ABSTRACT

The availability of various web-based services, both in the form of applications and information systems, has encouraged internet users to take advantage of as many services as possible, both for educational and work purposes. Each of these services requires users to sign in for identification purpose. The increasing number of services used, increasing the burden on users to manage each account. Single Sign On (SSO) is one of the methods used to address the management needs of the account, and the Central Authentication Service (CAS) Server can be used as a client-compatible authentication center from various programming languages. The increasing usage of E-learning and Blog Multiuser in STMIK Jenderal A. Yani, as well as password reset requests on the web services, encourage the need for practical user management implementations such as SSO. In order to provide reliable and durable authentication services, performance and security testing of these services is required.

This research is done by analyzing the authentication with CAS Server on SSO network which applied to web based services such as E-learning and Multiuser Blog. This study also discusses the testing of CAS Server performance and security levels by using some of the standards of the Open Web Application Security Project (OWASP) Top 10 Application Security Risk. Testing is done by utilizing some hacking tools to test the corresponding standards.

The results show that communication between SSO clients with CAS Server can not be penetrated by hacking application, if on CAS Server is used SSL security protocol. In addition, ports not used for authentication purposes should be closed. While the maximum level of performance (response time and load test) on CAS Server is 3,850,000 request with total request time 4,818.275 ms

Keywords : Single Sign On, CAS, Hacking

INTISARI

Ketersediaan berbagai layanan berbasis web, baik berupa aplikasi maupun sistem informasi, telah mendorong pengguna internet untuk memanfaatkan sebanyak mungkin layanan yang tersedia, baik untuk kepentingan pendidikan maupun pekerjaan. Masing-masing layanan tersebut mengharuskan setiap pengguna untuk *sign-in* guna identifikasi pengguna. Meningkatnya jumlah layanan yang digunakan, meningkatkan beban bagi pengguna untuk mengelola masing-masing akun. Single Sign On (SSO) adalah salah satu metode yang digunakan guna mengatasi kebutuhan pengelolaan akun tersebut, dan Central Authentication Service (CAS) Server dapat digunakan sebagai pusat otentikasi yang kompatibel dengan klien dari berbagai bahasa pemrograman. Tingginya tingkat penggunaan E-learning dan Blog Multiuser di STMIK Jenderal A. Yani, serta permintaan reset password pada layanan web tersebut, mendorong kebutuhan penerapan manajemen user yang praktis seperti SSO. Guna menyediakan layanan otentikasi yang *reliable* dan *durable*, diperlukan pengujian terhadap performa dan keamanan layanan tersebut.

Penelitian ini dilakukan dengan menganalisis otentikasi dengan CAS Server pada jaringan SSO yang diterapkan pada layanan berbasis web berupa E-learning dan Blog Multiuser. Penelitian ini juga membahas pengujian tingkat performa dan keamanan CAS Server dengan menggunakan beberapa standar dari Open Web Application Security Project (OWASP) *Top 10 Application Security Risk*. Pengujian dilakukan dengan memanfaatkan beberapa *tools* hacking guna menguji standar yang bersesesuaian.

Hasil penelitian menunjukkan bahwa komunikasi antara klien SSO dengan CAS Server tidak dapat ditembus oleh aplikasi *hacking*, jika pada CAS Server tersebut digunakan protokol keamanan SSL. Selain itu, port yang tidak digunakan untuk keperluan otentikasi sebaiknya ditutup. Sedangkan tingkat performa (*response time* dan *load test*) maksimal pada CAS Server adalah 3.850.000 request dengan total time request sebesar 4.818,275 ms.

Kata kunci – Single Sign On (SSO), CAS, Hacking.