Jurnal Manajemen Informatika (JAMIKA)
Volume 15 Nomor 1 Edisi April 2025
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

Implementasi *Multi-Factor Authentication* Untuk Optimalisasi Keamanan Akses Data

Implementation of Multi-Factor Authentication for Optimizing Data Access Security

Haeruddin[1], **Stefanus Eko Prasetyo**[2*], **Avista Mindy**[3]
Program Studi Teknologi Informasi, Universitas Internasional Batam, Batam, Indonesia
*E-mail: stefanus@uib.ac.id

Abstrak

Penelitian ini mengeksplorasi penerapan Multi-Factor Authentication (MFA) sebagai langkah strategis untuk meningkatkan keamanan data di PT. ABC, dimana sistem online PT. ABC sebelumnya hanya mengandalkan metode autentikasi tradisional berupa username dan password. Dalam konteks peningkatan pesat pengguna internet pasca pandemi Covid-19, keamanan data menjadi isu yang sangat mendesak. Melalui metode observasi, wawancar, dan pendekatan Network Development Life Cycle (NDLC), penelitian ini mengidentifikasi kelemahan keamanan yang ada dan mengusulkan solusi berbasis MFA menggunakan layanan Auth0. Implementasi ini diuji melalui penetrasi sistem menggunakan alat Burp Suite untuk memastikan ketahanan terhadap serangan siber. Hasil penelitian menunjukkan bahwa penerapan MFA secara signifikan meningkatkan perlindungan terhadap akses tidak sah, serta meningkatkan kesadaran keamanan di kalangan karyawan. Penelitian ini menggarisbawahi pentingnya adopsi teknologi autentikasi canggih sebagai bagian integral dari strategi keamanan data perusahaan untuk menghadapi tantangan siber yang semakin kompleks.

Kata kunci: *Multi-Faktor Autentikasi, Keamanan Siber, Auth0, Burp Suite, Tes Penetrasi.*

Abstract

This study explores the implementation of Multi-Factor Authentication (MFA) as a strategic measure to enhance data security at PT. ABC, where the company's online system previously relied solely on traditional authentication methods such as usernames and passwords. In the context of the rapid increase in internet users following the Covid-19 pandemic, data security has become a critical issue. Through observation, interviews, and the Network Development Life Cycle (NDLC) approach, this study identifies existing security vulnerabilities and proposes an MFA-based solution using the Auth0 service. The implementation was tested through system penetration using the Burp Suite tool to ensure resilience against cyber attacks. The results demonstrate that the implementation of MFA significantly improves protection against unauthorized access and increases security awareness among employees. This study highlights the importance of adopting advanced authentication technology as an integral part of a company's data security strategy to address increasingly complex cyber challenges.

Keywords: *Multi-Factor Authentication, Cybersecurity, Auth0, Burp Suite, Penetration Testing*.

Naskah diterima 07 Okt. 2024; direvisi 17 Des. 2024; dipublikasikan 01 Apr. 2025.

I. PENDAHULUAN

Perkembangan teknologi terus meningkat terutama setelah kondisi pandemik Covid-19. Hal ini berperan pada peningkatan pengguna internet di Indonesia yang naik hingga 20%[1]. Sebagian besar aktivitas masyarakat saat itu dilakukan di media online yang memerlukan koneksi internet. Menurut laporan Digital Global Statshot April 2022 oleh Simon Kemp bersama We Are Social dan juga Hootsuite [2] bahwa jumlah pengguna internet di dunia mencapai 5 miliar pengguna atau setara dengan 63% dari populasi dunia. Berdasarkan survei Asosiasi Penyelenggara Jasa Internet Indonesia, data tingkat penggunaan internet di Indonesia pada tahun 2023 sebesar 78,19%. Angka tersebut terus meningkat sebesar 1,17% dari tahun 2022 [3]. Kemajuan perkembangan teknologi ini telah membawa berbagai kemudahan dalam mendapatkan informasi dengan cepat dan akurat.

Kecepatan dalam mengakses informasi menjadi faktor krusial, terutama dalam konteks bisnis. Perusahaan harus mampu mengelola informasi dengan efisien dan cepat untuk meningkatkan efektivitas kerja. Namun, sistem online semakin sering menjadi sasaran serangan siber yang bertujuan meretas akun pengguna serta mengakses data atau sumber daya yang bersifat rahasia [4]. Data elektronik pun menjadi barang berharga yang sering dicuri, dan kecenderungan kebocoran data mengalami peningkatan, baik dari segi kuantitas

maupun motif, antara tahun 2005 hingga 2018 [5]. Dengan demikian, sangat diperlukan sebuah sistem yang mampu mengolah data secara aman, mengingat data merupakan aset penting dalam proses bisnis [6].

Kontrol akses menerapkan kebijakan yang memastikan pengguna hanya dapat beroperasi sesuai dengan izin yang diberikan. Jika terjadi kegagalan, hal ini biasanya dapat menyebabkan pengungkapan informasi tanpa izin, modifikasi, atau penghancuran data, serta memungkinkan pengguna menjalankan fungsi bisnis di luar wewenang mereka [7]. Di Indonesia pemberitaan terkait sejumlah pelanggaran keamanan dan kebocoran data menjadi hal yang menjadi perhatian semua pihak termasuk perusahaan dan penyedia layanan digital. Berdasarkan Liputan6.com, di sepanjang tahun 2022 [8], pemberitaan tentang pencurian data terus terjadi bahkan hingga saat ini. Laporan dari Identity Theft Resource Center mengungkapkan di satu sisi situasi global keamanan data cukup mengkhawatirkan. Terjadi penurunan dalam jumlah pelanggaran data secara keseluruhan sepanjang tahun 2022 dibandingkan dengan tahun sebelumnya, namun jumlahnya masih sangat besar [9]. Pertumbuhan pengguna dan data yang eksponensial mengharuskan kita untuk lebih peduli dengan kemanan data online dan masalah kontrol akses pada akun pengguna [10].

Dalam menyikapi hal ini, salah satu hal yang paling penting dalam upaya menjaga keamanan data adalah proses autentikasi. Autentikasi menjadi sebuah dasar dalam penerapan perlindungan terhadap akses tidak sah ke perangkat atau aplikasi [11]. Untuk otentikasi pengguna di sistem online, metode tradisional dan modern seperti kata sandi, PIN, dan One Time Password (OTP) sering digunakan [4]. Dalam konteks ini, penggunaan metode autentikasi yang lebih canggih menjadi krusial. Multi Factor Authentication (MFA), adalah salah satu solusi yang cukup efektif. Selain menggunakan nama pengguna dan kata sandi tradisional yang umum dilakukan, MFA mengharuskan pengguna memasukkan beberapa bentuk kode atau data tambahan yang hanya mereka sendiri yang memiliki kode tersebut [12]. Akses sistem online yang menggunakan MFA lebih sulit untuk ditembus secara ilegal dibandingkan situs yang hanya mengautentikasi penggunanya dengan satu faktor seperti kata sandi. Autentikasi berbasis kata sandi tetap menjadi metode autentikasi yang paling umum. Namun, metode ini memiliki kerentanan, terutama ketika menggunakan kata sandi yang sederhana, serta praktik penggunaan kata sandi yang sama di berbagai layanan. Hal ini dapat menyebabkan risiko serangan seperti tebakan kata sandi atau serangan berdasarkan kamus (dictionary attack)[13].

Peningkatan konektivitas dan eksposur data secara online telah membuka pintu bagi berbagai tantangan dan risiko siber. Oleh karena itu, penelitian ini berfokus pada upaya investigasi isu-isu keamanan data yang muncul dalam lingkungan PT. ABC dimana tidak ada penerapan MFA ketika memasuki sistem dan hanya menggunakan username dan password saja sehingga akses sistem lebih mudah untuk ditembus. Maka dari itu fokus pada metode autentikasi MFA sebagai salah satu solusi untuk meningkatkan keamanan akses pengguna terhadap data dan sistem di PT. ABC akan didemonstrasikan. Pada penerapannya juga dilakukan pengujian penetrasi untuk melakukan pengujian keamanan dan mendapatkan perbandingan dari beberapa jenis autentikasi MFA yang akan disesuaikan dengan kebutuhan sistem PT. ABC. Pada penerapannya, juga dilakukan pengujian penetrasi untuk melakukan pengujian keamanan.

Walaupun banyak penelitian telah mengkaji efektivitas dan kelemahan metode MFA, masih ada kekurangan dalam penerapan skema MFA yang menyeluruh, terutama di sektor-sektor. Nugroho et al. meneliti keamanan Service Oriented Architecture dengan OAuth 2.0 dan JSON Web Token, tetapi fokus mereka tidak sepenuhnya pada MFA menggunakan Auth0 [14]. Moepi dan Mathonsi menunjukkan peningkatan keamanan dengan skema MFA lima faktor di perbankan online, namun belum mencakup evaluasi penerapan MFA pada lingkungan perusahaan [15]. Hussain et al. membandingkan efektivitas MFA dan di lingkungan multi-cloud, tetapi penelitian mereka lebih menitikberatkan pada peningkatan keamanan [16]. Ariffin et al. mengidentifikasi kelemahan dalam skema MFA berbasis SMS dan panggilan telepon, tanpa menyoroti penggunaan aplikasi otentikasi modern seperti yang dilakukan dalam penelitian ini [17]. Dari keempat artikel penelitian sebelumnya [14][15][16][17] juga tidak ada yang melakukan analisis pengujian keamanan. Dengan demikian, penelitian ini mengisi kesenjangan dengan mengimplementasikan dan mengevaluasi metode MFA yang lebih canggih dan spesifik, termasuk Auth0, serta melakukan pengujian penetrasi menyeluruh untuk meningkatkan keamanan sistem di PT. ABC. Kontribusi signifikan dari penelitian ini adalah pemahaman yang lebih baik mengenai implementasi MFA dalam konteks perusahaan, yang mencakup penyediaan model implementasi MFA yang dapat diadopsi oleh perusahaan lain, identifikasi kelemahan dalam metode autentikasi tradisional, dan peningkatan kesadaran akan pentingnya keamanan data di kalangan karyawan melalui pelatihan dan implementasi teknis yang praktis. Namun, penelitian ini juga memiliki keterbatasan, di mana ruang lingkupnya terbatas pada PT. ABC, pengujian penetrasi dilakukan dengan Burp Suite yang mungkin tidak mencakup semua potensi kerentanan, serta tidak mempertimbangkan faktor-faktor eksternal yang dapat mempengaruhi keamanan data.

Jurnal Manajemen Informatika (JAMIKA)
Volume 15 Nomor 1 Edisi April 2025
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

II. METODE PENELITIAN

Pengumpulan data dilakukan dengan menggunakan beberapa cara, yaitu :

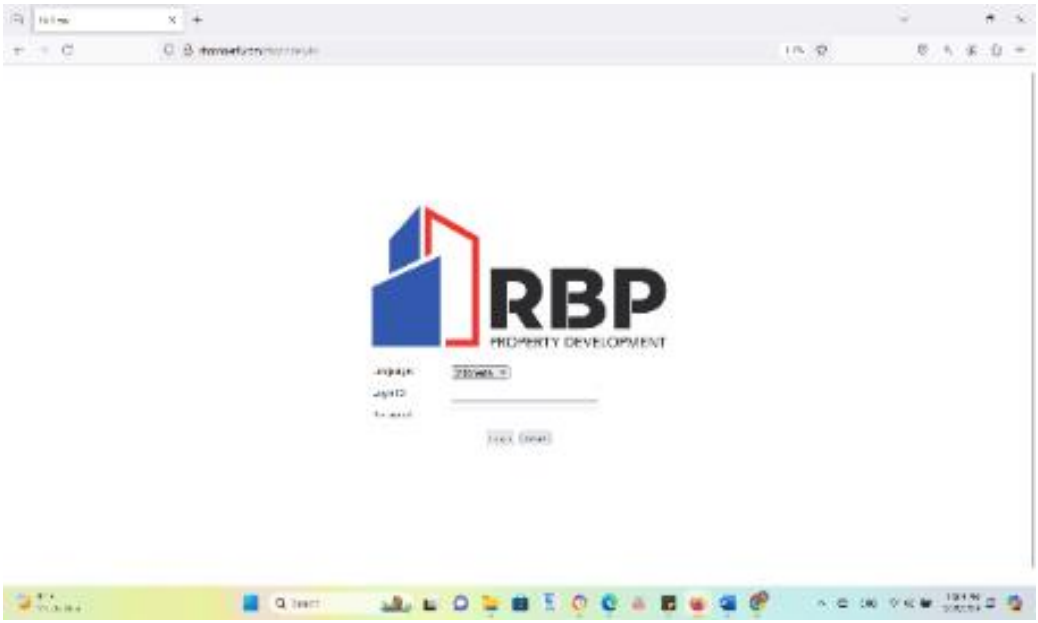
1. Wawancara dilakukan dengan mewawancarai karyawan yang memiliki kebijakan untuk mengakses sistem online PT. ABC. Tujuan dari wawancara ini adalah untuk memahami prosedur akses sistem, kendala yang dihadapi, dan kejadian atau risiko yang pernah terjadi. Berikut Tabel 1 mengenai divisi dan jumlah karyawan PT. ABC yang memiliki akses ke sistem online tersebut.

TABEL 1
JUMLAH KARYAWAN YANG MEMILIKI AKSES KE SISTEM ONLINE PT. ABC

No.	Divisi	Jumlah Karyawan
1.	Direktur	1
2.	Admin	1
3.	Finance	2
4.	Marketing	2

Adapun informasi yang didapatkan mengenai sistem online PT. ABC adalah sebagai berikut:
   a. Prosedur akses sistem online PT. ABC.
   b. Kendala dan tantangan yang dihadapi dalam pengelolaan sistem online.
   c. Kejadian ataupun risiko yang pernah terjadi.

2. Observasi, pada tahap ini, dilakukan dengan mengamati secara langsung sistem online PT. ABC, untuk melihat risiko apa yang pernah terjadi. Observasi langsung dilakukan ke sistem online PT. ABC secara mandiri setelah diberi izin akses dari perusahaan.



Gambar 1. Tampilan login page sistem online PT.ABC

Pada sistem online ini, ketika dilakukan proses login, dapat dilihat pada Gambar 1, hanya membutuhkan username dan password, tanpa adanya autentikasi tambahan, sehingga pengguna dapat langsung mengakses homepage.

Setelah dilakukan wawancara lebih lanjut dengan karyawan PT. ABC, pada riwayat login yang dilakukan oleh karyawan PT.ABC akan selalu tercatat siapa yang mengedit, menghapus ataupun menambah data. Sehingga bila salah satu pihak mencoba mengedit menggunakan username dan password dari pihak lain, maka yang tercatat dalam riwayat adalah user dari username yang dipakai.

Dari hasil observasi ini, dapat disimpulkan bahwa sistem online PT· ABC memiliki celah keamanan yang memungkinkan penyalahgunaan kredensial oleh pihak tidak berwenang. Oleh karena itu, metode Network Development Life Cycle (NDLC) dipilih untuk mengembangkan solusi keamanan berbasis autentikasi multi-faktor. Metode NDLC digunakan karena menyediakan pendekatan sistematis yang meliputi tahapan

Jurnal Manajemen Informatika (JAMIKA)
Volume 15 Nomor 1 Edisi April 2025
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

analisis kebutuhan, desain, implementasi, dan evaluasi yang relevan untuk meningkatkan keamanan sistem online PT. ABC secara menyeluruh.

Pada tahap ini juga dilakukan identifikasi kebutuhan perangkat yang mendukung proses implementasi penelitian ini sebagaimana tercantum pada Tabel 2 berikut:

TABEL 2
KEBUTUHAN PERANGKAT

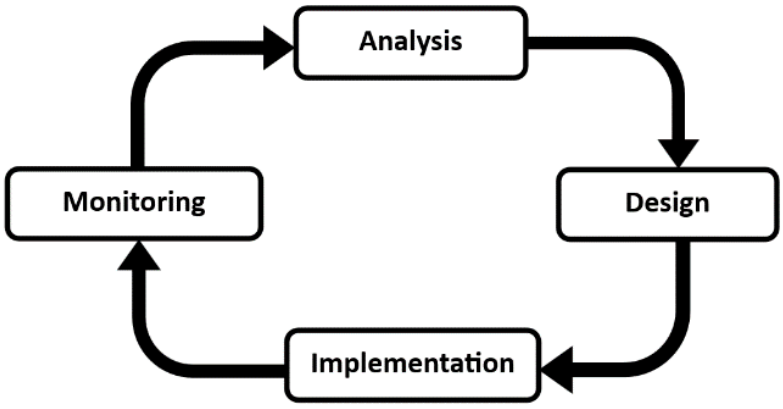
No.	Device	Spesifikasi
1.	Laptop / PC	- Asus Tuf Gaming F15 - RAM 16 GB - SSD 512 GB
2.	Sistem Operasi	Windows 11 Home Single Language
3.	Script website	Wordpress
4.	MFA Tools	Auth0
5.	Penetrasi Testing Tools	Burpsuite
6.	Domain	avistatest.authentication.my.id

3. Studi pustaka dilakukan dengan mencari berbagai sumber terkait dengan tema penelitian.

Network Development Life Cycle (NDLC)

Network Development Life Cycle (NDLC) adalah metode yang berguna untuk mengembangkan jaringan dengan melalui beberapa proses, seperti analisis, desain, implementasi, hingga pemantauan [18]. NDLC merupakan suatu metode untuk membangun sistem jaringan secara terstruktur, dimana pada setiap langkahnya mempunyai tujuan dan hasil masing-masing. NDLC bergantung pada proses pengembangan lain yang terjadi sebelumnya, seperti perencanaan strategi bisnis, siklus hidup pengembangan aplikasi, dan analisis distribusi data.

Dalam penelitian ini, digunakan pendekatan model *Network Development Life Cycle* (NDLC) yang dapat digambarkan dalam bentuk diagram pada Gambar 2 sebagai berikut:



Gambar 2. Tahapan NDLC

Tahapan dalam metode ini, yaitu:

a. Analysis

Pada tahap ini akan dilakukan analisis masalah ada di sistem online PT. ABC. Oleh karena itu akan dilakukan beberapa cara, yaitu:

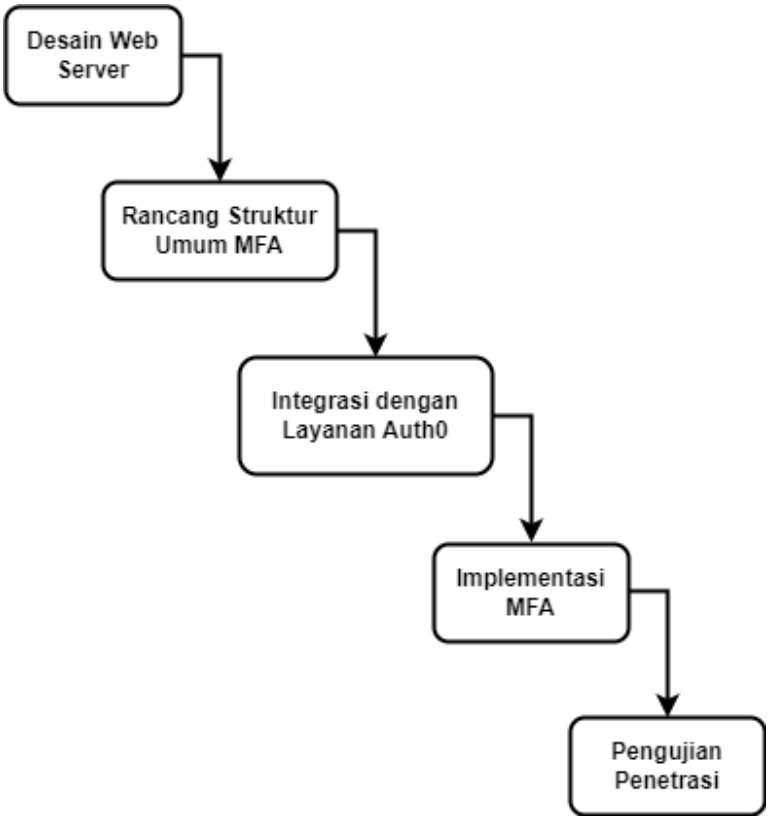
1. Analisis masalah yang muncul
   Identifikasi masalah atau kelemahan yang muncul pada sistem online PT. ABC. Masalah tersebut dapat berkaitan dengan keamanan data, kinerja, fungsionalitas, atau aspek lain dari sistem.
2. Menganalisis Kelemahan Keamanan Data yang Sudah Ada
   Tinjau kelemahan keamanan data yang sudah ada dalam sistem online PT. ABC. Ini dapat meliputi kerentanan pada aplikasi, kebijakan keamanan yang lemah, atau praktik keamanan yang buruk.
3. Observasi Langsung dengan Pihak PT. ABC
   Lakukan observasi langsung terhadap penggunaan sistem online PT. ABC di lokasi untuk memahami bagaimana sistem digunakan dalam konteks nyata. Observasi ini dapat memberikan wawasan tentang

cara kerja pengguna dengan sistem, tantangan yang mereka hadapi, dan potensi risiko keamanan yang mungkin terjadi.

4. Wawancara Secara Langsung dengan Karyawan PT. ABC
   Melakukan wawancara langsung dengan karyawan PT. ABC untuk mendapatkan pemahaman lebih dalam tentang pengalaman mereka dalam menggunakan sistem online, masalah yang mereka hadapi, dan saran mereka untuk meningkatkan keamanan data. Wawancara ini juga dapat mengungkapkan kesadaran mereka terhadap praktik keamanan dan tingkat pemahaman mereka tentang risiko keamanan.

b. Design

Tahap desain ini dapat mencakup desain integrasi dengan infrastruktur yang ada, desain akses data, dan lain sebagainya yang akan memperjelas proyek yang akan dibuat. Hal ini harus menunjukkan gambaran lengkap tentang kebutuhan.



Gambar 3. Tahapan Desain

Dapat dilihat pada Gambar 3 yang merupakan tahapan perancangan didalam penelitian ini, dimulai dengan perancangan struktur umum MFA yang akan diimplementasikan menggunakan layanan *Auth0* untuk meningkatkan keamanan dan kegunaan sistem online di situs *WordPress*. Proses ini melibatkan perencanaan struktural yang cermat, dengan fokus pada aspek penting seperti integrasi antara layanan *Auth0* dengan situs *WordPress*, konfigurasi kebijakan MFA, pengguna, dan faktor, serta adaptasi optimal terhadap kebutuhan pengguna. Desain ini bertujuan untuk menciptakan landasan yang kuat bagi penerapan MFA yang efektif dan sesuai dengan konteks spesifik lingkungan kantor, memastikan keamanan dan akses web yang tepercaya.

Setelah implementasi MFA berhasil dilakukan, selanjutnya menerapkan penetrasi testing untuk menguji keamanan dari layanan *Auht0*.

c. Implementation

Pada tahap implementasi seluruh rencana dan desain yang telah dibuat sebelumnya akan diimplementasikan. Fokus utama pada implementasi MFA menggunakan layanan *Auth0* sesuai dengan

Jurnal Manajemen Informatika (JAMIKA)
Volume 15 Nomor 1 Edisi April 2025
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

perancangan struktur sebelumnya dan kemudian menggunakan layanan *Burp Suite* untuk melakukan pengujian penetrasi.

Tahap ini dilakukan 2 implementasi, sebagai berikut:

1. Implementasi Multi Factor Authentication

   Implementasi MFA pada penelitian ini akan menggunakan layanan *Auht0* untuk penerapan autentikasi pada *Wordpress*. Terdapat 6 tahapan dalam pengerjaannya, sebagai berikut :

   a) Persiapan *tools* dan layanan
   Menyiapkan layanan dengan konfigurasi domain, ID klien, audiens, dan server yang diperlukan.

   b) Instalasi dan aktivasi plugin *Auth0*
   Melakukan instalasi dan aktivasi *plugin Auth0* pada *Wordpress*.

   c) Konfigurasi *plugin Auth0*
   Mengkonfigurasi *plugin Auth0* dan website *Auth0* untuk berintegrasi dengan situs *WordPress.*

   d) Pembuatan kebijakan MFA dan pengguna
   Membuat kebijakan MFA, mengatur pengguna, serta menyiapkan faktor autentikasi yang akan digunakan.

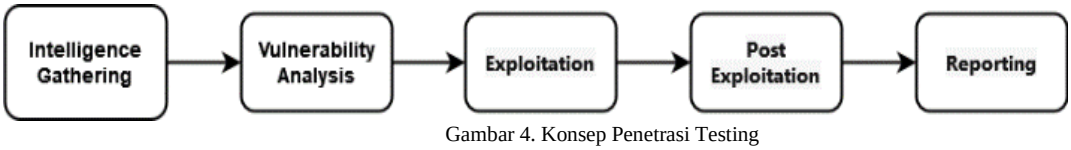
   e) Penerapan metode autentikasi
   Mengimplementasikan metode autentikasi seperti OTP dan email.

   f) Verifikasi identitas pengguna
   Memverifikasi identitas pengguna menggunakan metode autentikasi yang telah diatur.

2. Implementasi Penetrasi Testing

   Pengujian penetrasi adalah suatu metode yang bertujuan untuk mengidentifikasi informasi mengenai target, mengeksploitasi kelemahan yang ditemukan, dan memberikan rekomendasi perbaikan agar celah keamanan tersebut dapat diperbaiki dan dihilangkan sebelum menyebabkan kerusakan atau kerugian bagi pengguna [19].

   Pengujian penetrasi pada penelitian ini akan menggunakan tools *Burp Suite* sebagai alat pindai deteksi dini atas celah keamanan Wordpress. *Burp Suite* adalah perangkat lunak yang digunakan untuk melakukan pengujian penetrasi. Aplikasi ini dilengkapi dengan berbagai fitur yang berguna untuk menguji keamanan sistem [20]. Terdapat 5 tahapan dalam pengerjaan Pentest [21] yang diperlihatkan pada Gambar 4, sebagai berikut :



Gambar 4. Konsep Penetrasi Testing

1. Intelligence Gathering
   Pengujian dimulai dengan mengumpulkan informasi tentang sistem online.
2. Vulnerability Analysis
   Pada ada tahap ini, dilakukan pemindaian untuk mendeteksi kerentanan dan menentukan jenis serangan yang dapat dieksploitasi.
3. Exploitation
   Jika ditemukan kerentanan, pentester dapat mengambil alih situs atau mendapatkan akses lebih lanjut ke *Wordpress* target.
4. Post Exploitation
   Pada tahap ini, dilakukan perbaikan dan penerapan solusi atas kerentanan yang ditemukan pada sistem online, diikuti dengan pengujian ulang.
5. Reporting
   Setelah pengujian selesai, pentester menyusun laporan dengan temuan dan rekomendasi perbaikan. Pada tahapan ini hasil laporan yang didapat akan dibandingkan dengan parameter yang ditentukan sebagai acuan dalam pengujian pentest.

Jurnal Manajemen Informatika (JAMIKA)
Volume 15 Nomor 1 Edisi April 2025
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

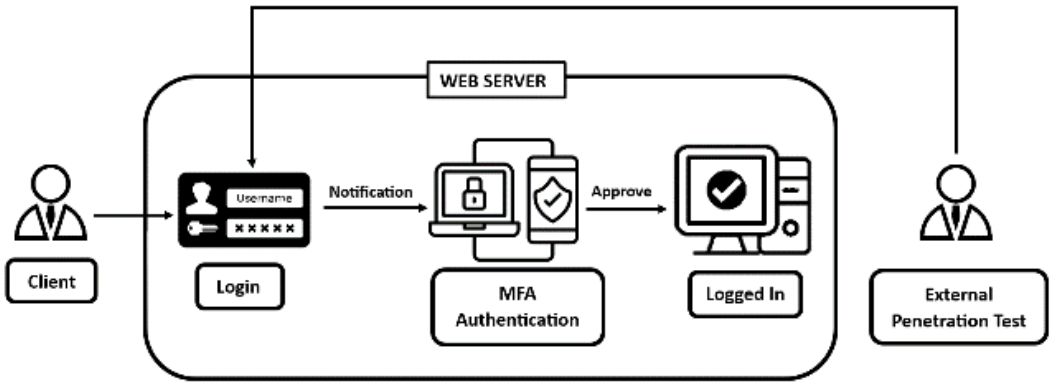
d. Monitoring

Tahap monitoring sangat penting setelah implementasi, karena tahap ini akan dilakukan verifikasi bahwa sistem memenuhi harapan dan tujuan pengguna sejak tahap analisis awal. Pemantauan melibatkan penggunaan layanan autentikasi dan API untuk melacak dan menganalisis peristiwa dan kinerja MFA, seperti jumlah permintaan MFA, tingkat keberhasilan dan kegagalan. Selain itu, dalam tahap penetrasi testing yang dilakukan menggunakan *Burp Suite*, perlu untuk memperhatikan hasil dari tes keamanan tersebut yang kemudian dibandingkan antara hasil penetrasi dengan parameter yang ditentukan dalam pengujian pentest. *Burp Suite* membantu mengidentifikasi kerentanan keamanan pada situs *WordPress*, termasuk celah keamanan yang dapat dieksploitasi oleh pihak yang tidak berwenang. Oleh karena itu, selama tahap monitoring, harus secara rutin memeriksa laporan hasil penetrasi testing dan mengambil tindakan korektif jika ditemukan kerentanan atau masalah keamanan.

III. HASIL DAN PEMBAHASAN

Design

Pada tahap ini akan dibuat desain alur kerja project yang bertujuan untuk meningkatkan keamanan dan efisiensi proses *website development*. Dua fokus utama dalam desainnya adalah MFA untuk memperkuat autentikasi pengguna dan *Burp Suite* untuk mendeteksi kerentanan pada website. Gambar 5 menggambarkan topologi alur pengerjaan project yang menunjukkan keseluruhan proses.

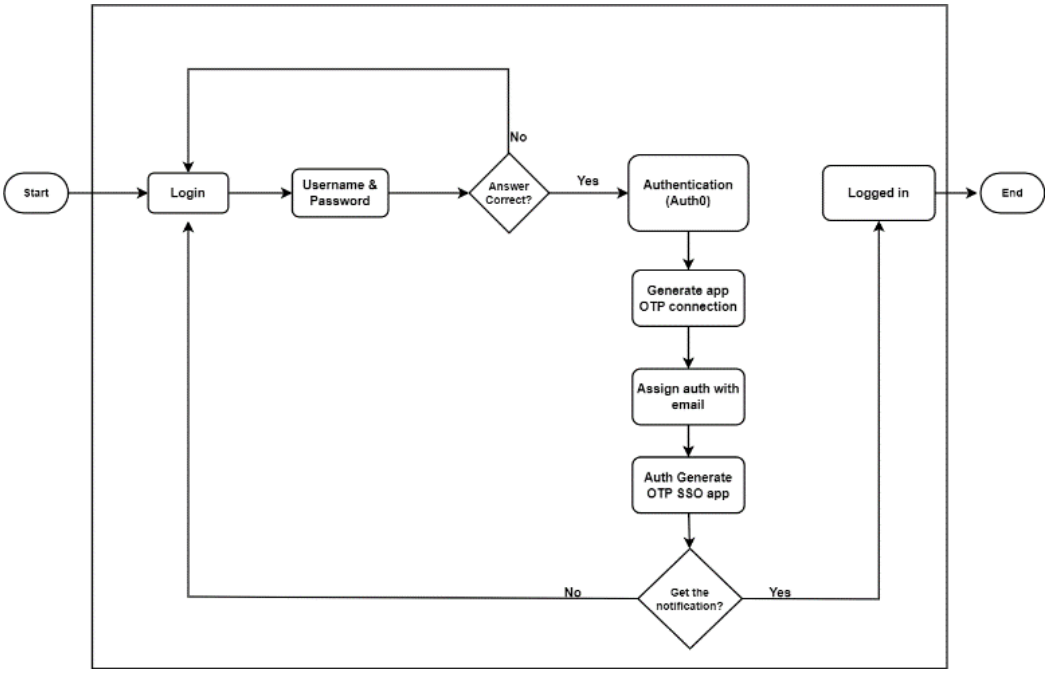


Gambar 5. Konsep Implementasi Multi Factor Authentication dan Penetrasi Testing

Dari Gambar 5, dapat dilihat alur kerja ini bertujuan untuk meningkatkan keamanan dan efisiensi proses website *development* dengan menggunakan MFA dan *Burp Suite*. MFA membantu melindungi akun pengguna dari akses yang tidak sah, sedangkan *Burp Suite* membantu mendeteksi dan mengatasi kerentanan pada website. Berikut penjelasan detail mengenai tahapan implementasi dari Gambar 5:

1. *Client*
   Pengguna memulai proses dengan mengakses *website* melalui *web browser*.
2. Sistem online
   Sistem online menerima permintaan dari client dan memprosesnya.
3. *Multi Factor Authentication*
   Jika MFA diaktifkan, sistem online akan mengarahkan *client* ke proses MFA. *Client* harus memasukkan informasi *login* dan menyelesaikan proses autentikasi tambahan, seperti memasukkan kode yang diterima dari *email client* atau OTP.

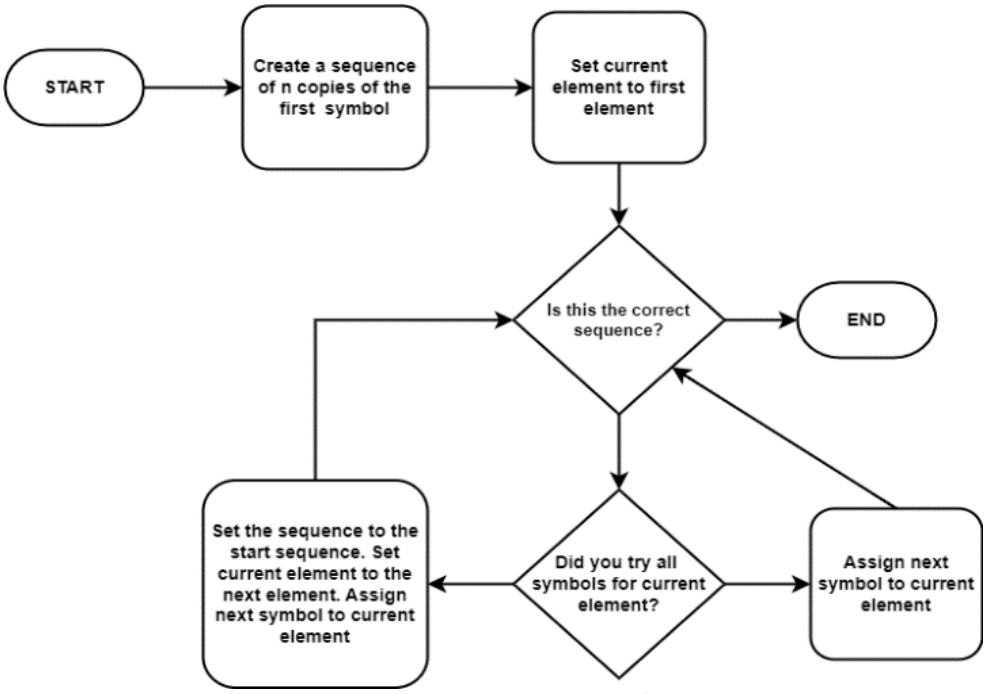
Jurnal Manajemen Informatika (JAMIKA)
Volume 15 Nomor 1 Edisi April 2025
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika



Gambar 6. Flowchart Cara Kerja Multi Factor Authentication

4. *External Penetration Testing*

Pada tahap ini akan dilakukan setelah penerapan MFA berhasil. Pada Gambar 7, dapat dilihat ketika Burpsuite dijalankan dengan mode brute force, alurnya dimulai dengan memasukkan URL target, daftar username, daftar password dan OTP. *Burp Suite* kemudian akan mencoba login dengan kombinasi angka dengan memberikan *range* angka untuk OTP tersebut. Jika login berhasil, Burp suite akan menandai akun tersebut sebagai vulnerable dan menampilkan informasi akun yang berhasil ditemukan. Proses ini akan terus berlanjut hingga seluruh kombinasi teruji atau akun target berhasil ditemukan. Hasilnya berupa informasi akun yang berhasil ditemukan dan laporan statistik mengenai proses brute force.



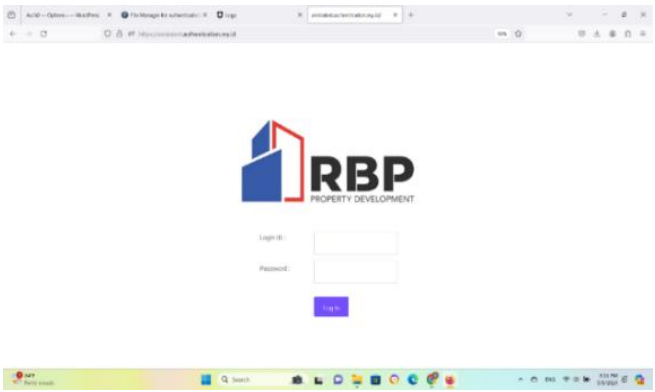
Gambar 7. *Flowchart* Cara Kerja *Bruteforce*

Jurnal Manajemen Informatika (JAMIKA)
Volume 15 Nomor 1 Edisi April 2025
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

Implementasi

a. Login Page

Pada tahap ini akan dilakukan perancangan tampilan *login page* di *Wordpress* yang dapat dilihat pada Gambar 8. Pada halaman ini pengguna perlu memasukkan login id dan password.

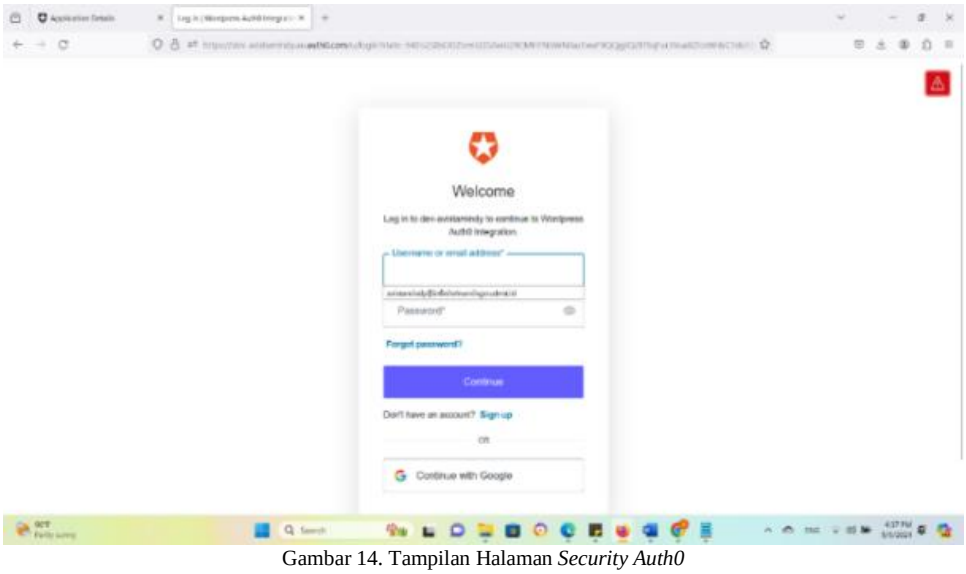


Gambar 8. Login Page

b. Implementasi *Multi Factor Authentication*

Pada tahap awal implementasi MFA, dilakukan penginstalan dan aktivasi *plugin Auth0* pada platform *WordPress*. Plugin ini digunakan untuk mengintegrasikan sistem autentikasi berbasis MFA ke dalam situs web. Setelah plugin diaktifkan, langkah selanjutnya adalah membuat akun pada layanan *Auth0*, yang kemudian diikuti dengan konfigurasi yang melibatkan input *Client ID, Domain, dan Client Secret.*

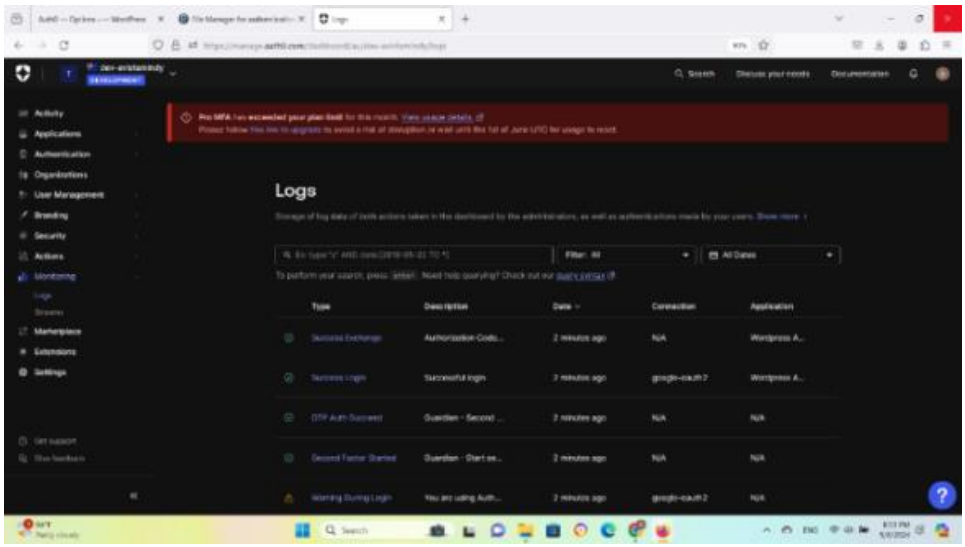
Setelah proses konfigurasi selesai, integrasi antara *WordPress* dan *Auth0* dilakukan dengan membuat aplikasi baru di *dashboard Auth0*. Aplikasi ini akan menghasilkan parameter-parameter yang diperlukan untuk konfigurasi lebih lanjut. Selanjutnya, pada bagian *Application URIs* di *dashboard Auth0*, *URL* situs *WordPress* dimasukkan ke dalam kolom *Allowed Callback URLs*, *Allowed Logout URLs*, dan *Allowed Web Origins*. Sedangkan di *WordPress*, pada halaman *plugin Auth0*, *Client ID, Domain*, dan *Client Secret* yang diperoleh dari *Auth0* dimasukkan untuk menyelesaikan proses integrasi. Setelah konfigurasi berhasil, setiap mengakses ke situs *WordPress* akan diarahkan melalui halaman *login* keamanan *Auth0* yang dapat dilihat pada Gambar 14. Pengguna kemudian diminta untuk melakukan autentikasi dengan memasukkan email dan kode OTP yang dikirimkan oleh *Auth0*.



Gambar 14. Tampilan Halaman *Security Auth0*

Untuk mengetahui apakah proses autentikasi berhasil dapat dilihat di *monitoring logs* pada *Auth0* ditunjukkan pada gambar 15.

Jurnal Manajemen Informatika (JAMIKA)
Volume 15 Nomor 1 Edisi April 2025
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika



Gambar 15. Halaman *Monitoring Logs*

Pada gambar 15 dapat dilihat bahwa proses dari awal user masuk melalu URL *wordpress* hingga berpindah ke halaman *security* dari *Auth0* dan juga proses autentikasi, semuanya berhasil. Ini menandakan bahwa proses autentikasi pada website telah berhasil diimplementasi.

c. Implementasi Pengujian Keamanan Auth0

Tahap pengujian keamanan sistem dilakukan dengan menggunakan Burp Suite. Pendekatan yang digunakan dalam pengujian ini adalah pengujian *black box*, yang bertujuan untuk mengidentifikasi potensi celah keamanan dan pengaturan autentikasi dalam sistem MFA. Pengujian dimulai dengan pemantauan lalu lintas *HTTP* melalui *HTTP History* untuk merekam interaksi antara klien dan server saat proses autentikasi berlangsung. Pada tahap ini, pengujian juga mencakup penggunaan *Repeater* pada *Burp Suite* untuk mensimulasikan serangan dengan mengirimkan permintaan autentikasi berulang-ulang menggunakan OTP yang salah.

Setelah proses pengujian, hasilnya dapat dilihat pada Tabel 3 berikut ini, yang merangkum hasil pengujian yang telah dilakukan menggunakan Burp Suite.

TABEL 3
HASIL PENGUJIAN *BLACK BOX* (BURP SUITE)

Kode Uji	Nama Pengujian	Kriteria Evaluasi	Hasil yang Diharapkan	Hasil Pengujian
BS01.1	HTTP Request Validation	Mengirimkan permintaan HTTP yang valid ke server autentikasi OTP	Sistem mengizinkan akses atau memberikan respons yang sesuai	Sesuai, respons 401 Unauthorized diterima
BS01.2	HTTP Request Manipulation	Mengirimkan permintaan HTTP dengan OTP yang salah	Sistem menolak akses dan memberikan pesan kesalahan	Sesuai, sistem menolak akses dan menampilkan pesan "Oops! something went wrong"
BS02.1	Cookie Management	Mengamati pengaturan dan pengelolaan cookie selama autentikasi	Tidak ada cookie sensitif baru yang diatur atau diungkap	Sesuai, tidak ada set-cookie baru setelah proses repeater

Jurnal JAMIKA Manajemen Informatika

Jurnal Manajemen Informatika (JAMIKA)
Volume 15 Nomor 1 Edisi April 2025
E ISSN: 2655-6960 | P ISSN: 2088-4125
OJS: https://ojs.unikom.ac.id/index.php/jamika

Kode Uji	Nama Pengujian	Kriteria Evaluasi	Hasil yang Diharapkan	Hasil Pengujian
BS03.1	Rate Limiting	Mengirimkan beberapa permintaan berulang ke server	Sistem menerapkan batasan jumlah permintaan untuk mencegah brute force	Sesuai, sistem menunjukkan header rate limit seperti 'X-Ratelimit-Limit', 'X-Ratelimit-Remaining', dan 'X-Ratelimit-Reset'
BS04.1	Error Handling	Mengirimkan permintaan dengan kredensial yang salah	Sistem memberikan pesan kesalahan yang tidak mengungkap informasi sensitive.	Sesuai, pesan kesalaha tidak mengungka informasi sensitif, hany masalah sesi

Dari Tabel 3, dapat dilihat bahwa ketika proses *Repeater* terjadi, server *Auth0* merespon dengan sangat baik dengan tidak menampilkan informasi sensitif seperti *username, password, email* bahkan OTP yang benar walaupun sudah kita lakukan penginputan OTP yang salah secara berulang. Sehingga tidak memungkinkan untuk dilakukan manipulasi *code* agar OTP yang telah kita input berhasil terverifikasi.

Pada status kode *Unauthorized* pada *Response server*. *Respons HTTP 401* menunjukkan bahwa permintaan tidak diotorisasi, yang berarti sistem menolak permintaan karena kredensial yang tidak valid atau sesi yang tidak valid. Ini adalah respons yang diharapkan ketika autentikasi gagal, menunjukkan bahwa sistem tidak menerima permintaan tanpa autentikasi yang benar.

Pada manajemen cookie, tidak ada '*set-cookie*' baru dalam respons server setelah proses *repeater* dilakukan, yang berarti sistem tidak secara otomatis mengatur ulang atau menambahkan cookie baru dalam respons ini, sehingga mengurangi risiko penyerangan *via cookie*.

Lalu pada pesan kesalahan yang diberikan oleh server, yaitu memberikan informasi tentang masalah sesi tetapi tidak memberikan rincian teknis yang dapat dimanfaatkan oleh penyerang. Ini adalah praktik yang baik dalam keamanan untuk menghindari kebocoran informasi sensitif.

Pada *Rate Limiting*, *Header 'X-Ratelimit-Limit', 'X-Ratelimit-Remaining',* dan *'X-Ratelimit-Reset'* menunjukkan bahwa sistem menerapkan batasan pada jumlah permintaan dalam periode waktu tertentu. Ini adalah mekanisme keamanan yang baik untuk mencegah *brute force* dan serangan *DDoS*.

IV. KESIMPULAN

Penelitian ini berhasil menunjukkan bahwa implementasi Multi-Factor Authentication (MFA) pada sistem online PT. ABC dapat secara signifikan meningkatkan keamanan data. Dengan menggunakan metode Network Development Life Cycle (NDLC), penelitian ini mengidentifikasi dan mengatasi kelemahan keamanan yang ada. Pengujian penetrasi dengan Burp Suite memastikan keandalan sistem setelah penerapan MFA. Hasil penelitian menunjukkan bahwa penerapan MFA secara signifikan meningkatkan perlindungan terhadap akses tidak sah, dengan bukti bahwa sistem dapat menolak login dengan kredensial yang salah serta menerapkan batasan permintaan untuk mencegah serangan brute force. Selain itu, implementasi MFA juga meningkatkan kesadaran karyawan mengenai pentingnya praktik keamanan data. Penelitian ini menegaskan bahwa adopsi teknologi autentikasi yang lebih canggih sangat penting untuk melindungi informasi sensitif di lingkungan perusahaan, sehingga MFA disarankan sebagai komponen kunci dalam strategi keamanan data perusahaan. Untuk penelitian lebih lanjut, disarankan agar peneliti mengeksplorasi penggunaan metode autentikasi tambahan atau alternatif lainnya serta melakukan studi longitudinal untuk menganalisis efektivitas jangka panjang dari implementasi MFA di berbagai sektor industri. Penelitian mengenai pelatihan keamanan bagi karyawan dan dampaknya terhadap perilaku keamanan juga dapat memberikan wawasan berharga untuk meningkatkan strategi perlindungan data.

UCAPAN TERIMA KASIH

Penelitian ini tidak akan berhasil tanpa dukungan dan kontribusi dari banyak pihak. Terima kasih kepada manajemen dan karyawan PT. ABC yang telah memberikan izin akses dan bersedia berpartisipasi dalam

wawancara dan observasi. Terima kasih juga kepada dosen-dosen yang telah memberikan masukan berharga dalam proses implementasi dan pengujian MFA. Semoga hasil penelitian ini bermanfaat bagi peningkatan keamanan data di perusahaan dan dapat menjadi referensi bagi penelitian-penelitian selanjutnya.

DAFTAR PUSTAKA

[1] Konsumen Cerdas, "Perlindungan Konsumen dan Data Pribadi di Era Ekonomi Digital," *Konsum. Cerdas*, no. 2, pp. 1–27, 2022.

[2] S. Kemp, "DIGITAL 2022: LAPORAN STATSHOT GLOBAL APRIL," *21 April 2022*, 2022. https://datareportal-com.translate.goog/reports/digital-2022-april-global-statshot?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=tc (accessed Oct. 22, 2023).

[3] APJII, "Survei Internet APJII 2023," *2023*, 2023. https://survei.apjii.or.id/ (accessed Oct. 22, 2023).

[4] N. A. Karim, H. Kanaker, W. K. Abdulraheem, M. A. Ghaith, E. Alhroob, and A. M. F. Alali, "Choosing the right MFA method for online systems: A comparative analysis," *Int. J. Data Netw. Sci.*, vol. 8, no. 1, pp. 201–212, 2024, doi: 10.5267/j.ijdns.2023.10.003.

[5] K. Jung, "Extreme Data Breach Losses: An Alternative Approach to Estimating Probable Maximum Loss for Data Breach Risk," *North Am. Actuar. J.*, vol. 25, no. 4, pp. 580–603, 2021, doi: 10.1080/10920277.2021.1919145.

[6] V. A. Simbolon and V. Juwono, "Comparative Review of Personal Data Protection Policy in Indonesia and The European Union General Data Protection Regulation," *J. Ilmu Adm. I*, vol. 11, no. 2, pp. 2022–178, 2022, [Online]. Available: http://dx.doi.org/10.31314/pjia.11.2.178-190.2022

[7] S. E. Prasetyo, N. Hasanah, and G. Wijaya, "Pengujian Keamanan Learning Management System TutorLMS Terhadap Kerentanan Insecure Design dan Broken Access Control," *Telcomatics*, vol. 7, no. 2, pp. 53–60, 2022, doi: 10.37253/telcomatics.v7i2.7357.

[8] A. S. Wardani, "422 Juta Data Pengguna Dicuri Sepanjang 2022," *27 January 2023*, 2023. https://www.liputan6.com/tekno/read/5191074/422-juta-data-pengguna-dicuri-sepanjang-2022?page=2 (accessed Oct. 22, 2023).

[9] I. T. R. Center, "Identity Theft Resource Center's 2022 Annual Data Breach Report Reveals Near-Record Number of Compromises," *01 January 2023*, 2023. https://www-idtheftcenter-org.translate.goog/post/2022-annual-data-breach-report-reveals-near-record-number-compromises/?_x_tr_sl=en&_x_tr_tl=id&_x_tr_hl=id&_x_tr_pto=tc (accessed Oct. 22, 2023).

[10] S. Das, B. Wang, Z. Tingle, and L. J. Camp, "Evaluating User Perception of Multi-Factor Authentication: A Systematic Review," 2019, [Online]. Available: http://arxiv.org/abs/1908.05901

[11] C. Wang, Y. Wang, Y. Chen, H. Liu, and J. Liu, "User authentication on mobile devices: Approaches, threats and trends," *Comput. Networks*, vol. 170, p. 107118, 2020, doi: 10.1016/j.comnet.2020.107118.

[12] J. Williamson and K. Curran, "The Role of Multi-factor Authentication for Modern Day Security," *Semicond. Sci. Inf. Devices*, vol. 3, no. 1, pp. 16–23, 2021, doi: 10.30564/ssid.v3i1.3152.

[13] T. Joseph, S. A. Kalaiselvan, S. U. Aswathy, R. Radhakrishnan, and A. R. Shamna, "A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment," *J. Ambient Intell. Humaniz. Comput.*, vol. 12, no. 6, pp. 6141–6149, 2021, doi: 10.1007/s12652-020-02184-8.

[14] T. A. Nugroho *et al.*, "Keamanan Berbasis Service Oriented Architecture Menggunakan Oauth 2.0 dan Json Web Token," *IJESPG J.*, vol. 1, no. 3, pp. 229–236, 2023, [Online]. Available: http://ijespgjournal.org

[15] G. L. Moepi and T. E. Mathonsi, "Implementation of an Enhanced Multi-Factor Authentication Scheme with a Track and Trace Capability for Online Banking Platforms," 2023, doi: 10.20944/preprints202311.0950.v1.

[16] M. I. Hussain *et al.*, "Aaaa: Sso and mfa implementation in multi-cloud to mitigate rising threats and concerns related to user metadata," *Appl. Sci.*, vol. 11, no. 7, 2021, doi: 10.3390/app11073012.

[17] N. A. M. Ariffin, F. A. Rahim, A. Asmawi, and Z. A. Ibrahim, "Vulnerabilities detection using attack recognition technique in multi-factor authentication," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 18, no. 4, pp. 1998–2003, 2020, doi: 10.12928/TELKOMNIKA.V18I4.14898.

[18] K. Ocha, K. Saputra, A. R. Supriyatna, and S. D. Putra, "Autentikasi User Dengan Metode Single Sign-On Berbasis Windows Active Directory Pada PT . XYZ User Authentication Through Windows Active Directory- Based Single Sign-On Method at PT . XYZ," vol. 2, no. 2, pp. 70–78, 2024, doi: 10.25181/rt.v2i2.3328.

[19] H. Haeruddin, "Analisa dan Implementasi Sistem Keamanan Router Mikrotik dari Serangan Winbox

Exploitation, Brute-Force, DoS," *J. Media Inform. Budidarma*, vol. 5, no. 3, p. 848, 2021, doi: 10.30865/mib.v5i3.2979.

[20] Ika Meilina and G. R. F. -, "Anticipate Password Security with Burp Suite Using the Brute Force Attack Method," *J. E-Komtek*, vol. 7, no. 1, pp. 118–127, 2023, doi: 10.37339/e-komtek.v7i1.1162.

[21] F. Fachri, "Optimasi Keamanan Web Server Terhadap Serangan Brute-Force Menggunakan Penetration Testing," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 10, no. 1, pp. 51–58, 2023, doi: 10.25126/jtiik.20231015872.