.



Gambar 4.2.36 Proses Login Attempt Throttling 4 (Akun Tidak Ditemukan)

d. **Cek Akun Terkunci**: Jika akun gagal login lebih dari 10 kali, akun terkunci selama 5 menit. Yang akan ditampilkan dibawah tombol "Remember Me" seperti yang terdapat pada gambar 4.4.17.



Gambar 4.2.37 Proses Login Attempt Throttling 5 (Akun Terkunci)

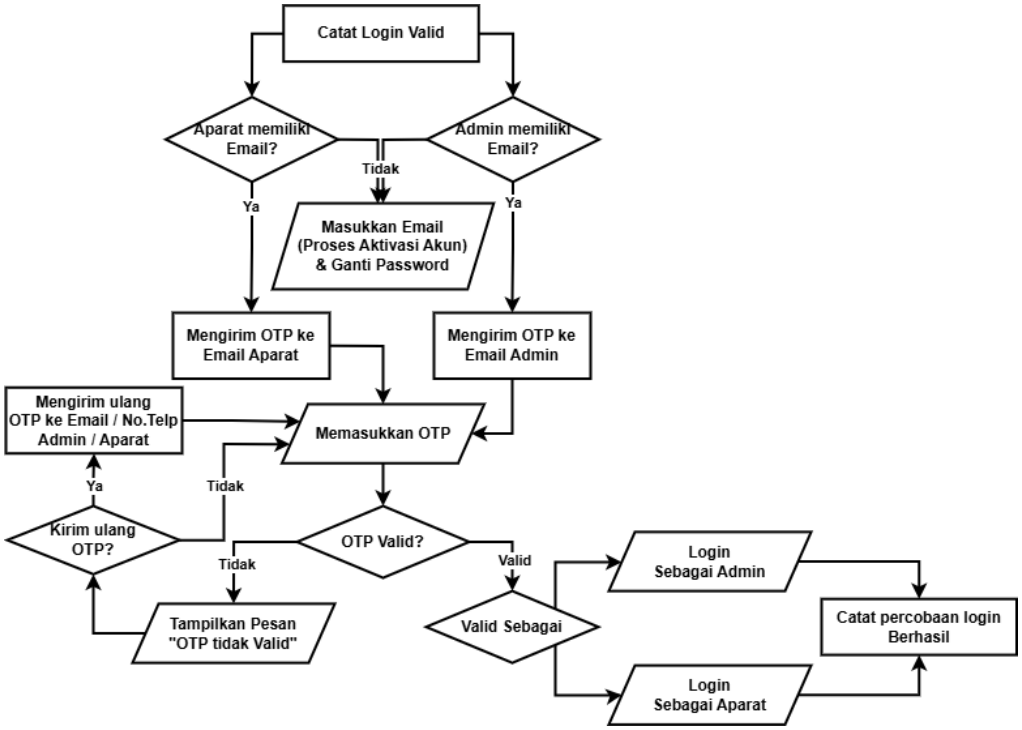
e. **Catat Login**:

Jika semua validasi terpenuhi, login berhasil dicatat diarahkan ke Halaman berikutnya yakni OTP atau Aktivasi akun (apabila akun belum teraktivasi).

Jika gagal, sistem mencatat login tidak berhasil.

3. Terapkan Multi-Factor Authentication (MFA) pada sistem login.

Penerapan Multi-Factor Authentication (MFA) pada mitigasi kerentanan sistem keamanan juga dapat diimplementasikan. Hal ini dikarenakan terdapat kerentanan seperti yang sudah diidentifikasi pada tahap *Threat Modelling* yakni Insider Attack. Gambar 4.4.18 akan menjelaskan bagaimana alur mitigasi ini berjalan.

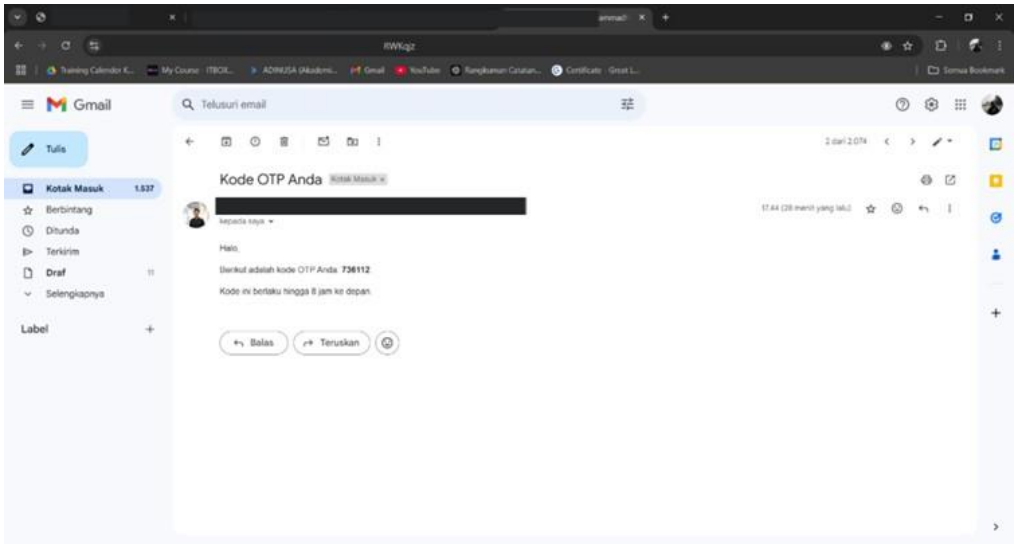


Gambar 4.2.38 Flowchart MFA (TOTP)

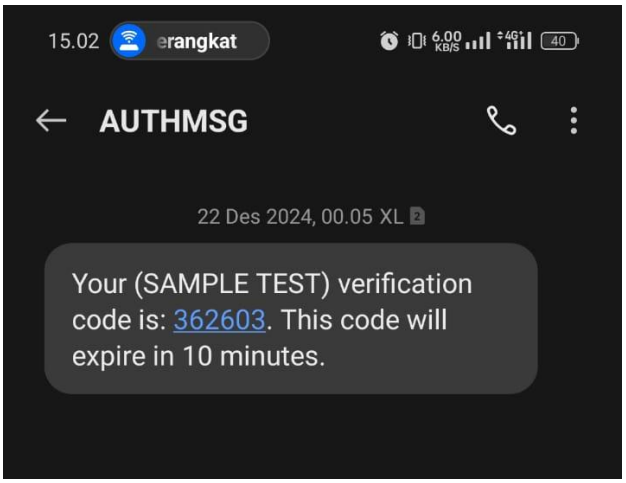
a. **Catat Login Valid**: Setelah kredensial login valid, sistem menentukan peran pengguna (Aparat atau Admin).

b. **Email Tersedia**:

Jika **Aparat memiliki email**: Sistem mengirimkan OTP ke email Aparat. Jika **Admin memiliki email**: Sistem mengirimkan OTP ke email Admin. Dan Jika tidak, pengguna diarahkan untuk memasukkan email guna aktivasi akun dan mengganti password.



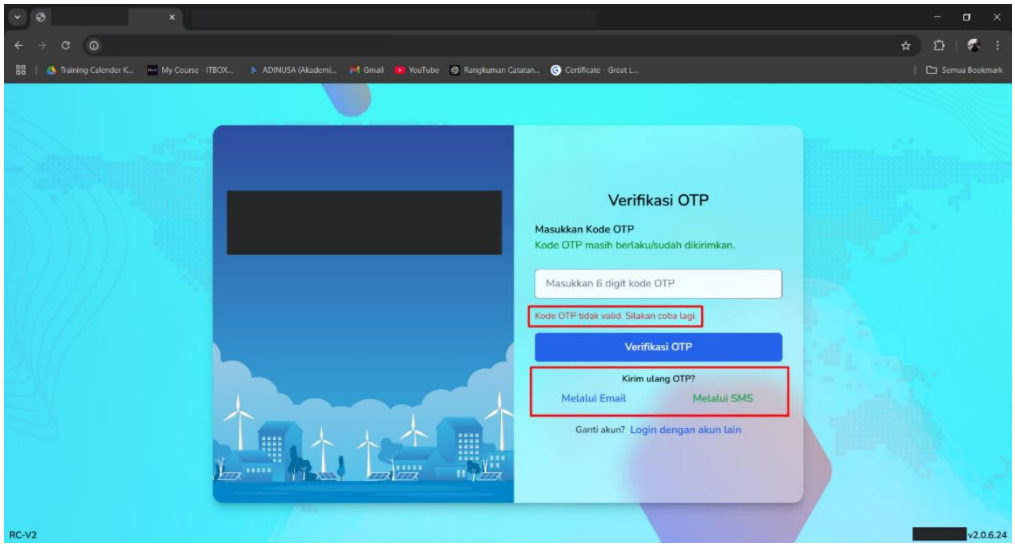
Gambar 4.2.39 Proses OTP 1
(Pengiriman kode OTP ke Email Admin/Aparat)



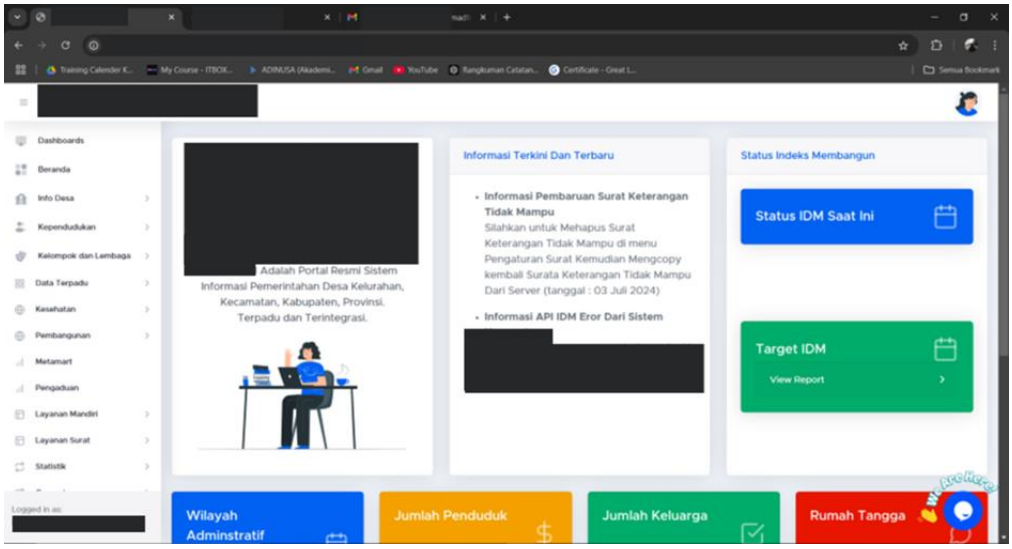
Gambar 4.2.40 Proses OTP 2
(Opsi Pengiriman kode OTP ke No. Telp)

c. Proses Validasi OTP

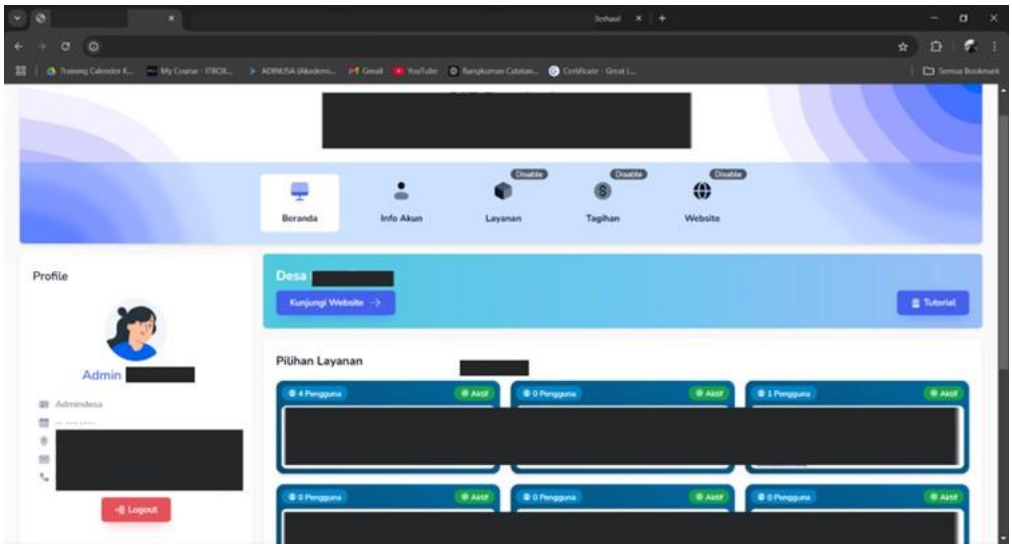
Pengguna memasukkan OTP yang diterima pada halaman OTP seperti pada gambar 4.4.21, Jika OTP tidak valid, pengguna diberi opsi untuk meminta pengiriman ulang OTP baik melalui Email atau SMS, Jika OTP valid, sistem menentukan pengguna login sebagai Aparat yang terlihat pada gambar 4.4.22 atau Admin pada gambar 4.4.23.



Gambar 4.2.41 Proses OTP 3 (OTP salah)



Gambar 4.2.42 Proses OTP 4 (Login Sebagai Aparat)



Gambar 4.2.43 Proses OTP 5
(Login Sebagai Admin)

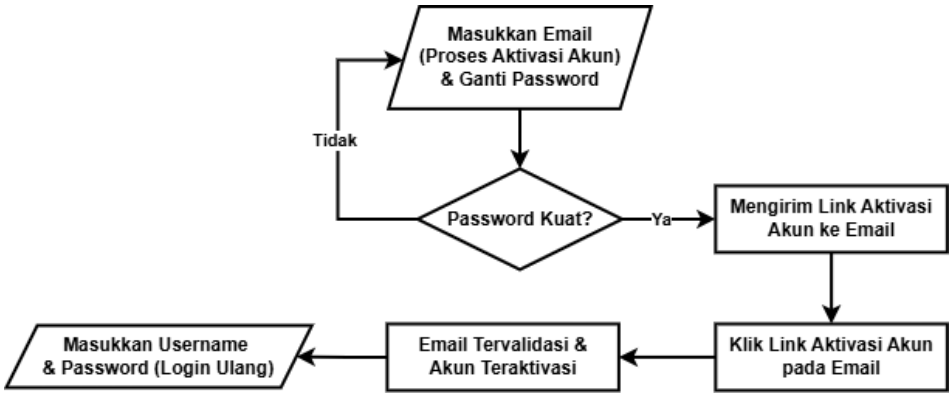
d. Login Berhasil:

Setelah validasi peran berhasil seperti yang terdapat pada gambar 4.4.22 dan 4.4.23, sistem mencatat percobaan login berhasil sesuai dengan peran pengguna.

B. Pengelolaan Akun

1. Fitur Wajib Ganti Password Default

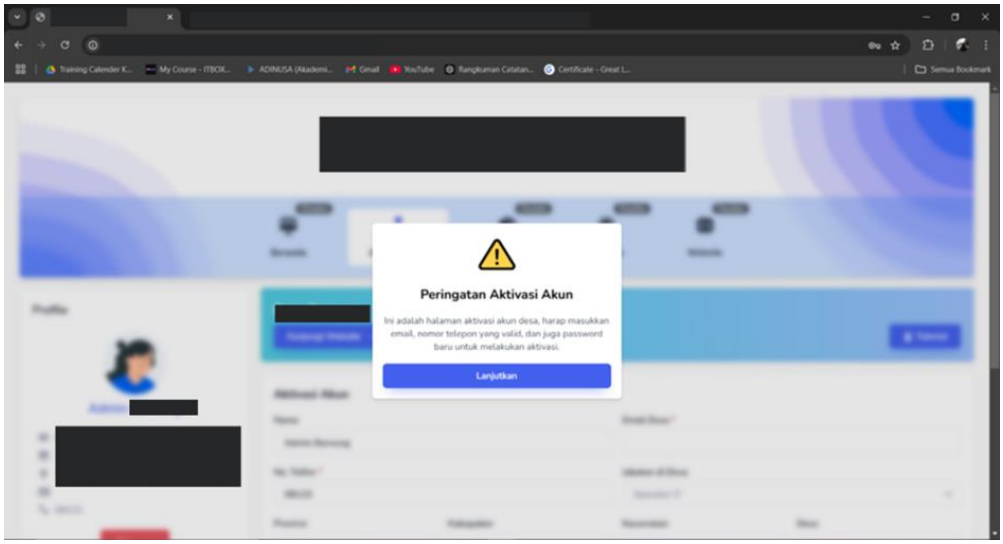
Terapkan fungsi yang mewajibkan user untuk mengganti password password default dengan kombinasi yang lebih kompleks dan unik untuk setiap akun. Adapun penjelasan mengenai alur dari Proses Mitigasinya terdapat pada gambar 4.4.24.



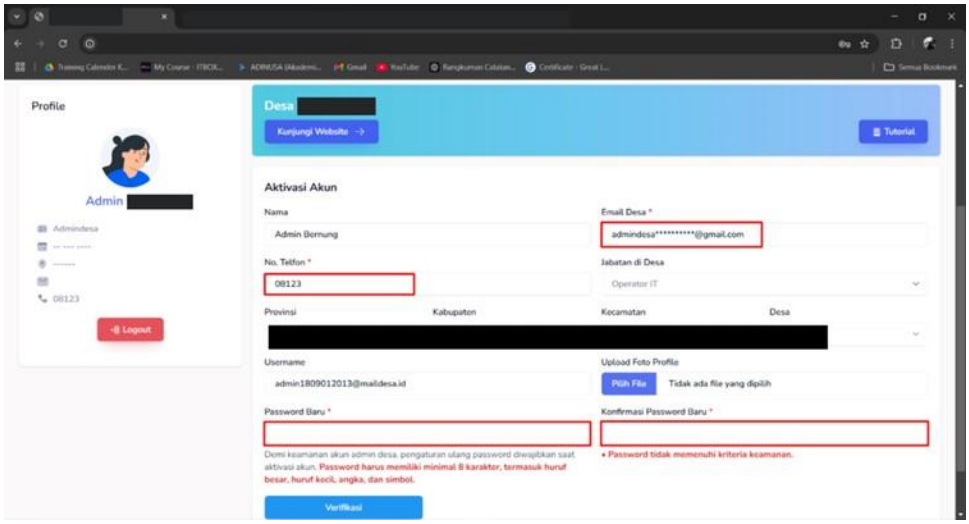
Gambar 4.2.44 Flowchart Mekanisme Wajib Ganti Password

b. **Proses Aktivasi dan Ganti Password**:

Setelah memasukkan username dan password default dari akun Pengguna yang terdapat pada halaman login berikutnya memasukkan email untuk memulai aktivasi akun dan mengganti password seperti pada gambar 4.4.26 yang sebelumnya diberikan peringatan terlebih dahulu pada gambar 4.4.25 untuk memberitahukan kepada aparat atau admin desa yang sedang melakukan Aktivasi Akun.



Gambar 4.2.45 Proses Aktivasi Akun 1 (Peringatan Aktivasi Akun)

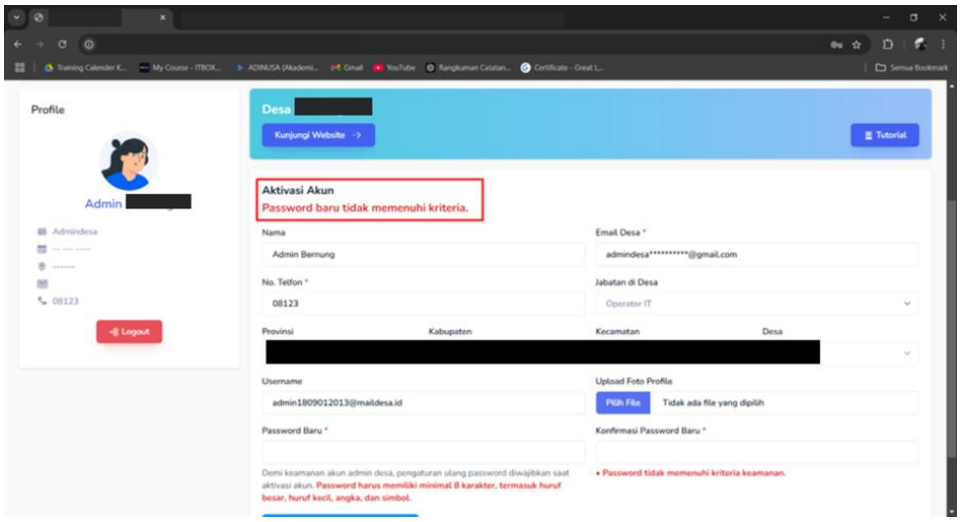


Gambar 4.2.46 Proses Aktivasi Akun 2
(Input Email dan Password yang kuat)

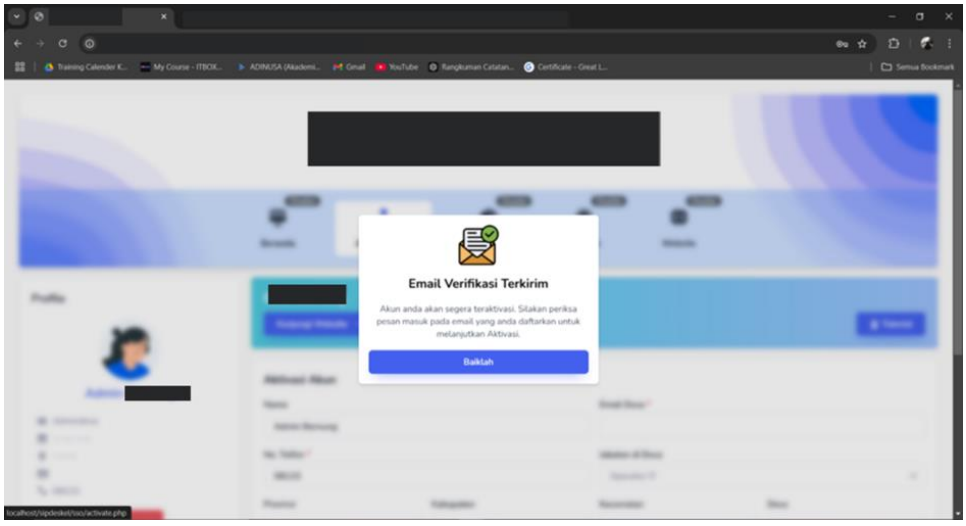
c. **Cek Kekuatan Password**:

Pada gambar 4.4.27 adalah visualisasi pesan Jika password tidak kuat atau tidak memenuhi kriteria. Kriteria password yang diizinkan untuk digunakan yakni password harus memiliki minimal 8 karakter, termasuk huruf besar, huruf kecil, angka, dan

simbol, serta harus cocok dengan kolom konfirmasi password. Pengguna diminta untuk mengulang proses penggantian password. Jika password kuat dan dilanjutkan, maka sistem akan mengirimkan link aktivasi akun ke email pengguna dengan memunculkan pesan notifikasi berupa email verifikasi berhasil terkirim seperti pada gambar 4.4.27.



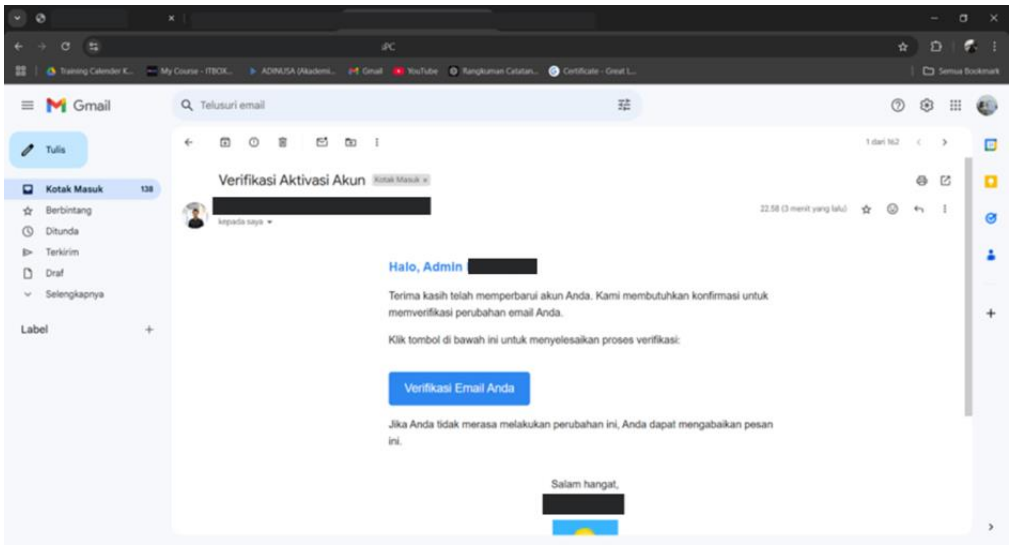
Gambar 4.2.47 Proses Aktivasi Akun 3 (Pemberitahuan password Tidak Kuat)



Gambar 4.2.48 Proses Aktivasi Akun 4 (Email Verifikasi Terkirim)

d. **Klik Link Aktivasi**:

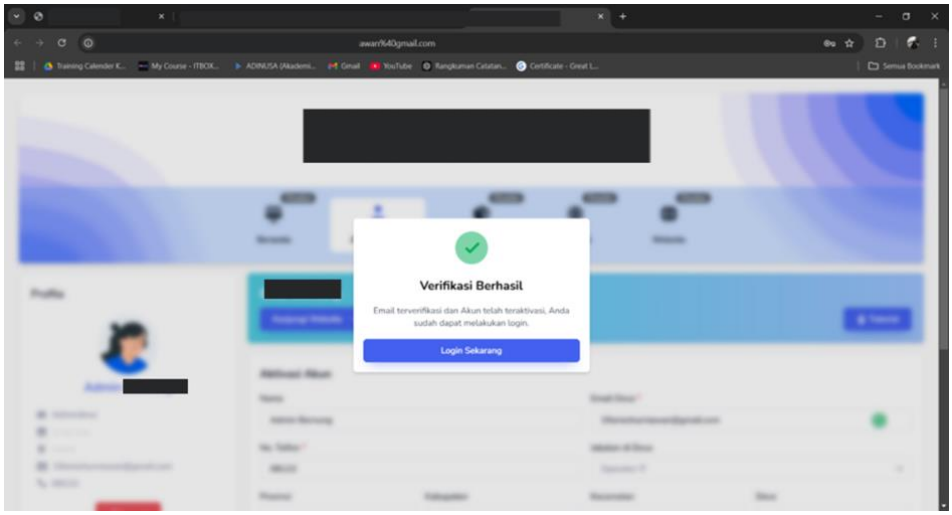
Email yang diterima oleh user akan memberikan tombol verifikasi akun yang tertera pada gambar 4.4.29 sehingga apabila di klik pengguna akan diarahkan ke halaman khusus untuk menampilkan keberhasilan verifikasi akun seperti pada gambar 4.4.30.



Gambar 4.2.49 Proses Aktivasi Akun 5
(Klik Verifikasi Akun pada Email)

e. **Akun Teraktivasi**:

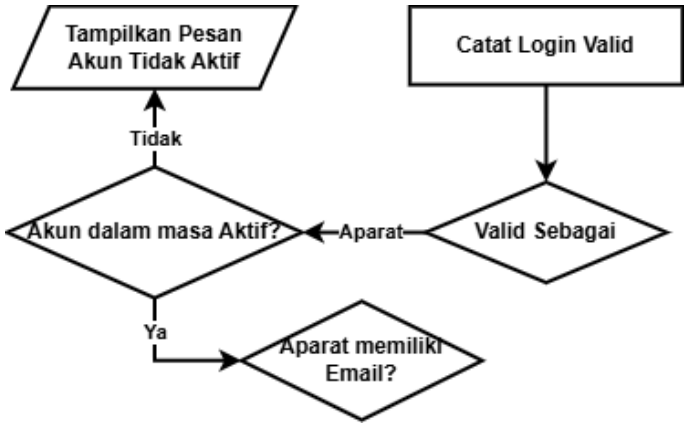
Setelah email tervalidasi dan akun teraktivasi, pengguna diminta untuk login ulang dengan username dan password yang telah diatur.



Gambar 4.2.50 Proses Aktivasi Akun 6 (Verifikasi Berhasil)

2. **Tetapkan kebijakan masa berlaku untuk akun yang tidak aktif (khusus untuk akun Aparat).**

   Berikutnya untuk menanggulangi serangan Insider Attack, juga di rekomenadikan penerapan mitigasi berupa pemberian masa berlaku akun level aparat yang memiliki masa berlaku, sehingga apabila masa tugas telah usai, pengguna tidak dapat masuk dengan kredensial yang valid pada saat masa berlaku. Alur proses dari mitigasi ini terdapat pada gambar 4.4.31.



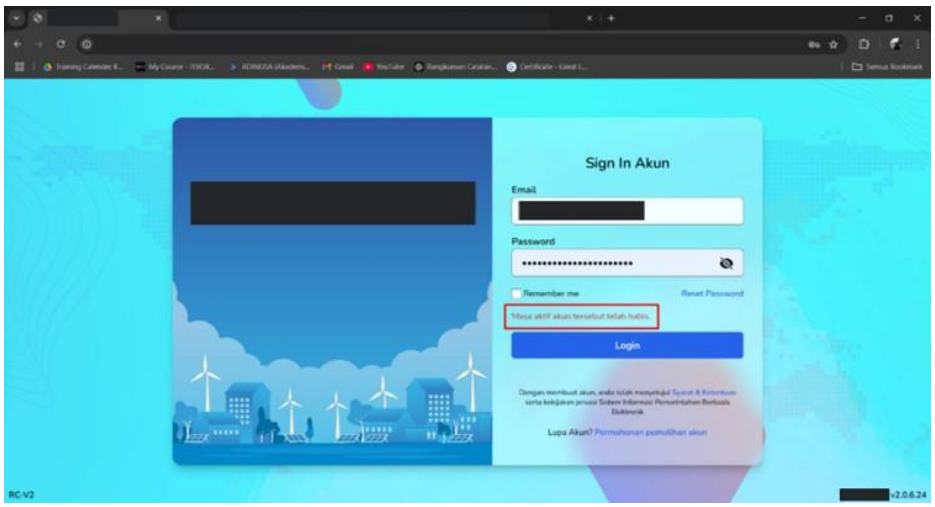
Gambar 4.2.51 Flowchart Masa berlaku Akun Aparat

a. **Catat Login Valid**:

Setelah login dinyatakan valid, sistem melanjutkan proses validasi status akun.

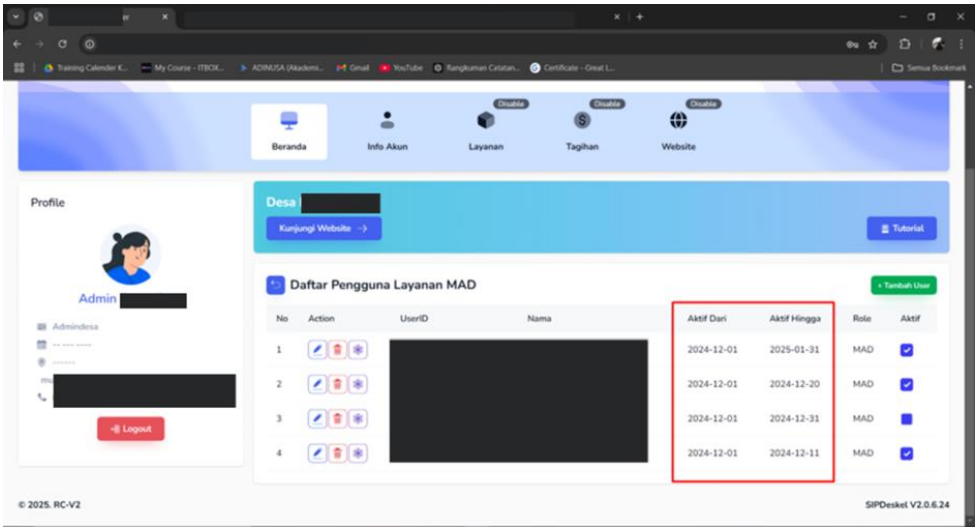
b. **Cek Status Akun**:

Jika akun tidak dalam masa aktif, sistem menampilkan pesan "Masa aktif akun tersebut telah habis." Seperti yang tertera pada gambar 4.4.32. Dan jika akun aktif, proses dilanjutkan dengan pengecekan email berdasarkan peran (Aparat).



Gambar 4.2.52 Pemrosesan Akun tidak Aktif

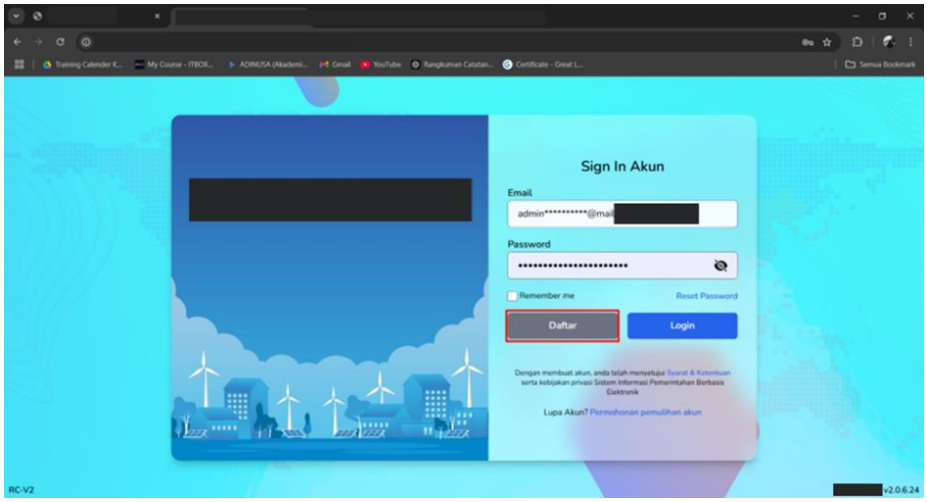
Adapun Pengelolaan masa aktif dilakukan oleh Admin melalui Dashboard dengan menambahkan pencatatan Masa Aktif dan Pengaktifan fitur status Aktif pada checklist masing masing Akun Aparat yang dikelolanya, khususnya di halaman pengelolaan akun aparat seperti pada gambar 4.4.33.



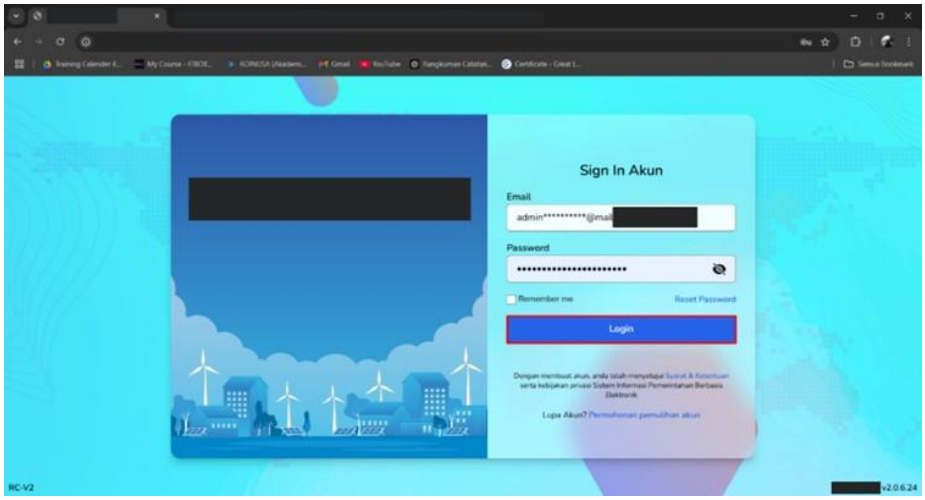
Gambar 4.2.53 Pembatasan Masa Aktif Akun Aparat oleh Admin Desa

c. Hilangkan tombol menuju halaman Pendaftaran

pada halaman login jika tidak diperlukan untuk mencegah kebocoran informasi. Tombol Pendaftaran sebelumnya terdapat pada halaman login yang mana sebenarnya tombol tersebut tidak berfungsi seperti berdasarkan pada tahap 3.3 *Intelligence Gathering.* Seperti pada gambar 4.4.34 yang masih menampakkan tombol “Daftar” yang mengarahkan ke halaman Pendaftaran, menjadi seperti pada gambar 4.4.35 yang menghilangkan tombol tersebut untuk mencegah kebocoran username seperti yang dijelaskan pada gambar 3.3.1.



Gambar 4.2.54 Penghilangan Tombol Daftar pada halaman Login (sebelum)

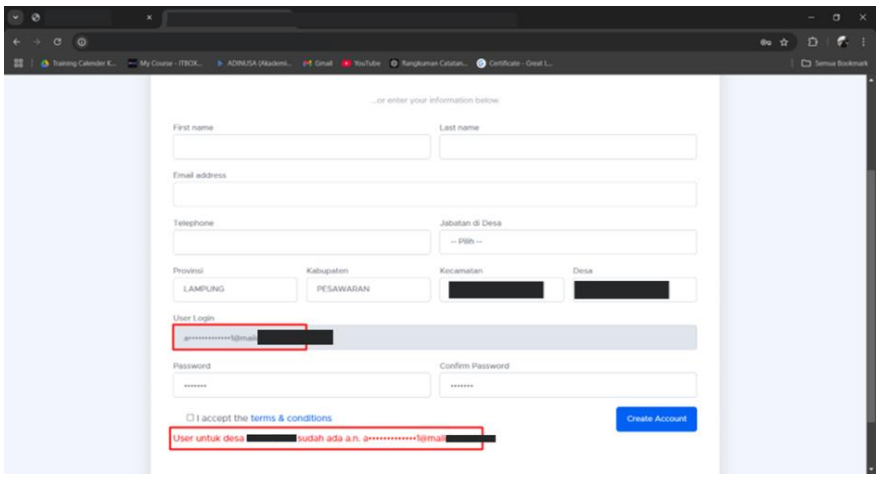


Gambar 4.2.55 Penghilangan Tombol Daftar pada Halaman Login (sesudah)

3. **Sembunyikan halaman "Pendaftaran" atau lakukan masking pada username apabila diperlukan.**

   Menyembunyikan halaman Pendaftaran bisa dengan mengganti alamat halaman sedangkan pemberian masking pada username yang bocor juga dapat efektif supaya menyembunyikan karakter sehingga

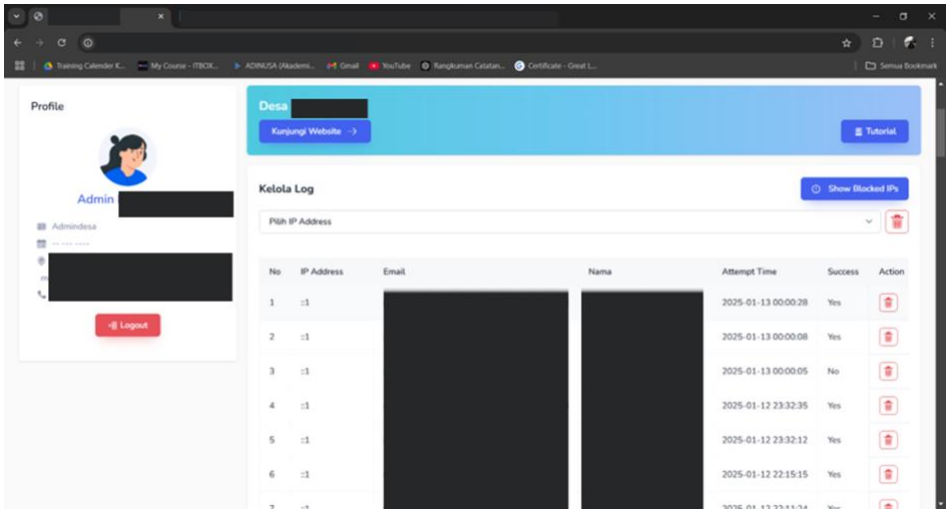
username yang muncul (apabila masih diperlukan) tidak memunculkan username yang asli seperti yang terdapat pada gambar 4.4.36.



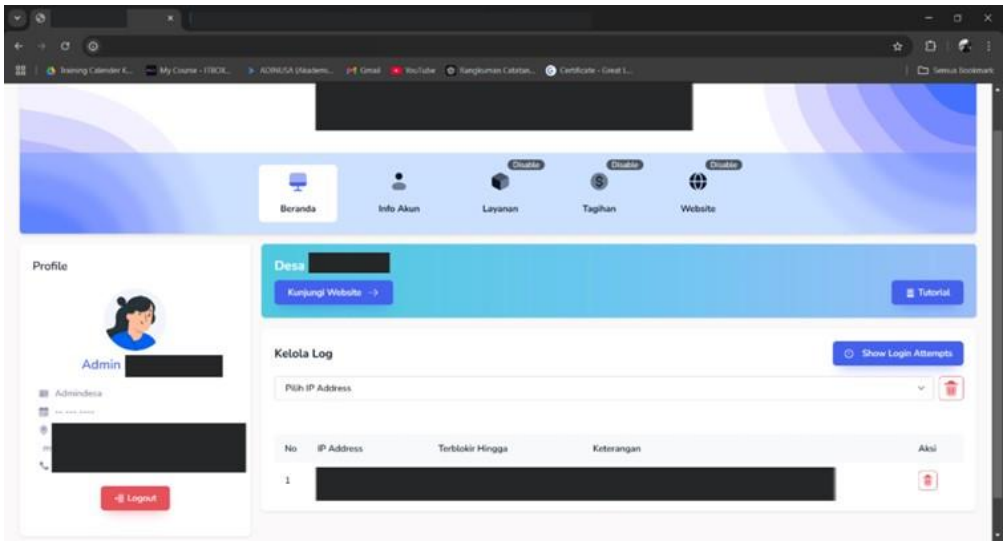
Gambar 4.2.56 Masking Username pada Halaman Pendaftaran

4. Monitoring dan Pendeteksian

Gambar 4.4.37 merupakan visualisasi dari rekomendasi sistem pemantauan aktivitas login *(logging)* untuk mendeteksi aktivitas mencurigakan dan menerapkan *Non-Repudiation*.Serta pada gambar 4.4.38 juga ditampilkan IP yang terblokir untuk memungkinkan Admin Desa mendapatkan informasi dari IP yang mencurigakan (gagal melakukan login sebanyak 5 kali).



Gambar 4.2.57 Halaman Monitoring dan Pendeteksian oleh Admin Desa



Gambar 4.2.58 Halaman Monitoring dan Pengelolaan IP yang terblokir oleh sistem

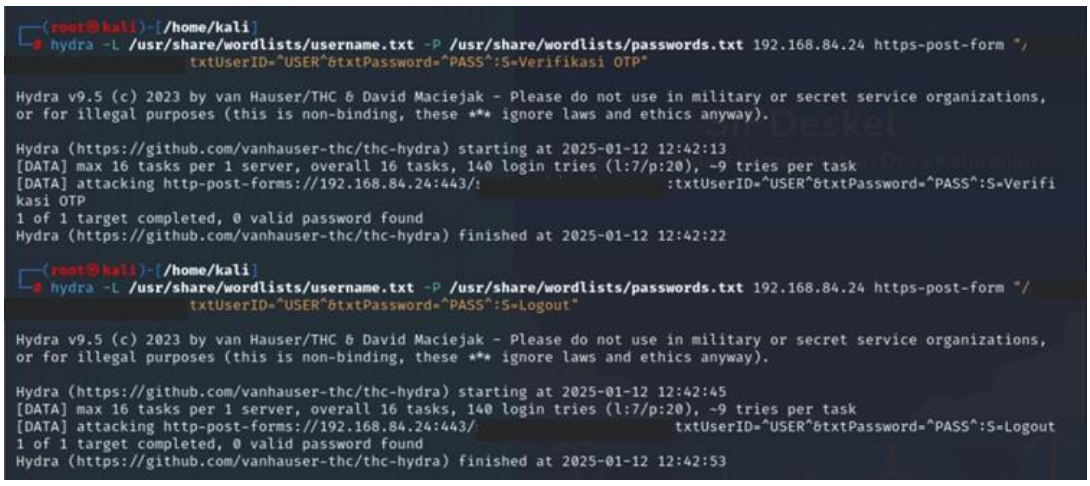
C. Edukasi dan Kesadaran Keamanan

Berdasarkan tahap *Pre-Engagement Interactions* terdapat kesimpulan bahwa masih kurangnya Arahan mengenai Keamanan yang ada pada sistem Website Desa, sehingga berikut ini adalah rekomendasi mitigasi untuk masalah ini.

a. Lakukan pelatihan kepada operator desa mengenai pentingnya menjaga keamanan akun. Meskipun pelatihan telah dilakukan, fokusnya lebih kepada fitur Manajemen Administrasi Desa dan tidak membahas aspek keamanan. Oleh karena itu, penting untuk memberikan edukasi tambahan mengenai keamanan akun.
b. Edukasi pengguna tentang praktik terbaik dalam membuat dan menjaga password, serta pentingnya tidak membagikan kredensial login kepada pihak lain.
c. Berikan edukasi khusus mengenai fitur pengelolaan akun aparat desa, sehingga akses akun admin desa hanya dimiliki oleh admin desa itu sendiri. Hal ini penting untuk mencegah penyalahgunaan akses dan menjaga integritas data desa.

5. Percobaan Pengujian Hybrid Attack setelah penerapan Mitigasi pada MockUP

Setelah penerapan mitigasi yang direkomendasikan, dilakukan pengujian untuk mengevaluasi ketahanan sistem terhadap serangan *hybrid attack* menggunakan *Hydra*. Berikut pada gambar 4.4.39 adalah hasil pengujiannya.



Gambar 4.2.59 Percobaan *Hybrid Attack* setelah penerapan Mitigasi

A. Analisis Hasil Pengujian:

a. Jumlah Percobaan Login: 140 percobaan login dilakukan dengan kombinasi username dan password yang telah ditentukan.

b. Hasil: Tidak ada password valid yang ditemukan, menunjukkan bahwa mitigasi yang diterapkan, seperti penerapan *Multi-Factor Authentication* (MFA) dan *Login Attempt Throttling*, berhasil meningkatkan keamanan sistem terhadap serangan brute force.

Tabel 4.4.1 berikut berisi ringkasan dari Tahap Reporting yang terdiri dari Kelemahan dan Rekomendai Mitigasinya.

Tabel 4.2.3 Hasil Mitigasi

No.	Kelemahan	Mitigasi
1.	Tidak adanya masa expire akun	Tetapkan kebijakan masa berlaku untuk akun yang tidak aktif (khusus untuk akun Aparat). Mengurangi risiko akun yang tidak terpakai tetap aktif dan dapat disalahgunakan.
2.	Password yang mudah ditebak	Terapkan fungsi yang mewajibkan user untuk mengganti password default dengan kombinasi yang lebih kompleks dan unik untuk setiap akun. Meningkatkan kekuatan password dan mengurangi kemungkinan akses tidak sah.
3.	Tidak ada pembatasan login (Login Attempt Throttling)	Implementasikan Login Attempt Throttling untuk membatasi jumlah percobaan login yang gagal. Mengurangi risiko serangan brute force dengan membatasi upaya login yang berlebihan.

4.	Perpaduan Insider Attack dan Dictionary Attack	Terapkan Multi-Factor Authentication (MFA) pada sistem login. Meningkatkan keamanan login dengan menambahkan lapisan perlindungan tambahan.
5.	Fitur “Reset Password” yang tidak berfungsi	Perbaiki fitur "Reset Password" agar dapat digunakan untuk pemulihan akses. Memastikan pengguna dapat memulihkan akses ke akun mereka dengan aman dan efisien.
6.	Potensi kebocoran informasi	Hilangkan tombol menuju halaman Pendaftaran pada halaman login jika tidak diperlukan. Mencegah penyerang dari mendapatkan informasi lebih lanjut tentang sistem.
7.	Informasi username terlihat	Sembunyikan halaman “Pendaftaran” atau lakukan masking pada username apabila diperlukan. Mengurangi kemungkinan penyerang untuk menebak username yang valid.

Pada tabel 4.4.1 terdapat 7 Mitigasi yang direkomendasikan untuk diterapkan untuk meningkatkan sistem keamanan pada Website Desa berdasarkan 7 kerentanan atau kelemahan yang diidentifikasi.

Penetration testing yang dilakukan pada penelitian ini tidak menggunakan perangkat otomatis seperti penggunaan tools Accunetix, melainkan menggunakan pengecekan manual, hal ini tentu tidak efektif untuk sistem yang lebih besar karena diperlukan waktu yang cukup lama.

Setelah menerapkan model Waterfall dalam pengembangan Website Desa, integrasi metode Penetration Testing Execution Standard (PTES) terbukti efektif dalam meningkatkan keamanan sistem. Meskipun Waterfall terdiri dari lima tahap, pengujian keamanan dengan PTES difokuskan pada tiga tahap utama. Pada tahap Requirement, dilakukan Pre-Engagement Interactions untuk memahami kebutuhan dan ruang lingkup pengujian. Tahap Design mencakup Intelligence Gathering, Threat Modeling, dan Vulnerability Analysis guna mengidentifikasi serta menganalisis potensi risiko keamanan. Kemudian, pada tahap Implementation, dilakukan Exploitation dan Post-Exploitation untuk menguji serta mengevaluasi kelemahan sistem, diakhiri dengan tahap Reporting untuk mendokumentasikan temuan dan rekomendasi perbaikan. Dengan pendekatan ini, pengembangan Website Desa Ini menjadi lebih aman, memastikan bahwa sistem tidak hanya berfungsi dengan baik tetapi juga terlindungi dari ancaman keamanan sebelum diterapkan secara penuh.