Perlindungan keamanan pada aplikasi reschedule kelas dengan mengunakan metode autentikasi

Susi Fanlay

Teknologi Informasi, Fakultas Sain Dan Teknologi, Universitas 'Aisyiyah Yogyakarta
Email: susifanlay@gmail.com

Abstrak

Era industri 4.0 menuntut segala aspek kehidupan masyarakat untuk memanfaatkan teknologi guna mempermudah dalam menyelesaikan suatu masalah, salah satu teknologi yang sangat populer adalah website, website menjadi populer karena dapat di akses melalui berbagai platforms, dengan populernya website menyebabkan meningkatnya serangan pada website. Pelaku kejahatan cyber (cyber criminals) biasanya mencuri akun dari administrator website guna memanipulasi data dan informasi, untuk itu perlu adanya metode keamanan untuk melindungi website dari serangan. Berbagai metode pengamanan akun telah banyak di kembangkan, salah satunya adalah metode two-factor authentication (2FA), metode ini digunakan untuk mengantisipasi apabila akun administrator di curi oleh cyber criminals, apabila akun tersebut di dapatkan orang lain, pelaku harus mendapatkan password ke dua yang di kirimkan sistem ke email maupun nomor handphone korban, sehingga untuk dapat masuk ke dalam website di perlukan dua langkah autentikasi.

Kata kunci : 2FA; Kebijakan firewall; website; Keamanan cyber

Security protection in class rescheduling applications by using authentication methods

Abstrak

The industrial era 4.0 requires all aspects of people's lives to utilize technology to make it easier to solve problems, one very popular technology is websites, websites are becoming popular because they can be accessed via various platforms, with the popularity of websites causing an increase in attacks on websites. Cyber criminals usually steal accounts from website administrators to manipulate data and information, for this reason there is a need for security methods to protect websites from attacks. Various account security methods have been developed, one of which is the two-factor authentication (2FA) method, this method is used to anticipate if the administrator account is stolen by cyber criminals, if the account is obtained by someone else, the perpetrator must get a second password. The system sends it to the victim's email or cellphone number, so that to be able to enter the website you need two steps of authentication.

***Keywords**: 2FA; Firewall policies; websites; Cyber security*

1. Pendahuluan

Teknologi informasi yang semakin berkembang, dapat di akses dengan mudah kapan saja dan di mana saja menimbulkan kecemasan bagi pengelola sistem karena tidak sedikit pelaku kejahatan memanfaatkan situasi ini untuk kepentingan diri sendiri (Huwaidi, 2022, 107). Website merupakan platform yang menjadi tulang punggung teknologi informasi, dapat di akses kapan saja dan di mana saja sehingga dapat meningkatkan resiko website dari kejahatan cyber (Saputra, 2022, 1). Website sebagian besar menggunakan metode otentikasi tunggal guna mengamankan akses halaman tertentu, proses otentikasi ini berfungsi untuk membuktikan kebenaran, ke aslian maupun validitas data kunci yang di inputkan guna masuk ke dalam sistem (Mustaqim, 2019, 1). a (2020, 361) berhasil membangun mekanisme 2FA menggunakan OTP yang di kirimkan melalui layanan SMS dan menjelaskan bahwa SMS membutuhkan biaya berupa pulsa guna mengirimkan kode OTP kepada pengguna, perlu adanya proses OTP yang dapat memanfaatkan layanan gratis seperti whatsapp, telegram maupun E-mail. (Anwar, 2021). Firewall policies (kebijakan firewall) terdapat dua macam yaitu allow all deny any memperbolehkan semua trafik yang masuk maupun keluar dari jaringan dan memblokir beberapa trafik, sedangkan kebijakan yang ke dua adalah deny all allow any yaitu memblokir semua trafik dan hanya mengizinkan trafik tertentu saja.

Dalam konteks pengelolaan akademik di berbagai universitas, penjadwalan kuliah pengganti adalah salah satu aspek yang penting dan kompleks. Ketika terjadi peristiwa yang mengakibatkan pembatalan jadwal kuliah, seperti keperluan dosen yang tidak dapat hadir atau keadaan darurat, penjadwalan kuliah pengganti perlu dilakukan agar proses pembelajaran dapat tetap berjalan lancar. Namun, dalam banyak kasus, proses penjadwalan kuliah pengganti masih menghadapi kendala dalam hal efisiensi, akurasi, dan komunikasi antara penanggung jawab mata kuliah, dosen, dan mahasiswa (Arlow & Neustadt, 2005).

Untuk mengatasi kendala tersebut, penggunaan aplikasi penjadwalan kuliah pengganti telah menjadi solusi yang semakin populer di berbagai universitas. Aplikasi ini, yang diunduh dan digunakan oleh penanggung jawab mata kuliah dan dosen di universitas manapun, menyediakan layanan yang memungkinkan penambahan jadwal kuliah pengganti tanpa mengganggu jadwal tetap yang sudah ditetapkan sebelumnya. Selain itu, aplikasi ini juga menyediakan fitur notifikasi yang berguna dalam saling mengingatkan antara pengguna aplikasi (Ben dkk, 2016; Subekti dkk, 2014).

Dalam konteks penggunaan aplikasi penjadwalan kuliah pengganti, aplikasi ini memberikan kemudahan dan keunggulan dalam beberapa aspek. Pertama, dengan menggunakan aplikasi ini, penanggung jawab mata kuliah dan dosen dapat menambahkan jadwal kuliah pengganti tanpa mempengaruhi jadwal tetap yang telah ditetapkan sebelumnya. Hal ini memungkinkan proses penjadwalan kuliah pengganti dilakukan dengan cepat dan efisien, menghemat waktu dan upaya yang diperlukan. Kedua, aplikasi ini menyediakan fitur notifikasi yang berguna untuk saling mengingatkan antara pengguna aplikasi. Fitur ini memastikan bahwa setiap pihak terlibat dalam penjadwalan kuliah pengganti, baik penanggung jawab mata kuliah, dosen, maupun mahasiswa, menerima pemberitahuan yang tepat waktu dan teratur mengenai perubahan jadwal atau informasi terkait lainnya. Dengan adanya notifikasi ini, pengguna aplikasi dapat menghindari kehilangan informasi penting dan menjaga komunikasi yang efektif antara semua pihak yang terlibat (Husni & Oktarino, 2021).

Oleh sebab itu, peneliti tertarik untuk menganalisis perlindungan keamanaan dari aplikasi Reschedule-In yang dapat menyelesaikan permasalahan agar penjadwalan kuliah pengganti agar dapat efektif dan efisien. Dengan adanya aplikasi Reschedule-In ini akan sangat bermanfaat untuk mahasiswa dan dosen dalam melakukan proses penjadwalan kuliah pengganti diberbagai universitas. Dalam penelitian ini akan dilakukan analisis desain sistem aplikasi menggunakan metode Metode Autentikasi(Larman & Vodde, 2016; Prasetya dkk, 2022; Rinaldi, 2019).

2. Metode

Penelitian di awali dengan proses studi literatur guna mengetahui cara kerja dan jenis 2FA, serta cara mengamankan halaman administrator website melalui mekanisme pengamanan menggunakan firewall, selanjutnya proses perancangan adalah tindak lanjut dari proses studi literatur sehingga mekanisme yang akan di bangun sesuai dengan studi yang mutakhir dan relevan, setelah proses perancangan hal yang dilakukan adalah melakukan implementasi mekanisme pengamanan 2FA dan implementasi firewall, setelah mekanisme di implementasi maka akan di lakukan proses testing dan evaluasi untuk mengetahui apakah mekanisme telah berhasil meningkatkan keamanan pada website.

Keamanan Sistem Informasi upaya untuk melindungi data, aplikasi, dan infrastruktur dari ancaman atau gangguan yang dapat merusak integritas, kerahasiaan, dan ketersediaannya. Menurut standar **ISO/IEC 27001** Autentikasi untuk proses untuk memverifikasi identitas pengguna sebelum memberikan akses ke sistem. Proses ini memastikan bahwa pengguna yang mencoba mengakses sistem adalah pihak yang sah.

Kontrol akses adalah mekanisme untuk menentukan dan membatasi hak akses pengguna terhadap suatu sistem. Terdapat dua pendekatan utama yaitu. Role-Based Access Control (RBAC), dan Discretionary Access Control (DAC). autentikasi dianggap sebagai komponen penting untuk melindungi keamanan aplikasi reschedule kelas. Implementasi metode autentikasi berbasis *username-password* yang dilengkapi dengan 2FA dapat memastikan hanya pengguna yang sah yang dapat mengakses sistem, serta meminimalkan risiko ancaman seperti akses tidak sah dan manipulasi data. Selain itu, kontrol akses berbasis peran (RBAC) diperlukan untuk membatasi hak akses sesuai fungsi masing-masing pengguna.

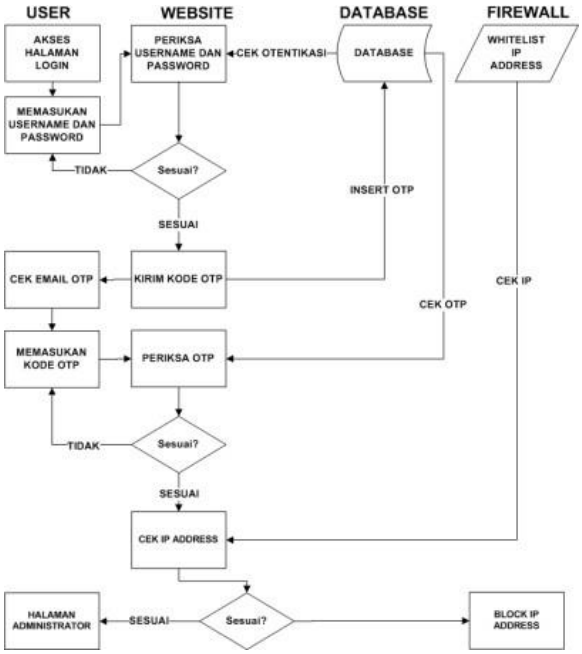
3. Hasil dan Pembahasan

Pada tahap studi pustaka telah di dapatkan beberapa kelebihan dan kelemahan dari metode 2FA dalam mengamankan sebuah website dan Penerapan metode autentikasi seperti password hashing, 2FA, dan JWT berhasil meningkatkan keamanan aplikasi reschedule kelas. Langkah-langkah mitigasi ancaman memastikan sistem tetap aman dari serangan yang umum terjadi.

Berdasarkan pengujian menggunakan **penetration testing tools** seperti OWASP ZAP dan Burp Suite, sistem menunjukkan ketahanan terhadap serangan umum. Penerapan metode autentikasi terbukti meningkatkan keamanan tanpa mengurangi kenyamanan pengguna.

3.1. Hasil

Mahardhika (2020), menjelaskan bahwa proses pengiriman kode otentikasi ganda menggunakan SMS sangat tergantung pada pulsa. Kemungkinan gagalnya kode terkirim karena pulsa habis sangat mungkin terjadi, maka pada penelitian ini akan memanfaatkan E-mail guna mengirimkan kode otentikasi tanpa terhalang pulsa dan hemat biaya. Pada tahap perancangan yang merupakan proses design sistem yang akan di bangun. Berikut ini gambar design mekanisme 2FA dan kebijakan firewall yang akan di bangun.



Gambar 1. design mekanisme 2FA

3.2. Pembahasan

Staff dan pengguna internet pada perusahaan. Proses login ke dalam halaman administrator di lakukan dengan memasukan username dan password, selanjutnya pengguna akan menerima email berupa kode acak yang telah di simpan ke database, sehingga kode yang diterima pengguna akan di masukan ke form otentikasi ke dua apabila kode tersebut cocok dengan kode yang ada pada database maka sistem akan mencocokan IP address pengguna dengan IP Address yang ada pada firewall, apabila alamat IP pengguna terdaftar pada whitelist firewall maka pengguna akan di arahkan ke halaman administrator.

Untuk meningkatkan keamanan pada halaman admin website pelu adanya proteksi whitelist pada IP tertentu, hal ini guna mengamankan halaman sensitif apabila website yang di kelola memang hanya untuk kepentingan internal, misal aplikasi transaksi, pencatatan logistik, input penilaian dan sebagainya, sehingga apabila 2FA telah di kuasai penyerang, penyerang hanya dapat mengakses halaman dengan alamat IP tertentu, yang pastinya akan menambah sulit penyerang untuk mengakses halaman administrator website.

4. Kesimpulan

Hasil penelitian Implementasi Two-Factor Authentication (2FA) dan Firewall Dalam Mengamankan Website mendapatkan hasil dan kesimpulan Dengan adanya mekanisme otentikasi ganda 2FA kemanan website menjadi meningkat, apabila akun pengguna di dapatkan oleh pelaku kejahatan cyber maka pelaku tidak akan dapat masuk ke dalam sistem karena harus memasukan kode 2FA yang di kirim ke email korban, secara tidak langsung untuk mendapatkan kode 2FA, pelaku harus mendapatkan akun email dari korban dan Penelitian ini bertujuan untuk memberikan solusi perlindungan keamanan pada aplikasi reschedule kelas menggunakan metode autentikasi yang dirancang untuk memastikan keamanan data pengguna serta keandalan sistem dalam mengelola penjadwalan ulang. Metode yang digunakan, mulai dari analisis kebutuhan, perancangan sistem, hingga implementasi dan pengujian autentikasi, dirancang untuk menjawab permasalahan utama terkait akses tidak sah, pencurian data, dan manipulasi informasi yang dapat terjadi pada aplikasi berbasis web. Pendekatan berbasis autentikasi, seperti *username-password* yang dilengkapi dengan **Two-Factor Authentication (2FA)**, diharapkan mampu meningkatkan tingkat keamanan aplikasi secara signifikan.

Ucapan terimakasih

Puji syukur kehadirat Tuhan yang Maha Esa. Atas rahmat dan hidayah-Nya, penulis dapat menyelesaikan Jurnal yang berjudul "Perlindungan Keamanan Pada Aplikasi Reschedule Kelas Dengan Mengunakan Metode Autentikasi" dengan tepat waktu. Selain itu, Jurnal ini bertujuan menambah wawasan untuk memperkuat dasar keilmuan bagi para pembaca dan juga bagi penulis. Penulis mengucapkan terima kasih kepada

1. Dr.Warsiti S.kp., M. Kep Sp. Mat., Selaku Rektor Universitas ‘Aisyiyah Yogyakarta,
2. Tika Ainunnisa Fitria, S.T., M.T., Ph.D Selaku Dekan Fakultas Sains Dan teknologi.
3. Tikaridha Hardiani, S.Kom., M. Eng. Selaku Dekan Teknologi Informasi,
4. Arizona Firdonsyah, S.Kom., M. Kom. Selaku Dosen pembimbing yang senantiasa meluangkan waktu dan tempatnya dalam memberikan bimbingan, pengarahan dan bantuan.
5. terima kasih juga kepada semua pihak yang telah membantu diselesaikannya jurnal ini.

Penulis menyadari bahwa jurnal ini masih jauh dari kata sempurna karena keterbatasan pengatahuan dan pengalaman.Meskipun demikian, penulis bersyukur karena telah dapat menyelesaikan jurnal penelitian ini dan kemajuan ilmu pengatahuan dimasa yang akan datang

Daftar Pustaka

Anwar, R. W. (2021). Security. Firewall Best Practices for Securing Smart Healthcare Environment: A Review. Applied Sciences, 11-19.

Choirul Mustaqim, A. H. (2019). Implementasi. Implementasi Two factor authentication Dan Algoritma Rsa Sebagai Metode Otentikasi Login Pada Si-Abka, 1.

Huwaidi, M. Z. (2022). Justin. Mencegah Serangan Rekayasa Sosial Dengan Human Firewall, 107-112.

Saputra, I. P. (2022). Computer. Comparison of anomaly based and signature based methods in detection of scanning vulnerability., 221-225.

Hero Raka Herdiantoro, M. R. (2023). MPLEMENTASI TWO-FACTOR AUTHENTICATION (2FA). IMPLEMENTASI TWO-FACTOR AUTHENTICATION (2FA), 8.

ISO/IEC. (27 01 2013). Information technology . Information technology – Security techniques – Information security management systems – Requirements., 6.

Kumar, A. &. (2021). A Review on Authentication Methods in Web Applications." . A Review on Authentication Methods in Web Applications." , 21(3), , 42, 52.