**PROTOKOL OTORISASI DAN OTENTIKASI PADA WEB STATIS**

*1Rolly Maulana Awangga,2Muhammad Yusril Helmi Setyawan, 3Muhammad Rifqi Daffa Ulhaq*

*123Teknik Informatika Universitas Logistik dan Bisnis Internasional*

*Jl. Sariasih No.54, Sarijadi, Kota Bandung 40151, Jawa Barat*

[1awangga@ulbi.ac.id,](mailto:1fitrianingsih@staff.gunadarma.ac.id,%20) [2yusrilhelmi@ulbi.ac.id,](mailto:2destimath@gmail.com,%20) [31204045@std.ulbi.ac.id](mailto:31204045@std.ulbi.ac.id)

**Abstrak**

*Keamanan dan efisiensi dalam pengembangan aplikasi web sangat penting dalam era digital. Penelitian ini mengimplementasikan skema autentikasi dan otorisasi yang aman pada website statis menggunakan metode autentikasi QR, autentikasi Google, dan Sandi Terenkripsi (STP). Teknologi yang digunakan meliputi Bcrypt untuk hashing password, MongoDB untuk penyimpanan data dengan pengaturan indexing pada field createdAt selama 5 menit, React untuk pengembangan client-side, serta pengiriman sandi melalui WhatsApp. Metode STP memanfaatkan popularitas WhatsApp untuk mengirim sandi login yang berlaku selama 5 menit, memudahkan adopsi oleh pengguna. Pengujian menunjukkan sistem tahan terhadap serangan brute force dan kamus, serta meningkatkan keamanan dan pengalaman pengguna pada website statis. Penelitian ini memberikan solusi praktis untuk meningkatkan keamanan web statis dengan metode yang efisien dan mudah diadopsi.*

***Kata Kunci****:* *Autentikasi, Otorisasi, Keamanan Web, Bcrypt, Web Statis.*

**Abstract**

*Security and efficiency in web application development are very important in the digital era. This research implements a secure authentication and authorization scheme on a static website using QR authentication, Google authentication, and Encrypted Password (STP) methods. The technologies used include Bcrypt for password hashing, MongoDB for data storage with indexing settings on the createdAt field for 5 minutes, React for client-side development, and sending passwords via WhatsApp. The STP method leverages the popularity of WhatsApp to send login passwords that are valid for 5 minutes, easing adoption by users. Tests show the system is resistant to brute force and dictionary attacks, and improves security and user experience on static websites. This research provides a practical solution to improve static web security with an efficient and easy-to-adopt method.*

***Key Words****:* *Authentication, Authorization, Web Security, Bcrypt, Static Web.*

**PENDAHULUAN**

Dalam era digital yang semakin maju, keamanan dalam pengembangan aplikasi web menjadi isu yang sangat krusial[1]. Menurut laporan dari Cybersecurity Ventures, kerugian global akibat kejahatan siber diperkirakan akan mencapai $10,5 triliun per tahun pada 2025[2]​​. Peningkatan signifikan ini menekankan urgensi untuk mengembangkan sistem keamanan yang lebih efektif dan efisien dalam melindungi data pengguna.

Web statis, yang memiliki konten tetap kecuali diperbarui oleh pengembang, sering digunakan untuk situs-situs yang menyajikan informasi statis seperti profil perusahaan, portofolio, atau dokumentasi[3]. Meskipun sederhana dan mudah dikelola, web statis tetap memerlukan mekanisme keamanan yang memadai untuk melindungi integritas data pengguna. Tantangan utama dalam web statis adalah kurangnya backend dinamis untuk memproses permintaan autentikasi secara real-time, yang membuat implementasi protokol otorisasi dan otentikasi menjadi lebih kompleks[4].

Otorisasi dan otentikasi pengguna adalah komponen kunci dalam menjaga integritas dan keamanan data di web[5]. Metode konvensional seperti OAuth2 dan Multi-Factor Authentication (MFA) sering digunakan untuk mengamankan aplikasi web dinamis, namun penerapannya pada web statis masih jarang dibahas[6]. OAuth2 memungkinkan aplikasi untuk mendapatkan akses terbatas ke sumber daya pengguna tanpa harus mengungkapkan kredensial pengguna[7], sementara MFA menambahkan lapisan verifikasi tambahan untuk meningkatkan keamanan[8].

Penelitian ini bertujuan untuk mengembangkan skema autentikasi dan otorisasi yang aman pada website statis dengan menggunakan berbagai metode seperti autentikasi QR, autentikasi Google, dan Sandi Terenkripsi (STP). Teknologi yang digunakan meliputi Bcrypt untuk hashing password, MongoDB untuk penyimpanan data dengan pengaturan indexing pada field createdAt selama 5 menit, React untuk pengembangan client-side, serta pengiriman sandi melalui WhatsApp untuk meningkatkan keamanan dan pengalaman pengguna. Penggunaan WhatsApp sebagai media pengiriman sandi dipilih karena popularitasnya yang tinggi di kalangan pengguna, sehingga memudahkan adopsi metode ini[9], [10].

Beberapa penelitian terdahulu telah membahas berbagai pendekatan dalam meningkatkan keamanan web. Misalnya, penelitian[11] yang mengeksplorasi penggunaan OAuth2 pada aplikasi web dinamis, dan studi[12] yang menunjukkan bagaimana OAuth2 dapat digunakan untuk mengamankan akses ke aplikasi web dengan memberikan hak akses terbatas tanpa mengungkapkan kredensial pengguna. Selain itu, penelitian[13], [14] menunjukkan bahwa penggunaan WhatsApp untuk autentikasi dua faktor dapat meningkatkan pengalaman pengguna dan keamanan data.

Metode Sandi Terenkripsi (STP) memanfaatkan popularitas WhatsApp untuk mengirim sandi login yang berlaku selama 5 menit. Pengujian yang dilakukan termasuk uji brute force dan serangan kamus, menunjukkan bahwa sistem yang dirancang mampu bertahan terhadap upaya pembobolan akun dan meningkatkan keamanan serta pengalaman pengguna pada website statis. Dengan menggabungkan berbagai metode autentikasi, penelitian ini diharapkan dapat memberikan solusi praktis dan efisien untuk meningkatkan keamanan web statis.

**METODE PENELITIAN**

Penelitian ini menggunakan metode eksperimental dengan tahapan yang sistematis untuk mengembangkan dan menguji mekanisme verifikasi password ganda. Setiap tahapan penelitian dirancang untuk memastikan bahwa mekanisme yang diusulkan dapat diimplementasikan dan diuji secara efektif, mulai dari analisis kebutuhan hingga analisis dan evaluasi hasil. Metode penelitian ini mencakup desain sistem, implementasi teknis, pengujian keamanan dan kinerja, serta evaluasi menyeluruh terhadap efektivitas pendekatan yang diusulkan.

1. Tahapan Penelitian

Tahapan penelitian ini mencakup langkah-langkah yang diambil untuk mencapai tujuan penelitian. Setiap tahapan dirancang untuk memastikan bahwa mekanisme verifikasi password ganda dapat dikembangkan dan diuji secara efektif. Tahapan ini meliputi analisis kebutuhan, desain sistem, implementasi, pengujian, serta analisis dan evaluasi hasil.

Berikut adalah tahapan, rancangan, dan prosedur penelitian yang dilakukan.

1. Studi Literatur

Mengumpulkan dan menganalisis penelitian terdahulu yang relevan dengan topik autentikasi, penggunaan WhatsApp untuk verifikasi, hashing password dengan bcrypt, dan penyimpanan data menggunakan MongoDB. Studi ini memberikan dasar teoritis dan metodologis yang kuat untuk penelitian. Analisis dilakukan untuk mengidentifikasi metode dan hasil penelitian yang dapat diterapkan dalam sistem yang dikembangkan.

1. Perancangan Sistem

Merancang sistem autentikasi yang menggunakan nomor handphone sebagai identitas utama dan WhatsApp untuk mengirimkan password sementara. Sistem ini mencakup:

* Autentikasi menggunakan kode QR
* Autentikasi menggunakan Google
* Autentikasi menggunakan Sandi Terenkripsi (STP)
* Penentuan teknologi yang digunakan: Golang untuk backend, MongoDB untuk penyimpanan data, dan React untuk frontend.

1. Implementasi Sistem

Mengimplementasikan sistem autentikasi menggunakan teknologi yang telah dipilih. Backend dikembangkan menggunakan Golang dan MongoDB, sementara frontend menggunakan React. Implementasi meliputi:

* Autentikasi kode QR
* Autentikasi Google
* Autentikasi STP

1. Pengujian dan Evaluasi

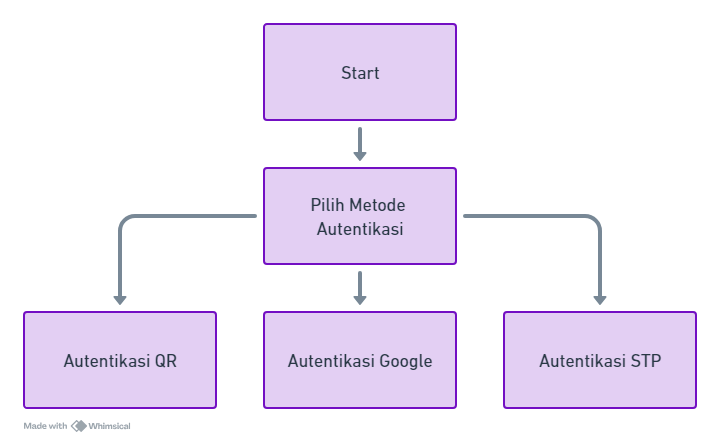
Melakukan pengujian fungsionalitas dan keamanan sistem autentikasi yang telah diimplementasikan. Pengujian meliputi:

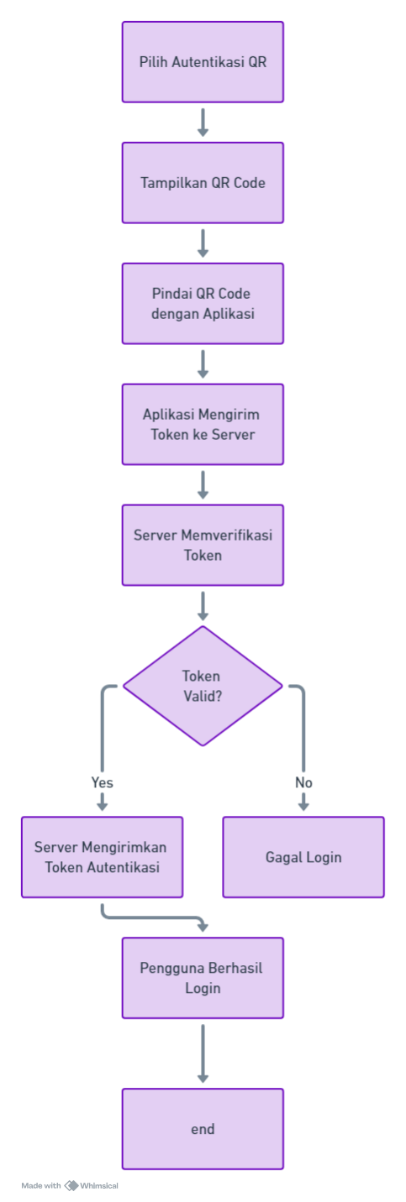
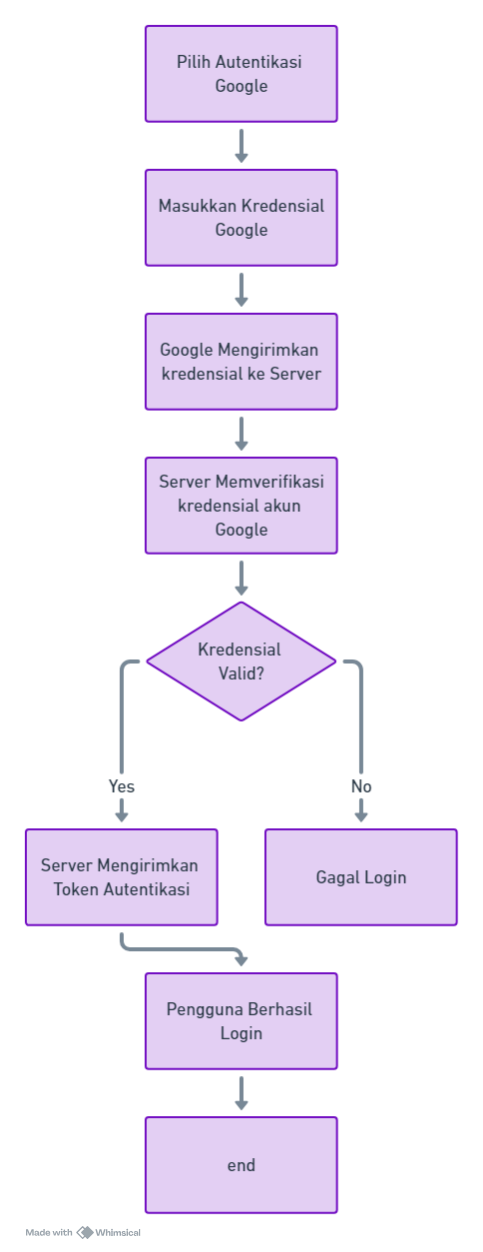
* Pengujian autentikasi menggunakan kode QR
* Pengujian autentikasi menggunakan Google
* Pengujian autentikasi menggunakan STP
* Evaluasi dilakukan untuk menilai kinerja dan keamanan sistem melalui uji brute force dan serangan dictionary.

1. Diagram Alur Metodologi Penelitian

Diagram ini menunjukkan skema autentikasi secara menyeluruh yang digunakan dalam penelitian ini, termasuk tiga metode autentikasi utama, autentikasi QR, autentikasi Google, dan autentikasi Sandi Terenkripsi (STP). Diagram ini membantu memvisualisasikan tahapan-tahapan dalam proses autentikasi dan menunjukkan alur logis dari setiap metode autentikasi yang diterapkan dalam sistem. Berikut adalah diagram alur metodologi penelitian yang memberikan gambaran jelas tentang proses penelitian:

1. Start, Aplikasi dimulai, dan pengguna disajikan dengan opsi untuk memilih metode autentikasi, yaitu Autentikasi Kode QR, Autentikasi Google, atau Autentikasi STP (Secure Temporary Password).



Gambar 1 Skema Autentikasi

Gambar 2 A Gambar 3 B

1. QR Code Authentication

Berikut adalah penjelasan alur dari gambar 2 A yang merupakan skema ketika pengguna memilih Autentikasi menggunakan kode QR.

* Pengguna memilih untuk mengautentikasi menggunakan kode QR.
* Aplikasi menampilkan kode QR untuk dipindai oleh pengguna.
* Pengguna memindai kode QR menggunakan kamera dari aplikasi Whatsapp.
* Aplikasi mobile mengirimkan token yang dipindai ke server.
* Server memeriksa validitas token.
* IF token is valid THEN

1. Server mengirim token Autentikasi kepada pengguna.
2. Pengguna berhasil login.

ELSE

1. Login gagal.
2. Google Authentication

Berikut adalah penjelasan alur dari gambar 3 B yang merupakan skema ketika pengguna memilih Autentikasi menggunakan google.

* Pengguna memilih untuk mengautentikasi menggunakan Google.
* Pengguna mengklik tombol "Login with Google".
* Pengguna memasukkan kredensial Google mereka.
* Google mengirimkan kredensial ke server.
* Server memverifikasi kredensial Google yang diterima.
* Server memeriksa validitas kredensial dari akun Google.
* IF crendential is valid THEN

1. Server mengirim token Autentikasi kepada pengguna.
2. Pengguna berhasil login.

ELSE

1. Login gagal.
2. STP (Secure Temporary Password)

Berikut adalah penjelasan alur dari gambar skema Autentikasi stp yang merupakan skema ketika pengguna memilih Autentikasi menggunakan stp.

* Pengguna memilih untuk mengautentikasi menggunakan STP.
* Pengguna memasukkan nomor telepon mereka.
* Sistem memverifikasi nomor telepon yang diberikan.
* Sistem memeriksa validitas nomor telepon.
* IF phonenumber is valid THEN

1. Server membuat password.

ELSE

1. Login gagal.

* Sistem menyimpan password yang di-hash dengan waktu kedaluwarsa 4 menit.
* Sistem mengirimkan password ke pengguna melalui WhatsApp.
* Pengguna menerima password melalui WhatsApp.
* Pengguna memasukkan password yang diterima pada halaman login.
* Sistem memverifikasi password yang dimasukkan dan memeriksa apakah sudah kedaluwarsa.
* Sistem memeriksa apakah password valid dan belum kedaluwarsa.
* IF password is valid THEN

Server mengirimkan token autentikasi kepada pengguna.

Pengguna berhasil login.

ELSE IF password is expired THEN

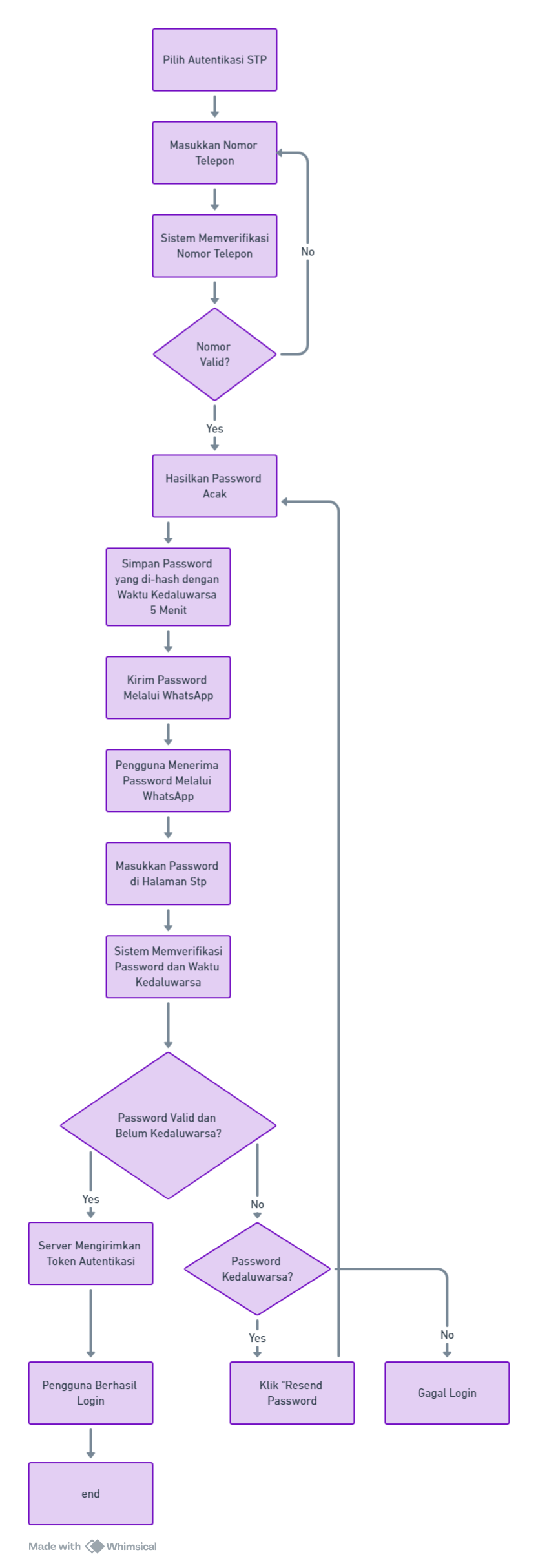
Pengguna mengklik "Resend Password" untuk menerima password baru.

Server mengirimkan token autentikasi kepada pengguna.

Pengguna berhasil login.

ELSE

Login gagal.



Gambar 4 Skema Autentikasi STP

1. End:

* Aplikasi berakhir setelah pengguna berhasil login menggunakan salah satu metode autentikasi.

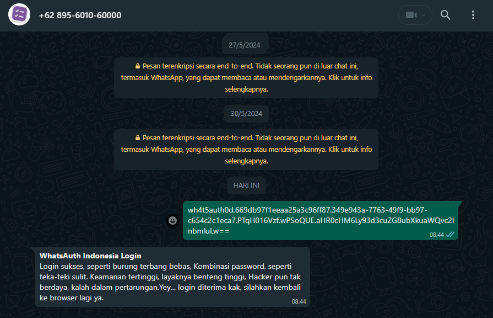
Diagram alur ini memberikan representasi rinci tentang proses autentikasi, termasuk metode autentikasi yang berbeda, langkah-langkah yang terlibat dalam setiap metode, dan titik keputusan yang menentukan keberhasilan atau kegagalan proses login. Penjelasan yang menyertai setiap langkah dan titik keputusan membantu memperjelas fungsi dan logika dari sistem yang diimplementasikan.

**HASIL DAN PEMBAHASAN**

1. Hasil

Penelitian ini bertujuan untuk mengimplementasikan skema autentikasi dan otorisasi yang aman pada website statis menggunakan berbagai metode autentikasi, seperti autentikasi QR, autentikasi Google, dan autentikasi STP. Hasil penelitian ini menunjukkan keberhasilan dalam mencapai tujuan tersebut melalui pengujian yang dilakukan.

1. Autentikasi QR

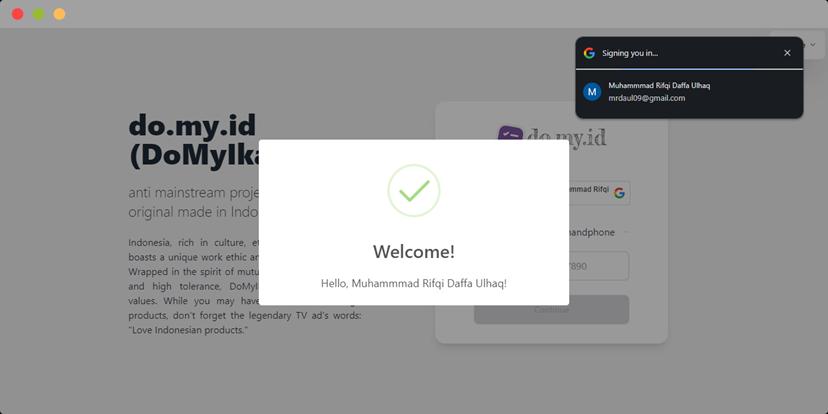
Autentikasi QR memungkinkan pengguna untuk memindai kode QR yang unik untuk mendapatkan akses ke sistem. Hasil pengujian menunjukkan bahwa metode ini sangat efektif dalam mengamankan akses pengguna, karena setiap kode QR hanya dapat digunakan sekali dan memiliki masa berlaku yang terbatas. Namun, kelemahan dari metode ini adalah pengguna membutuhkan perangkat tambahan yang mendukung pemindaian QR code.

Gambar 5 Autentikasi kode QR

Pengujian autentikasi QR menunjukkan bahwa metode ini dapat mengurangi risiko pencurian kredensial dengan menghindari input manual dari pengguna.

1. Autentikasi Google

Autentikasi Google menggunakan layanan Google Sign-In untuk memverifikasi identitas pengguna. Hasil pengujian menunjukkan bahwa metode ini mudah digunakan dan sangat aman. Pengguna cukup login menggunakan akun Google mereka, dan sistem memanfaatkan infrastruktur keamanan Google yang handal untuk mengamankan autentikasi pengguna. Kelebihan utama dari metode ini adalah pengguna tidak perlu mengingat password tambahan, karena mereka menggunakan kredensial Google yang sudah ada.



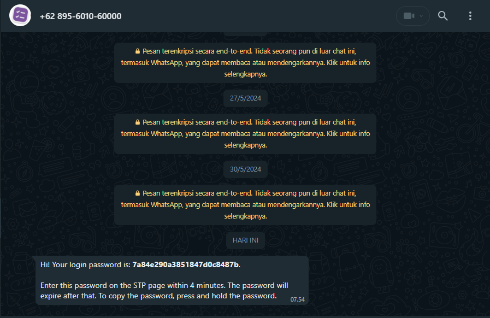
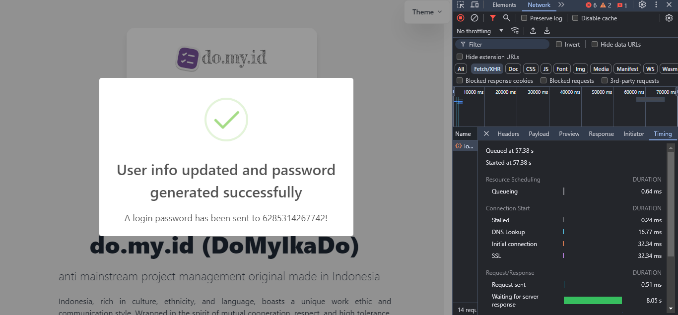
Gambar 6 Autentikasi Google

Autentikasi Google berhasil memanfaatkan infrastruktur keamanan Google untuk meningkatkan kepercayaan pengguna. Namun, risiko tetap ada jika token akses berhasil dicuri oleh pihak yang tidak berwenang.

1. Autentikasi STP

Autentikasi STP (Secure Temporary Password) mengirimkan password sementara melalui WhatsApp ke nomor ponsel pengguna. Hasil pengujian menunjukkan bahwa metode ini efektif dalam mengamankan akses pengguna, terutama bagi mereka yang sering lupa password. Berikut adalah skenario pengujian yang dilakukan untuk metode autentikasi STP:

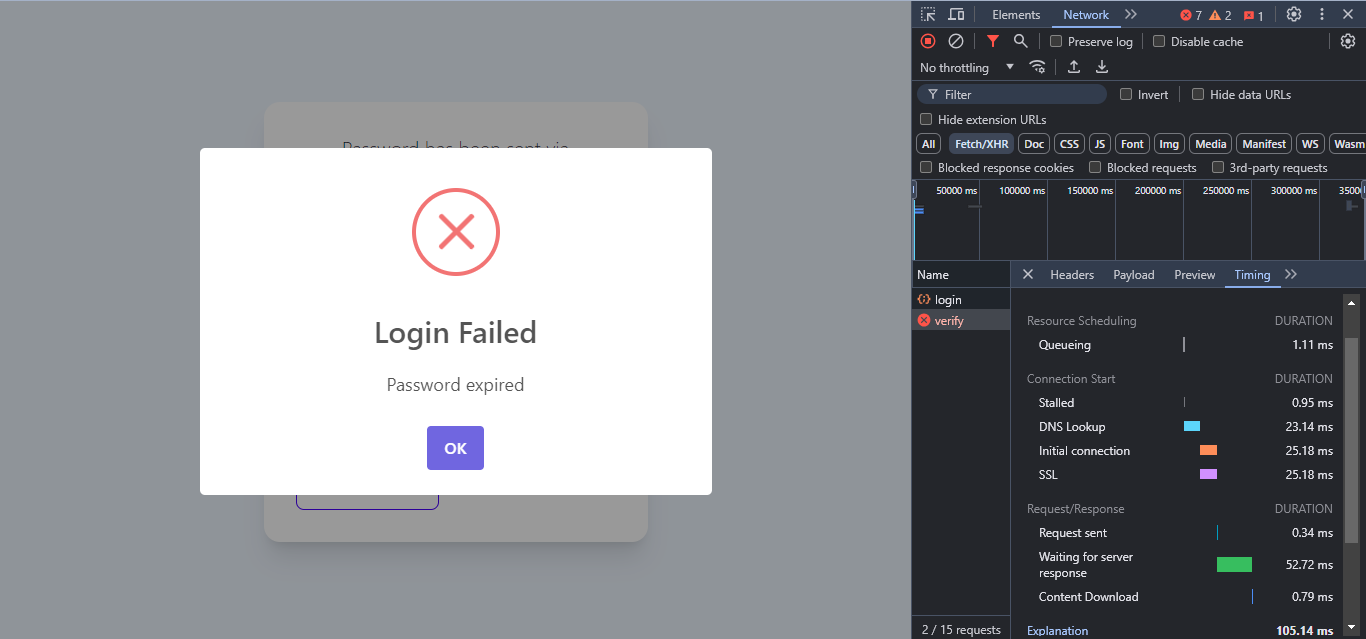
* Berhasil

Seperti yang terlihat pada gambar dibawah, pengguna yang memasukkan password dengan benar dalam batas waktu yang ditentukan berhasil masuk ke sistem.

Gambar 7 Autentikasi STP: Berhasil

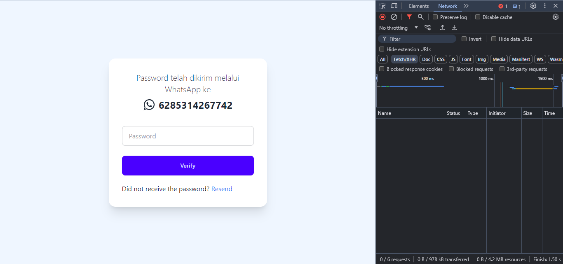
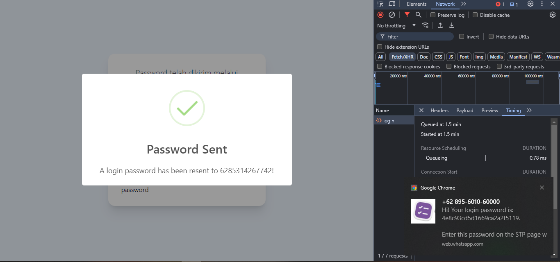
* Password Kedaluwarsa

Jika password telah kedaluwarsa, pengguna akan menerima pesan bahwa password telah kedaluwarsa dan harus meminta password baru.



Gambar 8 Autentikasi STP: Password kadaluwarsa

* Resend Password

Pengguna dapat mengirim ulang password jika tidak menerima atau jika password telah kedaluwarsa. Metode ini memastikan pengguna tetap dapat mengakses sistem meskipun terjadi kendala pada pengiriman password sebelumnya.

Gambar 9 Autentikasi STP: Kirim ulang password

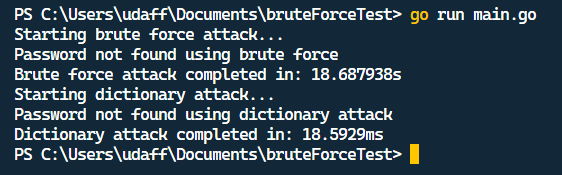
Hasil pengujian menunjukkan bahwa metode autentikasi STP meningkatkan keamanan sistem dengan memanfaatkan faktor autentikasi tambahan seperti pengiriman password melalui WhatsApp.

1. Pembahasan

Penelitian ini membahas tiga metode autentikasi yang diterapkan pada website statis dan mengevaluasi keefektifan masing-masing metode.

1. Keamanan

Setiap metode autentikasi yang diterapkan memiliki tingkat keamanan yang tinggi. Autentikasi QR dan Google Sign-In memanfaatkan teknologi canggih untuk memastikan keamanan identitas pengguna, sementara autentikasi STP menggunakan pengiriman password melalui WhatsApp yang populer dan mudah diadopsi oleh pengguna.



Gambar 10 Pengujian Brute Force dan Dictionary Attack

Hasil pengujian brute force dan dictionary attack menunjukkan bahwa penggunaan hashing password dengan bcrypt serta pengiriman password sementara melalui WhatsApp mampu meningkatkan keamanan sistem. Waktu yang dibutuhkan untuk memecahkan password dengan brute force dan dictionary attack sangat lama, yang membuktikan bahwa metode ini efektif dalam melindungi password pengguna.

Tabel 1 Hasil Pengujian Brute Force dan Dictionary

|  |  |  |
| --- | --- | --- |
| Jenis Serangan | Waktu (ms) | Keterangan |
| Brute Force | 18687.94 | Password tidak ditemukan |
| Dictionary | 18.5929 | Password tidak ditemukan |

1. Pengalaman Pengguna

Pengalaman pengguna juga menjadi fokus utama dalam penelitian ini. Autentikasi Google dan STP dirancang untuk memudahkan pengguna dalam mengakses sistem tanpa harus mengingat banyak password. Penggunaan WhatsApp sebagai sarana pengiriman password juga meningkatkan kenyamanan pengguna, mengingat popularitas WhatsApp yang tinggi di kalangan masyarakat.

**KESIMPULAN DAN SARAN**

Penelitian ini berhasil mencapai tujuan utama untuk meningkatkan keamanan autentikasi pengguna pada website statis dengan menggunakan berbagai metode autentikasi, yaitu autentikasi QR, autentikasi Google, dan Sandi Terenkripsi (STP). Implementasi aplikasi web dengan menggunakan React untuk frontend dan Go untuk backend menunjukkan efektivitas dalam melindungi password pengguna dari serangan brute force dan serangan dictionary. Hasil pengujian menunjukkan bahwa:

1. Autentikasi QR

Metode ini terbukti efektif dalam mengamankan akses pengguna dengan memberikan kode QR yang unik dan memiliki masa berlaku terbatas. Pengujian menunjukkan bahwa metode ini mampu mengurangi risiko pencurian kredensial.

1. Autentikasi Google

Penggunaan layanan Google Sign-In mempermudah pengguna dalam proses autentikasi dan memanfaatkan infrastruktur keamanan Google yang andal. Metode ini terbukti aman dan nyaman bagi pengguna.

1. Secure Temporary Password (STP)

Pengiriman password sementara melalui WhatsApp terbukti efektif dalam meningkatkan keamanan akses pengguna. Metode ini memanfaatkan popularitas WhatsApp untuk meningkatkan adopsi oleh pengguna dan menyediakan mekanisme autentikasi yang aman.

Untuk meningkatkan kenyamanan pengguna, disarankan untuk mengirimkan pesan yang di-embed dengan tombol salin password di WhatsApp. Dengan adanya tombol salin, pengguna dapat menyalin password dengan sekali klik tanpa harus menyeleksi teks secara manual, sehingga dapat mengurangi kesalahan pengguna dalam menyalin password dan mempercepat proses login. Meskipun sistem autentikasi saat ini telah cukup aman, penambahan fitur Multi-Factor Authentication (MFA) dapat meningkatkan keamanan lebih lanjut dengan memungkinkan pengguna memverifikasi identitas mereka melalui metode tambahan seperti kode OTP yang dikirim melalui SMS atau email.

Untuk menghadapi peningkatan jumlah pengguna di masa mendatang, disarankan untuk terus mengoptimalkan performa sistem. Penggunaan teknologi caching dan load balancing dapat membantu meningkatkan kecepatan respon server dan mengurangi beban pada server utama. Selain itu, menambahkan integrasi dengan layanan pihak ketiga seperti Github untuk opsi login dapat meningkatkan fleksibilitas dan kenyamanan pengguna, karena pengguna dapat memilih metode login yang paling sesuai dengan preferensi mereka.

Meningkatkan desain antarmuka pengguna (UI) dan pengalaman pengguna (UX) agar lebih intuitif dan mudah digunakan juga sangat penting. Melakukan pengujian dengan pengguna (user testing) untuk mendapatkan feedback langsung dapat membantu dalam perbaikan desain. Penggunaan teknik machine learning untuk mendeteksi pola penggunaan yang mencurigakan dan mencegah akses yang tidak sah juga disarankan. Algoritma machine learning dapat membantu dalam meningkatkan keamanan sistem secara otomatis.

Menyediakan dokumentasi yang lebih lengkap dan mudah dipahami bagi pengembang lain yang mungkin akan mengembangkan sistem ini lebih lanjut juga sangat penting. Dokumentasi yang baik akan mempermudah proses pengembangan dan pemeliharaan di masa mendatang. Terakhir, melakukan penelitian lanjutan untuk mengeksplorasi metode autentikasi lain yang lebih aman dan efisien sangat disarankan. Penggunaan teknologi terbaru dan pendekatan inovatif dapat membantu dalam terus meningkatkan keamanan dan kenyamanan pengguna.

**DAFTAR PUSTAKA**

[1] J. Shahid, M. K. Hameed, I. T. Javed, K. N. Qureshi, M. Ali, and N. Crespi, “A Comparative Study of Web Application Security Parameters: Current Trends and Future Directions,” *Applied Sciences*, vol. 12, no. 8, 2022, doi: 10.3390/app12084077.

[2] “Cybercrime To Cost The World $10.5 Trillion Annually By 2025.” Accessed: Jul. 22, 2024. [Online]. Available: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

[3] P. Kumari and M. Kumari, “Exploring Static Website Development A Fundamental Analysis of Design and Functionality”.

[4] D. V Kornienko, S. V Mishina, and M. O. Melnikov, “The Single Page Application architecture when developing secure Web services,” in *Journal of Physics: Conference Series*, 2021, p. 12065.

[5] A. Bucko, K. Vishi, B. Krasniqi, and B. Rexha, “Enhancing JWT Authentication and Authorization in Web Applications Based on User Behavior History,” *Computers*, vol. 12, no. 4, 2023, doi: 10.3390/computers12040078.

[6] D. Morais, A. Zúquete, and A. Mendes, “Adaptive, Multi-Factor Authentication as a Service for Web Applications,” in *2023 7th Cyber Security in Networking Conference (CSNet)*, 2023, pp. 74–80.

[7] J. Singh and N. K. Chaudhary, “OAuth 2.0: Architectural design augmentation for mitigation of common security vulnerabilities,” *Journal of Information Security and Applications*, vol. 65, p. 103091, 2022.

[8] S. P. Otta, S. Panda, M. Gupta, and C. Hota, “A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure,” *Future Internet*, vol. 15, no. 4, 2023, doi: 10.3390/fi15040146.

[9] C. E. (Catherine) Lee, H. H. Chern, and D. A. Azmir, “WhatsApp Use in a Higher Education Learning Environment: Perspective of Students of a Malaysian Private University on Academic Performance and Team Effectiveness,” *Educ Sci (Basel)*, vol. 13, no. 3, 2023, doi: 10.3390/educsci13030244.

[10] K. Manji, J. Hanefeld, J. Vearey, H. Walls, and T. De Gruchy, “Using WhatsApp messenger for health systems research: a scoping review of available literature,” *Health Policy Plan*, vol. 36, no. 5, pp. 774–789, 2021.

[11] J. Sen, *Theory and Practice of Cryptography and Network Security Protocols and Technologies*. Rijeka: IntechOpen, 2013. doi: 10.5772/56823.

[12] D. Fett, R. Küsters, and G. Schmitz, “A Comprehensive Formal Security Analysis of OAuth 2.0,” *CoRR*, vol. abs/1601.01229, 2016, [Online]. Available: http://arxiv.org/abs/1601.01229

[13] E. Mostafa, M. M. Hassan, and W. Said, “An Interactive Multi-Factor User Authentication Framework in Cloud Computing,” *International Journal of Computer Science & Network Security*, vol. 23, no. 8, pp. 63–76, 2023.

[14] Z. S. Paki, S. Sani, and G. I. Diri, “Connection to the use of free Android apps in Kebbi State, Nigeria,” *Journal of Social Sciences*, no. 3, pp. 144–154, 2022.