**PROTOKOL OTORISASI DAN OTENTIKASI PADA WEB STATIS**

**TUGAS AKHIR**

**Diajukan Sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana Terapan Teknik Informatika (S.Tr.Kom.) pada Program Pendidikan D4 Teknik Informatika**



**Oleh :**

**MUHAMMAD RIFQI DAFFA ULHAQ**

**1204045**

**PROGRAM DIPLOMA IV TEKNIK INFORMATIKA SEKOLAH VOKASI**

**UNIVERSITAS LOGISTIK DAN BISNIS INTERNASIONAL BANDUNG**

**2024**

**PROTOKOL OTORISASI DAN OTENTIKASI PADA WEB STATIS**

**TUGAS AKHIR**

**Diajukan Sebagai Salah Satu Syarat untuk Memperoleh Gelar Sarjana Terapan Teknik Informatika (S.Tr.Kom.) pada Program Pendidikan D4 Teknik Informatika**



**Oleh :**

**MUHAMMAD RIFQI DAFFA ULHAQ**

**1204045**

**PROGRAM DIPLOMA IV TEKNIK INFORMATIKA SEKOLAH VOKASI**

**UNIVERSITAS LOGISTIK DAN BISNIS INTERNASIONAL BANDUNG**

**2024**

# HALAMAN PERNYATAAN ORISINALITAS

Yang bertanda tangan dibawah ini :

Nama : Muhammad Rifqi Daffa Ulhaq  
NPM : 1204045  
Program Studi : D4 Teknik Informatika  
Perguruan Tinggi : Universitas Logistik dan Bisnis Internasional

Dengan ini menyatakan bahwa tugas akhir yang telah saya buat dengan judul: “**Protokol Otorisasi Dan Otentikasi Pada Web Statis”** adalah asli (orisinil) dan belum pernah diterbitkan/dipublikasikan dimanapun dan dalam bentuk apapun. Demikianlah surat pernyataan ini saya buat dengan sebenar-benarnya tanpa ada paksaan dari pihak manapun juga. Apabila dikemudian hari ternyata saya memberikan keterangan palsu dan atau ada pihak lain yang mengklaim bahwa tugas akhir yang telah saya buat adalah hasil karya milik seseorang atau badan tertentu, saya bersedia diproses baik secara pidana maupun perdata dan kelulusan saya dari Universitas Logistik dan Bisnis Internasional dicabutkan/dibatalkan.

|  |
| --- |
| Dibuat di : Bandung |
| Pada tanggal. : Juli 2024 |
| Yang menyatakan, |
|  |
| Materai Rp. 10000 |
| Muhammad Rifqi Daffa Ulhaq |

# 

# HALAMAN PENGESAHAN

# KATA PENGANTAR

Penulis panjatkan segala puji terhadap Tuhan Yang Maha Esa atas berkat-Nya, yang memungkinkan penyelesaian laporan tugas akhir tanpa kendala yang berarti. Keberhasilan dalam penulisan laporan ini merupakan hasil dari dukungan dari berbagai pihak yang memberikan masukan untuk meningkatkannya. Kemudian, penulis mengucapkan banyak terima kasih terhadap semua pihak yang telah memberikan kontribusi:

1. Allah Yang Maha Esa dengan limpahan berkat-Nya, penulis berhasil membuat laporan ini dengan baik.
2. Orang tua dan rekan-rekan yang senantiasa memberikan doa dan dukungan.
3. Bapak Rolly Maulana Awangga, S.T., MT., CAIP, SFPC selaku pembimbing internal.
4. Bapak M. Yusril Helmi Setyawan, S. Kom., M. Kom., SFPC selaku pembimbing internal.
5. Bapak Roni Andarsyah, S.T., M. Kom., SFPC selaku Kepala Program Studi DIV Teknik Informatika Universitas Logistik Bisnis Internasional.
6. Bapak M. Yusril Helmi Setyawan, S. Kom., M. Kom., SFPC selaku Koordinator tugas akhir tahun 2024/ 2025.

Penulis menyadari bahwa penyusunan laporan tugas akhir ini masih memiliki ruang untuk peningkatan. Kritik dan saran sangat diharapkan dan dapat disampaikan melalui penulis.

# HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Logistik dan Bisnis Internasional (ULBI), saya yang bertanda tangan di bawah ini:

|  |  |
| --- | --- |
| Nama : | Muhammad Rifqi Daffa Ulhaq |
| Npm : | 1204045 |
| Program Studi : | D4 Teknik Informatika |
| Jenis karya : | Tugas Akhir |

Demi pengembangan ilmu pengetahuan, memberikan kepada ULBI Hak Bebas Royalti Noneksklusif (Non-exclusive Royalty- Free Right) atas karya ilmiah saya yang berjudul:

**“Protokol Otorisasi Dan Otentikasi Pada Web Statis”**

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non eksklusifini Universitas Logistik dan Bisnis Internasional berhak menyimpan, mengalihmedia/format- kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Tugas Akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

|  |
| --- |
| Dibuat di : Bandung |
| Pada tanggal. : Juli 2024 |
| Yang menyatakan, |
|  |
| Materai Rp. 10000 |
|  |
| Muhammad Rifqi Daffa Ulhaq |

# ABSTRAK

Dalam era digital yang semakin maju, keamanan dan efisiensi dalam pengembangan aplikasi *web* menjadi sangat penting. Otorisasi dan autentikasi pengguna merupakan komponen kunci dalam menjaga integritas dan keamanan data di *web*. Penelitian ini mengimplementasikan skema autentikasi dan otorisasi yang aman pada *website* statis dengan menggunakan berbagai metode, seperti autentikasi QR, autentikasi Google, dan autentikasi *Short-term Password* (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.

Metode STP memungkinkan pengguna menerima sandi login melalui WhatsApp, yang berlaku selama 5 menit. Penggunaan WhatsApp sebagai media pengiriman sandi dipilih karena popularitasnya yang tinggi di kalangan pengguna, sehingga memudahkan adopsi metode ini. Sistem autentikasi yang dirancang telah diuji melalui serangkaian eksperimen, termasuk uji *brute* *force* dan serangan *dictionary*, yang menunjukkan ketahanan terhadap upaya pembobolan akun. Hasil penelitian ini menunjukkan bahwa kombinasi berbagai metode autentikasi yang diterapkan dapat meningkatkan keamanan dan memberikan pengalaman pengguna yang lebih baik pada *website* statis.

Penelitian ini berkontribusi dengan memberikan solusi praktis untuk meningkatkan keamanan *web* statis, yang seringkali diabaikan dalam diskusi tentang keamanan *web*. Temuan ini relevan bagi pengembang *web* yang mencari cara untuk melindungi data pengguna dengan metode yang efisien dan mudah diadopsi.

Keywords: Autentikasi, Otorisasi, Keamanan *Web*, *Bcrypt*, *Web* Statis.

# ABSTRACT

*In the increasingly advanced digital era, security and efficiency in web application development have become very important. User authorization and authentication are key components in maintaining data integrity and security on the web. This research implements a secure authentication and authorization scheme on a static website using various methods, such as QR authentication, Google authentication, and Encrypted Password (STP) authentication. 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 to improve security and user experience.*

*The STP method allows users to receive a login password via WhatsApp, which is valid for 5 minutes. The use of WhatsApp as a medium for sending passwords was chosen due to its high popularity among users, thus facilitating the adoption of this method. The designed authentication system has been tested through a series of experiments, including brute force tests and dictionary attacks, demonstrating resilience against account breach attempts. The results of this research show that the combination of various authentication methods applied can improve security and provide a better user experience on static websites.*

*This research contributes by providing practical solutions to improve static web security, which is often overlooked in discussions about web security. The findings are relevant to web developers who are looking for ways to protect user data with efficient and easy-to-adopt methods.*

*Keywords:* *Authentication, Authorization, Web Security, Bcrypt, Static Web.*

# DAFTAR ISI

[HALAMAN PERNYATAAN ORISINALITAS i](#_Toc172569842)

[HALAMAN PENGESAHAN ii](#_Toc172569843)

[KATA PENGANTAR iii](#_Toc172569844)

[HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS iv](#_Toc172569845)

[DAFTAR ISI vii](#_Toc172569846)

[DAFTAR TABEL xi](#_Toc172569847)

[DAFTAR GAMBAR xii](#_Toc172569848)

[DAFTAR LAMPIRAN xiii](#_Toc172569849)

[BAB 1 1](#_Toc172569850)

[PENDAHULUAN 1](#_Toc172569851)

[1. 1 Latar Belakang 1](#_Toc172569852)

[1. 2 Identifikasi Masalah 2](#_Toc172569853)

[1. 3 Tujuan dan Manfaat 2](#_Toc172569854)

[1. 4 Ruang Lingkup 3](#_Toc172569855)

[BAB II 4](#_Toc172569856)

[LANDASAN TEORI 4](#_Toc172569857)

[2. 1 Deskripsi Topik Yang Sama 4](#_Toc172569858)

[2. 2 Deskripsi Metode Yang Sama 5](#_Toc172569859)

[BAB III 7](#_Toc172569860)

[METODOLOGI PENELITIAN 7](#_Toc172569861)

[3. 1 Metodologi Penelitian 7](#_Toc172569862)

[3. 2 Tahapan Tahapan Diagram Metodologi Penelitian 8](#_Toc172569878)

[BAB IV 11](#_Toc172569879)

[EKSPERIMEN DAN HASIL 11](#_Toc172569880)

[4. 1 Eksperimen 11](#_Toc172569881)

[4. 2 Hasil 13](#_Toc172569882)

[BAB V 20](#_Toc172569883)

[KESIMPULAN 20](#_Toc172569884)

[5. 1 Kesimpulan Masalah 20](#_Toc172569885)

[5. 2 Kesimpulan Metode 20](#_Toc172569886)

[5. 3 Kesimpulan Eksperimen 21](#_Toc172569887)

[BAB VI 23](#_Toc172569888)

[SARAN 23](#_Toc172569889)

[DAFTAR PUSTAKA 25](#_Toc172569890)

# DAFTAR TABEL

[Tabel 4. 1 Hasil Pengujian Brute Force dan Dictionary 30](#_Toc172567058)

# DAFTAR GAMBAR

[Gambar 3. 1 Diagram Alur Penelitian 22](#_Toc172566912)

[Gambar 4. 1 Hasil Autentikasi QR 26](#_Toc172567005)

[Gambar 4. 2 Hasil Autentikasi Google 26](#_Toc172567006)

[Gambar 4. 3 Skenario Autentikasi STP: Berhasil 28](#_Toc172567007)

[Gambar 4. 4 Skenario Autentikasi STP: Password kadaluarsa 29](#_Toc172567008)

[Gambar 4. 5 Skenario Autentikasi STP: Kirim ulang password 30](#_Toc172567009)

[Gambar 4. 6 Pengujian Brute Force dan Dictionary Attack 30](#_Toc172567010)

# DAFTAR LAMPIRAN

# BAB 1

# PENDAHULUAN

## Latar Belakang

Dalam era digital yang semakin maju, keamanan dan efisiensi dalam pengembangan aplikasi *web* menjadi hal yang sangat penting[1]. Menurut laporan dari *Cybersecurity* *Ventures*, kerugian global akibat kejahatan *cyber* diperkirakan akan mencapai $10,5 triliun per tahun pada 2025, menunjukkan urgensi peningkatan keamanan *web*[2]. Salah satu aspek utama dalam keamanan *web* adalah otorisasi dan otentikasi pengguna[3]. Kedua konsep ini merupakan komponen penting dalam menjaga integritas dan keamanan data di *web*.

*Web* statis, yang memiliki konten yang tidak berubah kecuali diperbarui oleh pengembang, sering digunakan untuk situs-situs yang menyajikan informasi tetap, seperti profil perusahaan, portofolio, atau dokumentasi[4]. Meskipun sederhana dan mudah dikelola, *web* statis tetap memerlukan mekanisme keamanan yang memadai. Karena *web* statis tidak memiliki *backend* dinamis untuk memproses permintaan autentikasi secara *real*-*time*, muncul tantangan unik dalam implementasi protokol otorisasi dan otentikasi[5].

Penggunaan protokol 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]. Integrasi OAuth2 dengan layanan seperti *Google* dapat memberikan solusi otorisasi yang efisien dan aman. Selain itu, penerapan MFA dapat meningkatkan proteksi keamanan dengan menambahkan lapisan verifikasi tambahan selain kata sandi[8].

Namun, tidak semua pengguna familiar dengan protokol OAuth2 atau merasa nyaman menggunakan MFA[9], [10]. Dalam situasi ini, mengirimkan *password* melalui *WhatsApp* bisa menjadi alternatif yang lebih familiar bagi pengguna. *WhatsApp* adalah aplikasi pesan instan yang sangat populer dan banyak digunakan oleh berbagai kalangan masyarakat[11], [12]. Penggunaan *WhatsApp* untuk menyampaikan *password* dapat meningkatkan pengalaman pengguna dan memudahkan mereka dalam proses autentikasi.

Penelitian ini bertujuan untuk mengatasi masalah keamanan dan kemudahan pengguna dalam autentikasi dengan mengembangkan sistem otorisasi dan otentikasi pada halaman *web* statis. Sistem ini menggunakan modifikasi protokol OAuth2 yang terintegrasi dengan Google dan WhatsApp. Dalam penelitian ini, sistem dirancang dengan menggunakan teknologi seperti *bcrypt* untuk *hashing* *password* dan MongoDB untuk manajemen data. Selain itu, terdapat *field* *createdAt* yang diberikan *indexing* selama 5 menit sehingga password akan otomatis terhapus dari *database* demi keamanan. Dengan pendekatan ini, diharapkan sistem yang dihasilkan tidak hanya aman tetapi juga *user*-*friendly* bagi pengguna awam.

## Identifikasi Masalah

Penelitian ini didasarkan pada beberapa permasalahan utama yang sering dihadapi dalam sistem autentikasi konvensional. Masalah-masalah ini perlu diidentifikasi dan dianalisis untuk menemukan solusi yang lebih aman dan efisien.

1. Bagaimana mengamankan autentikasi dan otorisasi *user* pada *website* statis
2. Bagaimana menghitung resiko keamanan yang terjadi dari setiap skema autentikasi dan otorisasi

## Tujuan dan Manfaat

Tujuan dari penelitian ini adalah untuk mengembangkan sistem autentikasi yang lebih aman dan efisien menggunakan STP yang dikirim melalui *WhatsApp*. Manfaat yang diharapkan dari penelitian ini adalah peningkatan keamanan dan kemudahan penggunaan sistem autentikasi.

1. Membuat skema otorisasi dan authentikasi pada *website* statis
2. Menghitung resiko pembobolan akun

## Ruang Lingkup

Untuk mencapai tujuan penelitian, ruang lingkup penelitian ini mencakup beberapa aspek teknis dan fungsional yang harus dibatasi, guna menjaga fokus dan esensi dari penelitian.

1. Pengembangan sistem otorisasi dan autentikasi untuk *website* statis.
2. Implementasi protokol OAuth2 yang terintegrasi dengan *Google* dan *WhatsApp*.
3. Pemanfaatan teknologi *bcrypt* untuk *hashing* *password* dan MongoDB untuk manajemen data.
4. Implementasi *client* menggunakan *React* untuk membangun aplikasi *web* statis dan SPA (*Single* *Page* *Application*).
5. Penggunaan *WhatsApp* sebagai media penyampaian *password* kepada pengguna.

# BAB II

# LANDASAN TEORI

## Deskripsi Topik Yang Sama

Bagian ini akan membahas tentang berbagai penelitian dan implementasi terkait yang memiliki tujuan dan pendekatan serupa dengan penelitian ini, untuk memberikan konteks dan mendemonstrasikan relevansi penelitian yang sedang dilakukan.

Penelitian tentang sistem autentikasi dan otorisasi telah banyak dilakukan mengingat pentingnya keamanan data di era digital. Beberapa topik yang relevan dengan penelitian ini mencakup:

1. Keamanan *Web* dan Autentikasi

Penelitian[13] menekankan pentingnya protokol keamanan pada aplikasi web, namun belum fokus pada web statis dan modifikasi OAuth2. Penelitian ini mengkaji berbagai protokol keamanan dan menyoroti kebutuhan akan metode autentikasi yang lebih aman dan efisien.

1. Implementasi OAuth2 dalam Autentikasi

Penelitian[14] menjelaskan implementasi OAuth2 dalam autentikasi. Penelitian ini menunjukkan bagaimana OAuth2 dapat digunakan untuk mengamankan akses ke aplikasi web dengan memberikan hak akses terbatas tanpa mengungkapkan kredensial pengguna.

## Deskripsi Metode Yang Sama

Bagian ini akan menjelaskan berbagai metode yang digunakan dalam penelitian sebelumnya yang serupa dengan metode yang digunakan dalam penelitian ini, untuk menunjukkan bagaimana metode tersebut telah berhasil diterapkan dan mendukung relevansi serta validitas metode yang dipilih.

1. Autentikasi dengan Nomor Handphone

Metode ini melibatkan penggunaan nomor *handphone* sebagai kunci utama untuk identifikasi pengguna. Dalam penelitian ini, nomor *handphone* dikirimkan melalui formulir login, kemudian server memvalidasi nomor tersebut dan mengirimkan password sementara melalui WhatsApp. Penelitian[15], [16]menggunakan pendekatan serupa dengan validasi nomor handphone melalui SMS.

1. Pengiriman Password melalui WhatsApp

Menggunakan API WhatsApp untuk mengirimkan *password* sementara kepada pengguna. Metode ini memastikan bahwa password hanya diterima oleh pemilik nomor *handphone* yang terdaftar. Penelitian[17], [18] menunjukkan bahwa pengiriman OTP melalui WhatsApp meningkatkan keberhasilan verifikasi dan pengalaman pengguna.

1. Hashing Password dengan bcrypt

*Bcrypt* digunakan untuk mengenkripsi password sebelum disimpan di basis data. Metode ini melibatkan *hashing* *password* dengan *salt* untuk mencegah serangan *brute* *force*. Penelitian[19], [20] menunjukkan keunggulan *bcrypt* dalam melindungi password pengguna.

1. Penyimpanan Data di MongoDB

MongoDB digunakan untuk menyimpan informasi pengguna termasuk nomor *handphone*, *password* *hash*, dan waktu pembuatan *password*. Penelitian[21], [22] menunjukkan bahwa MongoDB cocok untuk manajemen data pengguna yang skalabel dan aman.

1. *Timestamp* untuk Masa Berlaku *Password*

Menyimpan *timestamp* ketika *password* dibuat dan memberikan masa berlaku tertentu untuk *password* tersebut. Penelitian[23], [24] menjelaskan bagaimana metode ini dapat meningkatkan keamanan dengan memastikan *password* hanya berlaku untuk waktu singkat.

# BAB III

# METODOLOGI PENELITIAN

1. Metodologi Penelitian

Penelitian ini menggunakan metode eksperimental dengan tahapan yang sistematis untuk mengembangkan dan menguji mekanisme verifikasi password melalui WhatsApp. Metodologi ini dirancang untuk mengoptimalkan keamanan dan kenyamanan pengguna dalam proses autentikasi di aplikasi web statis dan *Single* *Page* *Application* (SPA). Tahapan penelitian ini melibatkan beberapa langkah utama, yaitu:

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.

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 STP.

1. Implementasi Sistem

Mengimplementasikan sistem autentikasi menggunakan teknologi yang telah dipilih. *Backend* dikembangkan menggunakan bahasa pemrograman Golang dan MongoDB untuk penyimpanan data, sementara *frontend* dikembangkan menggunakan *React* untuk membangun aplikasi *web* statis dan SPA. Dengan menggunakan ekosistem seperti ini, diimplementasikan beberapa autentifikasi menggunakan beberapa metode yaitu kode QR, google, dan STP.

1. Pengujian dan Evaluasi

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

* Pengujian autentikasi menggunakan kode QR;
* Pengujian autentifikasi menggunakan google;
* Pengujian autentifikasi menggunakan STP;
* Evaluasi kinerja dan keamanan sistem.

1. Dokumentasi dan Pelaporan

Menyusun laporan penelitian yang mencakup latar belakang, metodologi, hasil, dan kesimpulan dari penelitian ini. Laporan ini juga mencakup rekomendasi untuk pengembangan lebih lanjut dan aplikasi praktis dari hasil penelitian.

## Tahapan Tahapan Diagram Metodologi Penelitian

Bagian ini akan memvisualisasikan tahapan-tahapan metodologi penelitian dalam bentuk diagram alur untuk memberikan gambaran yang jelas tentang proses penelitian. Berikut adalah diagram alur metodologi penelitian:

1. Studi Literatur

* Mengumpulkan penelitian terdahulu;
* Menganalisis metode dan hasil penelitian yang relevan.

1. Perancangan Sistem

* Merancang skema autentikasi;
* Menentukan teknologi yang digunakan (Golang, MongoDB, React, WhatsApp).

1. Implementasi Sistem

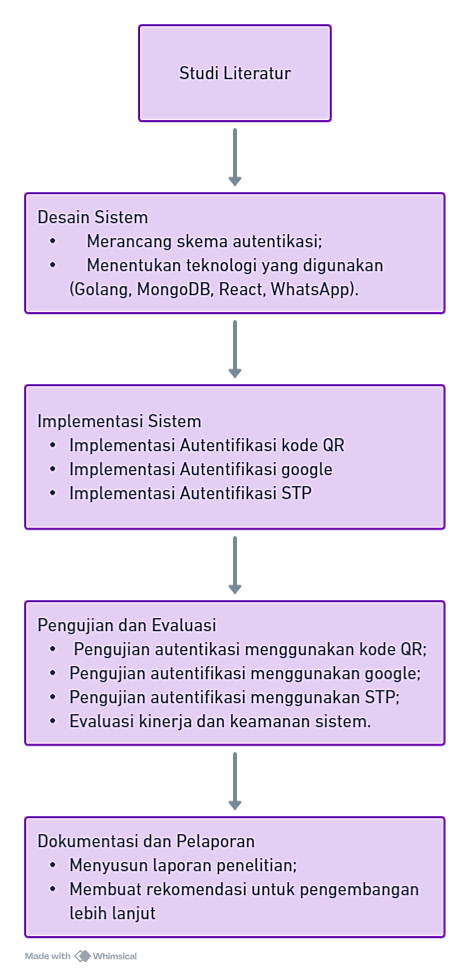
* Implementasi Autentifikasi kode QR
* Implementasi Autentifikasi google
* Implementasi Autentifikasi STP.

1. Pengujian dan Evaluasi

* Pengujian autentikasi menggunakan kode QR;
* Pengujian autentifikasi menggunakan google;
* Pengujian autentifikasi menggunakan STP;
* Evaluasi kinerja dan keamanan sistem.

1. Dokumentasi dan Pelaporan

* Menyusun laporan penelitian;
* Membuat rekomendasi untuk pengembangan lebih lanjut.



Gambar 3. 1 Diagram Alur Penelitian

# BAB IV

# EKSPERIMEN DAN HASIL

## Eksperimen

Bagian ini menjelaskan langkah-langkah dan prosedur yang diambil untuk menguji sistem autentikasi dan otorisasi yang diimplementasikan pada website statis. Pengujian dilakukan dalam tiga jenis autentikasi utama, yaitu autentikasi QR, autentikasi Google, dan autentikasi STP (*Secure Temporary Password*). Setiap jenis autentikasi diuji berdasarkan beberapa skenario untuk memastikan keamanan dan keefektifan sistem.

1. Autentikasi QR

Autentikasi QR adalah metode yang memungkinkan pengguna untuk login dengan memindai kode QR menggunakan perangkat mobile mereka. Metode ini bertujuan untuk mengurangi risiko pencurian kredensial karena tidak melibatkan input manual dari pengguna. Langkah-langkah Pengujian:

* Pengguna mengakses halaman login dan memilih opsi autentikasi QR.
* Sistem menampilkan kode QR yang unik untuk setiap sesi.
* Pengguna memindai kode QR menggunakan aplikasi otentikasi di ponsel mereka.
* Sistem memverifikasi hasil pemindaian dan mengizinkan akses jika berhasil.

1. Autentikasi Google

Autentikasi Google memanfaatkan OAuth2 untuk mengizinkan pengguna login menggunakan akun Google mereka. Metode ini memanfaatkan infrastruktur keamanan Google, sehingga meningkatkan kepercayaan dan keamanan. Langkah-langkah Pengujian:

* Pengguna mengakses halaman login dan memilih opsi autentikasi Google.
* Sistem mengarahkan pengguna ke halaman login Google.
* Pengguna memasukkan kredensial Google mereka dan memberikan izin akses.
* Sistem menerima token dari Google dan memverifikasi identitas pengguna.
* Jika verifikasi berhasil, sistem mengizinkan akses.

1. Autentikasi STP (*Secure* *Temporary* *Password*)

Autentikasi STP menggunakan *password* sementara yang dikirimkan melalui WhatsApp. Metode ini dirancang untuk mengurangi risiko pencurian *password* dengan menggunakan *password* yang berumur pendek dan dikirimkan melalui saluran yang aman. Skenario Pengujian:

1. Autentikasi Berhasil

* Pengguna mengakses halaman login dan memasukkan nomor telepon.
* Sistem mengirimkan *password* sementara ke nomor WhatsApp pengguna.
* Pengguna memasukkan *password* sementara pada halaman STP.
* Sistem memverifikasi *password* dan mengizinkan akses jika berhasil.

1. *Password* Expired

* Pengguna mengakses halaman login dan memasukkan nomor telepon.
* Sistem mengirimkan *password* sementara ke nomor WhatsApp pengguna.
* Pengguna mencoba login setelah 5 menit (masa berlaku *password* berakhir).
* Sistem menolak akses dan menampilkan pesan bahwa *password* telah kedaluwarsa.

1. Resend Password

* Pengguna mengakses halaman login dan memasukkan nomor telepon.
* Sistem mengirimkan *password* sementara ke nomor WhatsApp pengguna.
* Pengguna memilih opsi untuk mengirim ulang *password* setelah waktu tunggu habis.
* Sistem mengirimkan *password* baru dan pengguna dapat login menggunakan *password* baru tersebut.

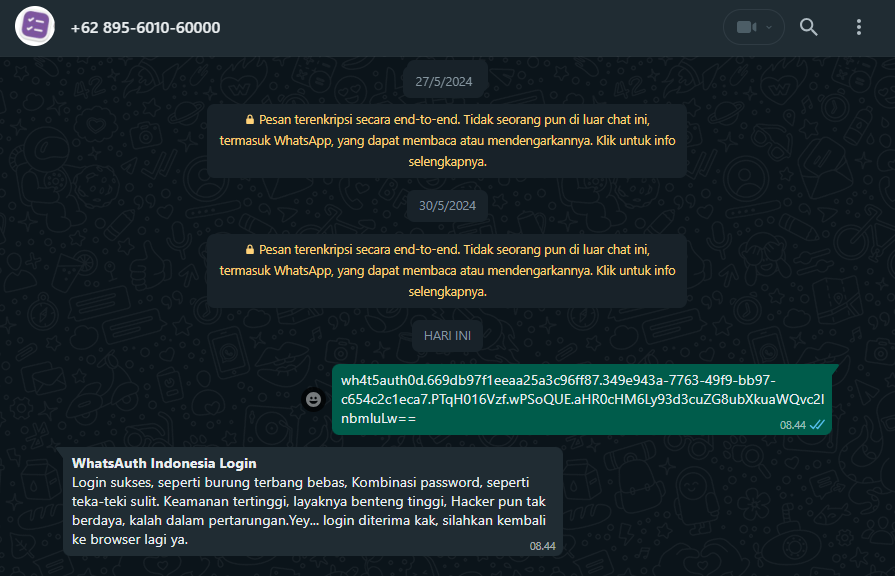
## Hasil

Bagian ini menyajikan hasil dari setiap skenario pengujian yang telah dilakukan. Hasil tersebut dianalisis untuk mengevaluasi keamanan dari setiap metode autentikasi.

1. Hasil Autentikasi QR

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

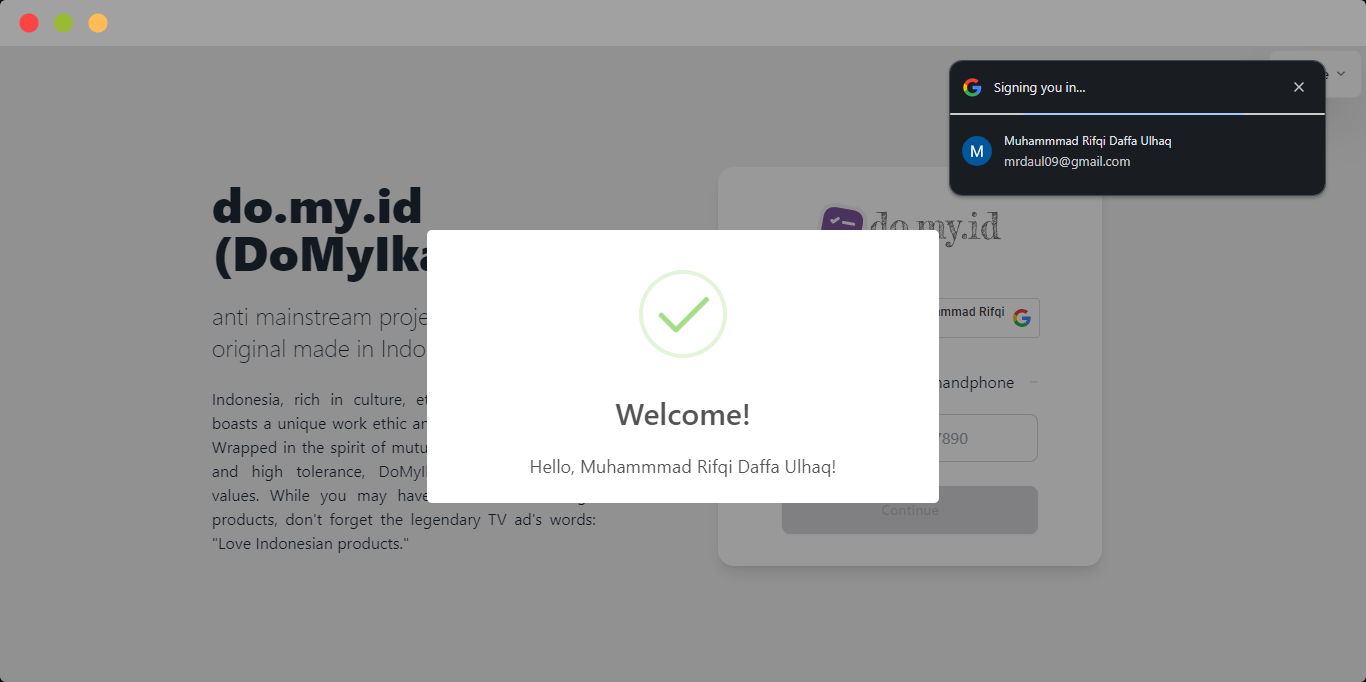




Gambar 4. 1 Hasil Autentikasi QR

1. Hasil Autentikasi Google

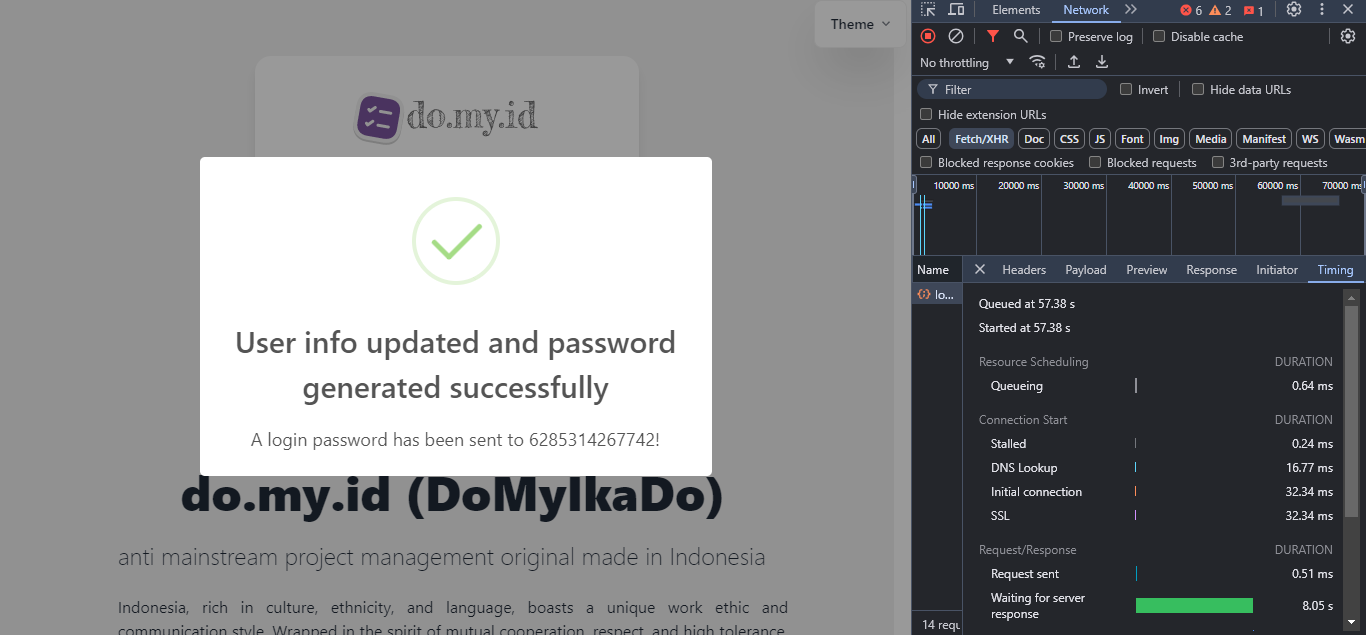
Autentikasi Google berhasil memanfaatkan infrastruktur keamanan Google untuk meningkatkan kepercayaan pengguna. Namun, risiko tetap ada jika token akses berhasil dicuri oleh pihak yang tidak berwenang.

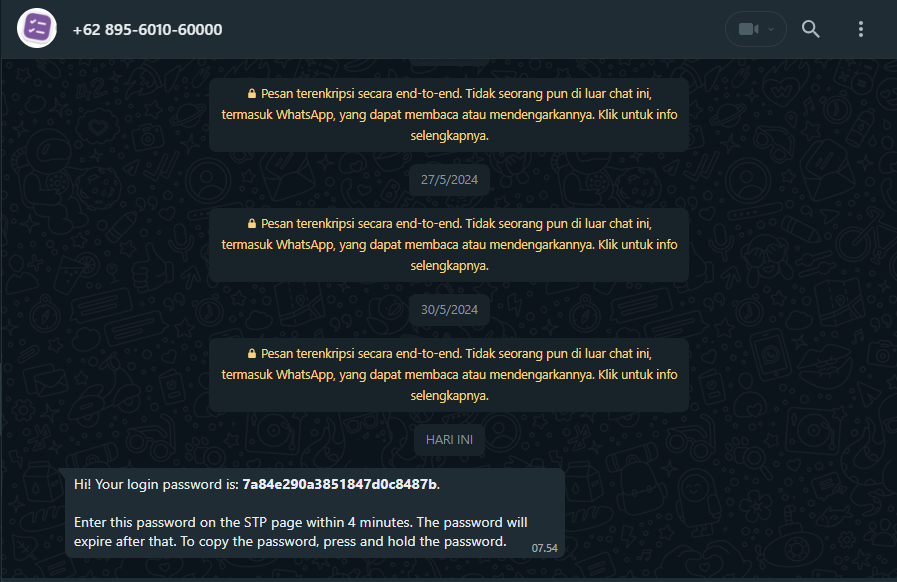


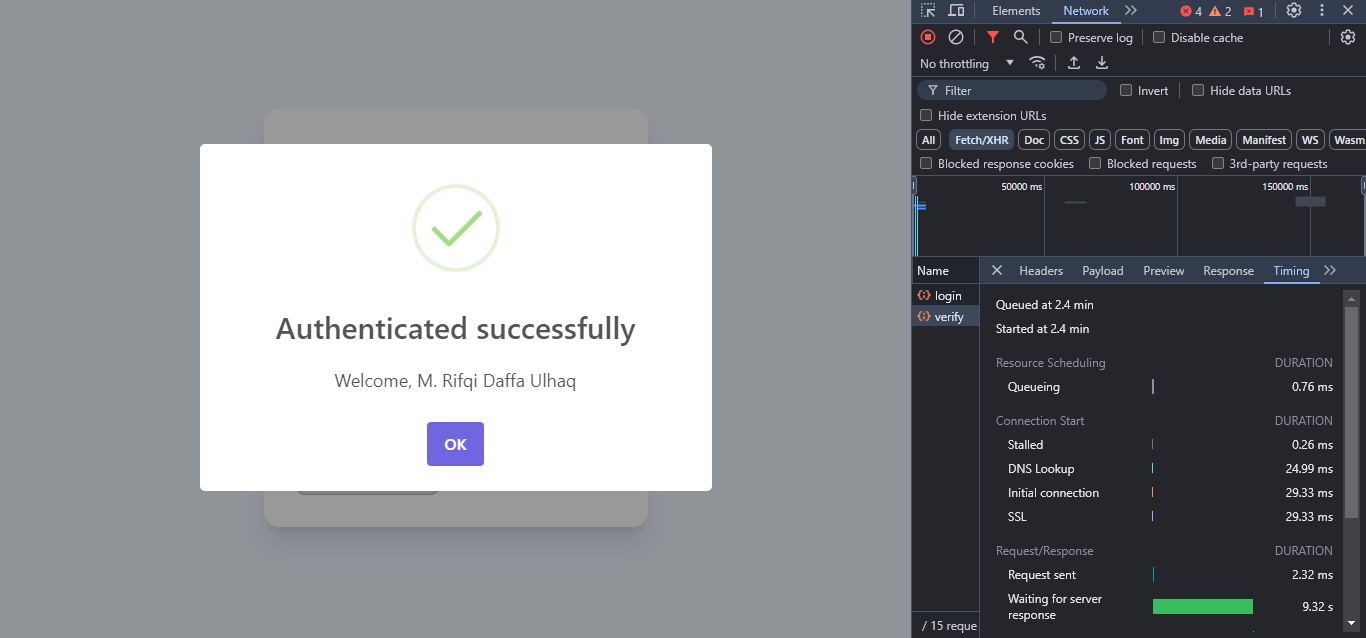
Gambar 4. 2 Hasil Autentikasi Google

1. Hasil Autentikasi STP

* Autentikasi Berhasil





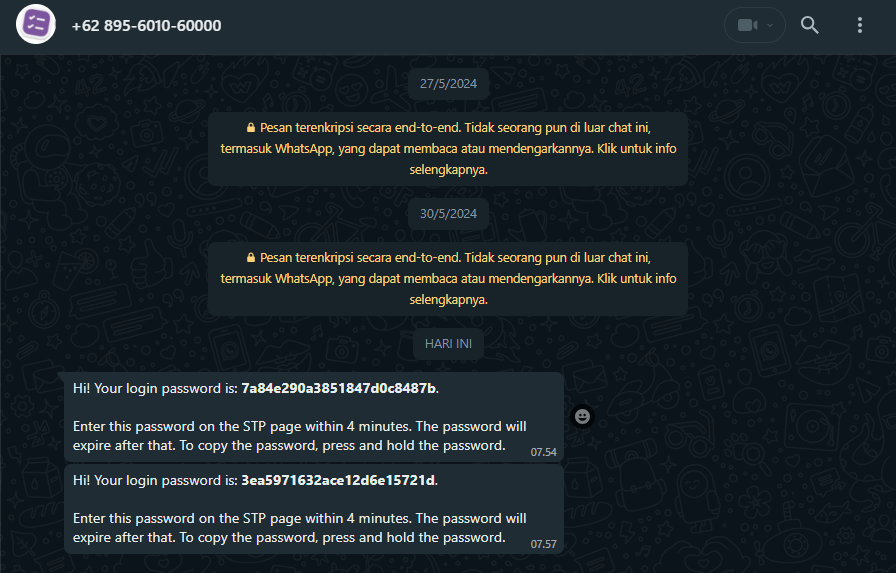


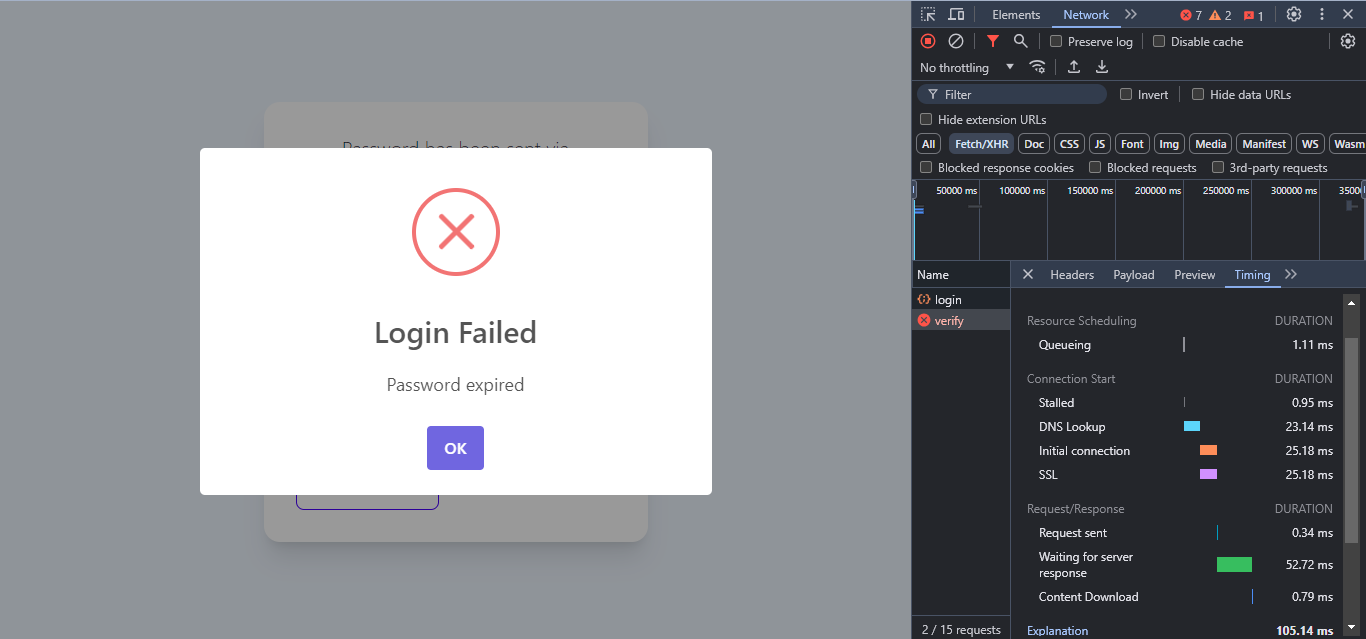
Gambar 4. 3 Skenario Autentikasi STP: Berhasil

Pengujian menunjukkan bahwa pengguna dapat login dengan sukses menggunakan password sementara yang dikirimkan melalui WhatsApp. Metode ini meningkatkan keamanan karena menggunakan durasi password valid yang singkat.

* *Password* *Expired*

Pengujian menunjukkan bahwa sistem berhasil menolak akses jika pengguna mencoba login setelah masa berlaku *password* berakhir. Hal ini menambah lapisan keamanan tambahan.

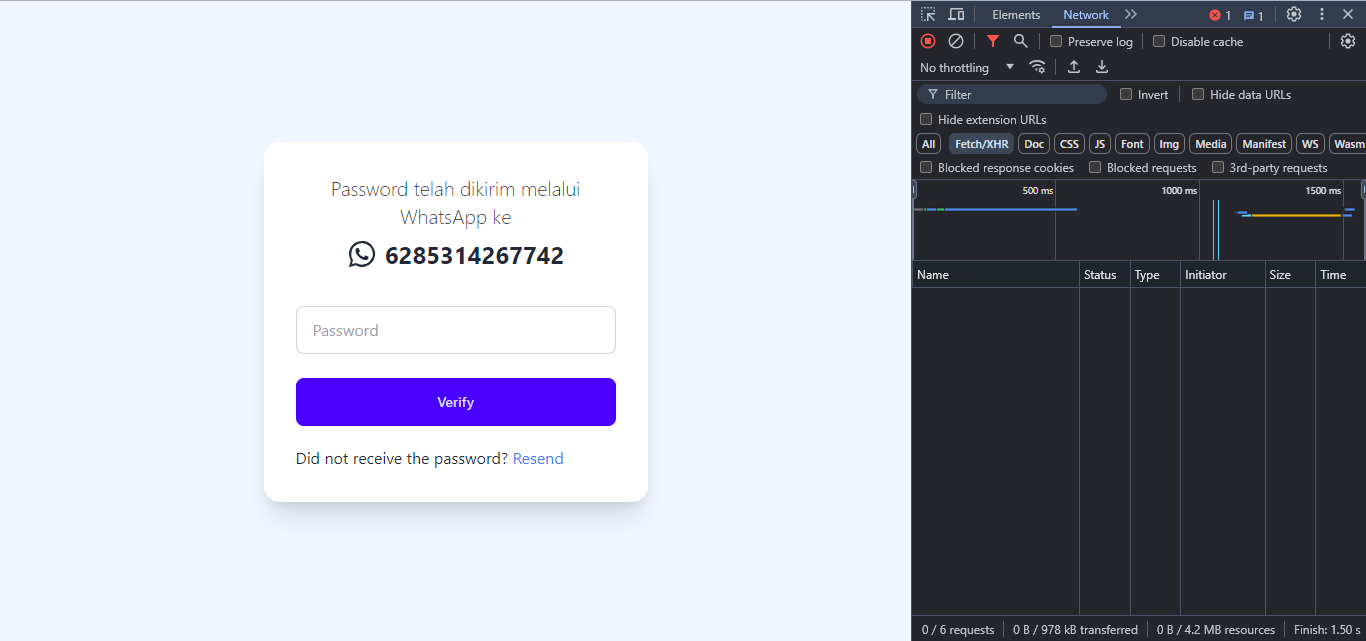


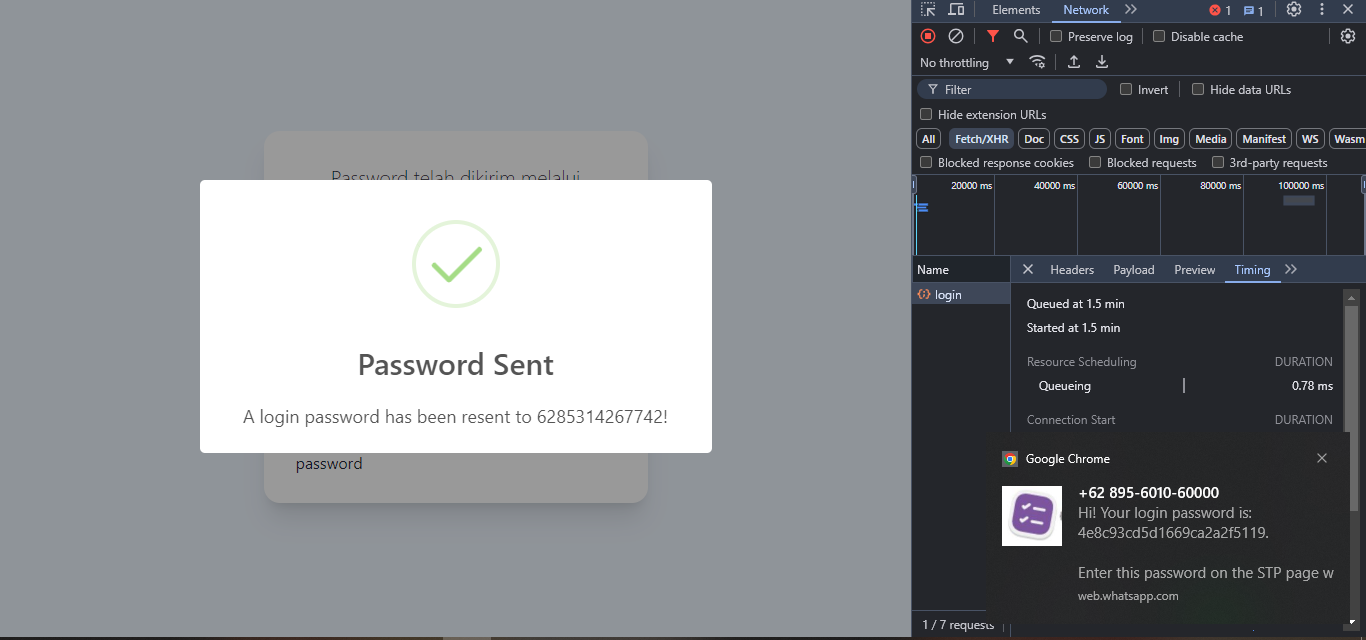


Gambar 4. 4 Skenario Autentikasi STP: Password kadaluarsa

* Resend *Password*

Pengujian menunjukkan bahwa pengguna dapat meminta pengiriman ulang *password* dan berhasil login menggunakan *password* baru. Ini menunjukkan fleksibilitas sistem dalam menangani skenario dimana pengguna tidak menerima atau lupa *password* sementara.





Gambar 4. 5 Skenario Autentikasi STP: Kirim ulang password

* Pengujian *brute* *force* dan *dictionary* *attack*

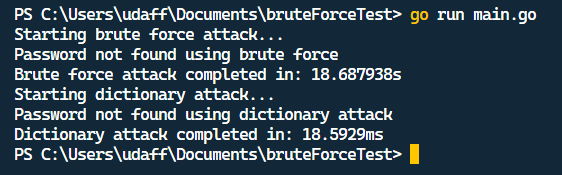
Menunjukkan bahwa *password* yang dihasilkan oleh sistem STP cukup kuat dan tidak mudah ditebak dalam waktu yang wajar. Pengujian tambahan dilakukan dengan menggunakan dua teknik utama untuk mencoba menebak *password* yang dihasilkan oleh sistem STP:

* *Brute* *Force* *Attack*

Mencoba semua kemungkinan kombinasi karakter hingga panjang tertentu.

* *Dictionary* *Attack*

Mencoba menebak *password* menggunakan daftar kata-kata yang sering digunakan sebagai password.



Gambar 4. 6 Pengujian Brute Force dan Dictionary Attack

Dan Hasil pengujian adalah sebagai berikut

Tabel 4. 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 |

Hasil pengujian menunjukkan bahwa ketiga metode autentikasi ini efektif dalam meningkatkan keamanan dan memberikan pengalaman pengguna yang lebih baik. Namun, setiap metode memiliki kekurangan dan risiko yang perlu diperhatikan untuk peningkatan di masa depan. Selain itu, hasil dari pengujian dengan *brute* *force* dan *dictionary* *attack* juga menunjukkan, bahwa *password* yang dihasilkan oleh sistem STP cukup kuat dan tidak mudah ditebak menggunakan kedua metode tersebut dalam waktu yang wajar. Hal ini menunjukkan bahwa sistem STP yang dikembangkan mampu memberikan keamanan yang tinggi terhadap serangan *brute* *force* dan *dictionary* *attack*.

# BAB V

# KESIMPULAN

## Kesimpulan Masalah

Bagian ini merangkum kesimpulan dari permasalahan yang diidentifikasi selama penelitian. Kesimpulan ini akan menjawab permasalahan yang telah diuraikan di bagian sebelumnya.

1. Bagaimana mengamankan autentikasi dan otorisasi *user* pada *website* statis?

Penelitian ini berhasil mengimplementasikan skema autentikasi dan otorisasi yang aman pada *website* statis menggunakan berbagai metode autentikasi, seperti autentikasi QR, autentikasi Google, dan autentikasi STP. Setiap metode telah diuji dan menunjukkan efektivitas dalam mengamankan akses pengguna.

1. Bagaimana menghitung resiko keamanan yang terjadi dari setiap skema autentikasi dan otorisasi?

Penelitian ini juga menganalisis resiko keamanan dari setiap skema autentikasi yang digunakan. Metode yang diterapkan terbukti dapat mengurangi resiko pembobolan akun dengan memanfaatkan faktor autentikasi tambahan seperti pengiriman *password* melalui WhatsApp.

## Kesimpulan Metode

Bagian ini menyimpulkan metode yang digunakan dalam penelitian ini. Kesimpulan ini akan menilai efektivitas metode yang diterapkan dalam mencapai tujuan penelitian.

1. Metode Autentikasi dan Otorisasi pada *Website* Statis

Skema autentikasi dan otorisasi yang dikembangkan mencakup berbagai metode yang sesuai untuk *website* statis, seperti autentikasi QR, autentikasi Google, dan autentikasi STP. Implementasi metode ini terbukti meningkatkan keamanan tanpa mengurangi kenyamanan pengguna.

1. Menghitung Resiko Pembobolan Akun

Dengan menghitung resiko pembobolan akun dari setiap metode autentikasi, penelitian ini berhasil mengidentifikasi metode yang paling efektif dan aman untuk diterapkan pada *website* statis. Hasilnya menunjukkan bahwa kombinasi berbagai metode autentikasi dapat mengurangi resiko pembobolan akun secara signifikan.

## Kesimpulan Eksperimen

Bagian ini menyimpulkan hasil eksperimen yang telah dilakukan selama penelitian. Kesimpulan ini akan menilai keberhasilan sistem berdasarkan hasil pengujian yang telah dilakukan.

1. Autentikasi QR

Eksperimen autentikasi QR menunjukkan bahwa metode ini sangat efektif dalam mengamankan akses pengguna. Namun, metode ini memerlukan perangkat tambahan seperti ponsel yang mendukung QR *code* *scanner*.

1. Autentikasi Google

Autentikasi menggunakan Google *Sign*-*In* terbukti mudah digunakan dan aman. Metode ini memanfaatkan infrastruktur keamanan Google, yang sudah terbukti handal dalam menangani autentikasi pengguna.

1. Autentikasi STP

* Berhasil

Pengguna yang memasukkan *password* dengan benar dalam batas waktu yang ditentukan dapat berhasil masuk ke sistem.

* *Password* Kedaluwarsa

Jika password telah *kedaluwarsa*, pengguna harus meminta *password* baru.

* 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.

1. Pengujian *Brute* *Force* dan *Dictionary* *Attack*

Pengujian tambahan dengan *brute* *force* dan *dictionary* *attack* menunjukkan bahwa *password* yang dihasilkan oleh sistem STP cukup kuat dan tidak mudah ditebak dalam waktu yang wajar. Hal ini menunjukkan bahwa sistem STP yang dikembangkan mampu memberikan keamanan yang tinggi terhadap serangan tersebut.

Kesimpulan dari penelitian ini menunjukkan bahwa metode yang diterapkan efektif dalam mengatasi permasalahan yang diidentifikasi. Sistem autentikasi yang dirancang berhasil meningkatkan keamanan dan efisiensi, serta memberikan pengalaman pengguna yang lebih baik. Implementasi teknologi yang digunakan, seperti *Bcrypt*, MongoDB, *React*, dan WhatsApp, terbukti berhasil dalam mencapai tujuan penelitian.

# BAB VI

# SARAN

Bagian ini memberikan saran untuk pengembangan lebih lanjut berdasarkan temuan penelitian. Saran ini bertujuan untuk meningkatkan sistem yang telah dikembangkan serta mengatasi kendala yang mungkin dihadapi di masa mendatang.

* Penggunaan *Embedded* *Message* di WhatsApp

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. Hal ini dapat mengurangi kesalahan pengguna dalam menyalin password dan mempercepat proses login.

* Pengembangan Fitur *Multi*-*Factor* *Authentication* (MFA)

Meskipun sistem autentikasi saat ini telah cukup aman, penambahan fitur MFA dapat meningkatkan keamanan lebih lanjut. Pengguna dapat memverifikasi identitas mereka melalui metode tambahan seperti kode OTP yang dikirim melalui SMS atau *email*.

* Optimisasi Performa Sistem

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.

* Integrasi dengan Layanan Pihak Ketiga

Menambahkan integrasi dengan layanan pihak ketiga seperti Github untuk opsi login dapat meningkatkan fleksibilitas dan kenyamanan pengguna. Pengguna dapat memilih metode login yang paling sesuai dengan preferensi mereka.

* Peningkatan UX/UI

Meningkatkan desain antarmuka pengguna (UI) dan pengalaman pengguna (UX) agar lebih intuitif dan mudah digunakan. Melakukan pengujian dengan pengguna (*user* *testing*) untuk mendapatkan *feedback* langsung dapat membantu dalam perbaikan desain.

* Penerapan Teknik *Machine* *Learning*

Menggunakan teknik *machine* *learning* untuk mendeteksi pola penggunaan yang mencurigakan dan mencegah akses yang tidak sah. Algoritma *machine* *learning* dapat membantu dalam meningkatkan keamanan sistem secara otomatis.

* Penyempurnaan Dokumentasi

Menyediakan dokumentasi yang lebih lengkap dan mudah dipahami bagi pengembang lain yang mungkin akan mengembangkan sistem ini lebih lanjut. Dokumentasi yang baik akan mempermudah proses pengembangan dan pemeliharaan di masa mendatang.

* Penelitian Lanjutan

Melakukan penelitian lanjutan untuk mengeksplorasi metode autentikasi lain yang lebih aman dan efisien. Penggunaan teknologi terbaru dan pendekatan inovatif dapat membantu dalam terus meningkatkan keamanan dan kenyamanan pengguna.

Dengan implementasi saran-saran di atas, diharapkan sistem autentikasi ini dapat terus berkembang dan memberikan keamanan serta kenyamanan yang lebih baik bagi pengguna. Penelitian ini telah menunjukkan potensi besar dalam penggunaan teknologi untuk meningkatkan keamanan dan efisiensi dalam autentikasi pengguna, dan masih banyak ruang untuk pengembangan lebih lanjut.

# 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] 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.

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

[5] 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.

[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.-J. Chae, K.-B. Kim, and H.-J. Cho, “A study on secure user authentication and authorization in OAuth protocol,” *Cluster Comput*, vol. 22, Jul. 2019, doi: 10.1007/s10586-017-1119-6.

[10] B. Gao, F. Liu, S. Du, and F. Meng, “An OAuth2.0-Based Unified Authentication System for Secure Services in the Smart Campus Environment,” in *Computational Science – ICCS 2018: 18th International Conference, Wuxi, China, June 11–13, 2018 Proceedings, Part III*, Berlin, Heidelberg: Springer-Verlag, 2018, pp. 752–764. doi: 10.1007/978-3-319-93713-7\_73.

[11] 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.

[12] 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.

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

[14] 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

[15] Association for Computing Machinery, USENIX Association, Google (Firm), Facebook (Firm), and Mozilla Foundation, *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security (SOUPS ’19) : Santa Clara, CA, USA, August 12 - 13, 2019,*.

[16] O. Olaleye, A. Olaniyan, O. Eboda, and A. Awolere, “SMS-Based Event Notification System,” vol. 3, no. 10, 2013, [Online]. Available: www.iiste.org

[17] 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.

[18] 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.

[19] G. Hatzivasilis, “Password Management: How Secure Is Your Login Process?,” in *International workshop on model-driven simulation and training environments for cybersecurity*, 2020, pp. 157–177.

[20] C. Skanda, B. Srivatsa, and B. S. Premananda, “Secure Hashing using BCrypt for Cryptographic Applications,” in *2022 IEEE North Karnataka Subsection Flagship International Conference (NKCon)*, 2022, pp. 1–5.

[21] S. Dwivedi, R. Balaji, P. Ampatt, and S. D. Sudarsan, “A Survey on Security Threats and Mitigation Strategies for NoSQL Databases: MongoDB as a Use Case,” in *International Conference on Information Systems Security*, 2023, pp. 57–76.

[22] A. Kanade and S. Kanade, “A Study of Mongodb Data Models and a Novel Hybrid Data Modeling Approach,” in *2021 5th International Conference on Trends in Electronics and Informatics (ICOEI)*, 2021, pp. 1554–1562.

[23] M. I. M. Metilda, D. Lalitha, and S. Vaithyasubramanian, “Data security-web login authentication process using password generating tile array token interval timed coloured Petri nets,” *International Journal of Wireless and Mobile Computing*, vol. 24, no. 2, pp. 134–143, 2023.

[24] Z. Yang, C. Jin, J. Ning, Z. Li, A. Dinh, and J. Zhou, “Group time-based one-time passwords and its application to efficient privacy-preserving proof of location,” in *Proceedings of the 37th Annual Computer Security Applications Conference*, 2021, pp. 497–512.