ANALISIS KEAMANAN SISTEM LOGIN MULTI-USER TERHADAP SERANGAN CREDENTIAL STUFFING

Rakhmadi Rahman[1], Nabigha Nailatul Saida[2], Afrianda[3]
rakhmadi.rahman@ith.ac.id[1], nabighanailatuls@gmail.com[2], nandafrindaa@gmail.com[3]
Institut Teknologi Bacharuddin Jusuf Habibie

ABSTRAK

Sistem autentikasi login merupakan komponen penting dalam pengelolaan akses pada aplikasi berbasis web karena berfungsi sebagai mekanisme pengendali interaksi pengguna dengan sistem. Seiring meningkatnya jumlah insiden kebocoran data kredensial di berbagai platform digital, serangan credential stuffing menjadi salah satu metode serangan yang paling sering digunakan untuk memperoleh akses tidak sah ke akun pengguna. Serangan ini memanfaatkan kombinasi kredensial hasil kebocoran sebelumnya dan dieksekusi secara otomatis dalam skala besar. Penelitian ini bertujuan untuk mengevaluasi ketahanan mekanisme autentikasi pada sistem login multi-user terhadap serangan credential stuffing melalui pendekatan analisis keamanan. Analisis dilakukan dengan mengkaji respons sistem login terhadap simulasi serangan otomatis serta menilai efektivitas penerapan mekanisme autentikasi berlapis. Hasil evaluasi menunjukkan bahwa sistem login yang hanya mengandalkan autentikasi satu faktor memiliki tingkat kerentanan yang tinggi, sedangkan penerapan autentikasi berlapis mampu meningkatkan ketahanan sistem secara signifikan terhadap upaya akses tidak sah. Temuan ini menegaskan bahwa autentikasi berlapis merupakan strategi yang relevan dan efektif dalam meminimalkan risiko serangan credential stuffing pada sistem login multi-user.
Kata Kunci: Keamanan Login, Autentikasi Berlapis, Credential Stuffing, Sistem Multi-User.

ABSTRACT

Authentication mechanisms play a vital role in controlling access to web-based applications, as they regulate user interaction with protected resources. The increasing number of credential leakage incidents across digital platforms has led to the widespread use of credential stuffing attacks, which exploit previously compromised login data to gain unauthorized access automatically and at scale. This study aims to evaluate the resilience of multi-user login authentication mechanisms against credential stuffing attacks through a security analysis approach. The evaluation is conducted by examining system responses to automated attack simulations and assessing the effectiveness of layered authentication mechanisms. The results demonstrate that login systems relying solely on single-factor authentication exhibit a high level of vulnerability, whereas layered authentication significantly enhances system resistance to unauthorized access attempts. These findings confirm that layered authentication is an effective strategy for mitigating credential stuffing threats in multiuser login environments.
***Keywords**: Login Security, Layered Authentication, Credential Stuffing, Multi-User Systems.*

PENDAHULUAN

Sistem login merupakan elemen fundamental dalam hampir seluruh aplikasi berbasis web, baik pada sektor pendidikan, pemerintahan, maupun industri komersial. Keberadaan sistem login bertujuan untuk memastikan bahwa hanya pengguna yang memiliki hak akses yang dapat memanfaatkan layanan dan sumber daya yang tersedia. Oleh karena itu, keamanan sistem login menjadi faktor krusial dalam menjaga kerahasiaan dan integritas data pengguna.

Namun, meningkatnya ketergantungan masyarakat terhadap layanan digital turut diiringi oleh peningkatan ancaman keamanan siber. Salah satu ancaman yang paling menonjol adalah credential stuffing, yaitu metode serangan yang memanfaatkan kombinasi username dan password hasil kebocoran data dari platform lain. Serangan ini dijalankan

secara otomatis dan mampu menargetkan ribuan akun dalam waktu singkat. Tingginya tingkat keberhasilan credential stuffing sebagian besar disebabkan oleh perilaku pengguna yang menggunakan kredensial yang sama pada berbagai layanan digital.

Banyak sistem login masih mengandalkan autentikasi satu faktor sebagai mekanisme pengamanan utama. Pendekatan ini dinilai tidak lagi memadai dalam menghadapi serangan otomatis berskala besar. Oleh karena itu, diperlukan evaluasi terhadap ketahanan autentikasi login multi-user dengan mempertimbangkan peran autentikasi berlapis sebagai mekanisme mitigasi. Penelitian ini difokuskan pada analisis keamanan sistem login multi-user terhadap serangan credential stuffing tanpa melakukan perancangan atau pembangunan sistem baru.

METODOLOGI

Penelitian ini menggunakan metode analisis keamanan dengan pendekatan evaluatif. Metode ini dipilih karena tujuan penelitian bukan untuk mengembangkan sistem autentikasi baru, melainkan untuk mengkaji dan mengevaluasi tingkat ketahanan mekanisme autentikasi yang umum diterapkan pada sistem login multi-user.

HASIL DAN PEMBAHASAN

Hasil analisis menunjukkan bahwa sistem login multi-user yang hanya mengandalkan autentikasi satu faktor memiliki tingkat kerentanan yang tinggi terhadap serangan credential stuffing. Pada skenario simulasi serangan, penggunaan kombinasi kredensial yang valid memungkinkan penyerang untuk memperoleh akses tanpa adanya mekanisme verifikasi tambahan yang mampu membedakan antara aktivitas pengguna sah dan serangan otomatis. Kondisi ini menunjukkan bahwa autentikasi berbasis username dan password saja tidak lagi memadai untuk menghadapi pola serangan siber modern yang bersifat masif dan terotomatisasi.

Lebih lanjut, hasil analisis memperlihatkan bahwa keberhasilan serangan credential stuffing tidak hanya dipengaruhi oleh kelemahan sistem login, tetapi juga oleh perilaku pengguna dalam mengelola kredensial. Penggunaan kata sandi yang sama pada berbagai layanan digital menyebabkan kebocoran data dari satu platform dapat berdampak langsung pada keamanan platform lain. Dalam konteks ini, sistem login multi-user yang tidak memiliki mekanisme proteksi tambahan cenderung menjadi target empuk bagi penyerang.

Pada skenario analisis yang melibatkan penerapan autentikasi berlapis, terjadi penurunan signifikan terhadap tingkat keberhasilan serangan. Meskipun kredensial utama berhasil digunakan, sistem tetap menolak akses karena tidak terpenuhinya faktor autentikasi tambahan. Hal ini menunjukkan bahwa autentikasi berlapis mampu memutus rantai serangan credential stuffing dengan menghilangkan ketergantungan sistem pada satu jenis verifikasi saja. Dengan demikian, kebocoran kredensial tidak serta-merta berujung pada pengambilalihan akun.

Selain itu, analisis terhadap mekanisme verifikasi tambahan menunjukkan bahwa pembatasan akses berbasis waktu memiliki peran penting dalam mempersempit ruang gerak penyerang. Ketika sistem menerapkan verifikasi sementara dengan batas waktu tertentu, peluang penyerang untuk melakukan eksploitasi lanjutan menjadi sangat terbatas. Mekanisme ini secara tidak langsung meningkatkan efisiensi pengendalian akses tanpa harus menambah kompleksitas sistem secara berlebihan.

Dari sisi keamanan transmisi data, hasil pengamatan menunjukkan bahwa perlindungan terhadap proses autentikasi juga perlu mempertimbangkan jalur komunikasi antara pengguna dan sistem. Sistem login yang tidak melindungi data kredensial selama proses transmisi berpotensi membuka celah penyadapan. Oleh karena itu, keberadaan

mekanisme pengamanan pada tahap komunikasi menjadi faktor pendukung dalam memperkuat ketahanan sistem login secara keseluruhan.

Hasil analisis ini sejalan dengan temuan penelitian sebelumnya yang menyatakan bahwa autentikasi berlapis merupakan salah satu strategi paling efektif dalam meningkatkan keamanan sistem login. Namun demikian, penelitian ini menekankan bahwa penerapan autentikasi berlapis harus disesuaikan dengan karakteristik sistem dan kebutuhan pengguna agar tidak menimbulkan hambatan akses yang berlebihan. Dengan kata lain, peningkatan keamanan perlu diimbangi dengan pertimbangan terhadap kenyamanan dan efisiensi penggunaan sistem.

Secara keseluruhan, pembahasan ini menunjukkan bahwa ketahanan sistem login multi-user terhadap serangan credential stuffing tidak dapat dicapai hanya dengan memperkuat satu komponen keamanan. Diperlukan pendekatan yang menyeluruh melalui kombinasi mekanisme autentikasi, pengendalian akses, serta pengamanan jalur komunikasi. Pendekatan ini memungkinkan sistem login untuk tetap adaptif terhadap perkembangan pola serangan siber yang semakin kompleks.

KESIMPULAN

Berdasarkan hasil analisis yang telah dilakukan, dapat disimpulkan bahwa sistem login multi-user yang hanya menggunakan autentikasi satu faktor memiliki tingkat risiko yang tinggi terhadap serangan credential stuffing. Evaluasi menunjukkan bahwa penerapan autentikasi berlapis secara signifikan meningkatkan ketahanan sistem terhadap upaya akses tidak sah. Oleh karena itu, autentikasi berlapis merupakan pendekatan yang efektif untuk meminimalkan dampak serangan credential stuffing pada sistem login multi-user.

Saran

Penelitian selanjutnya disarankan untuk memperluas analisis dengan melibatkan lebih banyak variasi skenario serangan dan kondisi lingkungan jaringan. Selain itu, kajian mengenai keseimbangan antara peningkatan keamanan dan kenyamanan pengguna perlu dilakukan agar sistem login tetap aman tanpa mengurangi efisiensi penggunaan.

DAFTAR PUSTAKA

Azhar, W., Arkarni, A., & Atthariq. (2020). Sistem keamanan pada halaman login menggunakan one-time password. JESSI (Journal of Embedded Systems, Security and Intelligent Systems), 1(2).

Buana, K. G. J. W., Widyawati, L., & Asroni, O. (2025). Analisis dan implementasi keamanan authentication menggunakan multi-factor authentication pada aplikasi web. Prosiding Seminar Nasional CORISINDO.

Khairina, D. M. (2011). Analisis keamanan sistem login. Jurnal Informatika Mulawarman, 6(2).

Thomas, K., Grier, C., Paxson, V., & Song, D. (2019). Protecting accounts from credential stuffing with password breach alerting. In Proceedings of the 28th USENIX Security Symposium (pp. 155–172).

U.S. Department of Health and Human Services. (2019). Credential stuffing. HHS Cybersecurity Program (HC3) White Paper.