SECURITY ASSESSMENT MENGGUNAKAN *TOOL* NESSUS UNTUK MENCARI CELAH KEAMANAN WEB APLIKASI MOU INSTITUSI PENDIDIKAN

Security Assessment by Using Tool Nessus To Find Security Vulnerabilities of MoU Web Application in Educational Institution

Firman Tito Widyantoro, Chayadi Oktomy Noto S., Dwijoko Purbohadi

ABSTRACT

Artikel ini berisi tentang hasil *security assessmet* yang dilakukan di institusi pendidikan. Institusi pendidikan telah menggunakan teknologi informasi untuk mendukung proses bisnis serta proses akademis untuk itu aspek keamanan menjadi suatu hal yang penting untuk diperhatikan. Salah satu aset teknologi informasi yang penting untuk dilindungi adalah web aplikasi MoU. Aspek keamanan pada web aplikasi penting untuk diteliti karena web aplikasi ini merupakan aset teknologi informasi yang menyimpan informasi berupa perjanjian dan nota kesepahaman antara institusi pendidikan dan pihak lain sehingga jika terjadi serangan dikhawatirkan informasi yang bersifat rahasia dapat dicuri dan disalahgunakan. Di lokasi penelitian diketahui belum pernah dilakukan *security assessment* Hal ini menjadi kekhawatiran tersendiri bagi organisasi jika sewaktu waktu terjadi penyerangan. Dengan belum dilakukannya *security assessment* maka belum diketahui pula jenis serangan yang mungkin terjadi pada web aplikasi MoU. Pada penelitian ini dilakukan dengan metode VAPT (*Vulnerability Assessment & Penetration Testing*), VAPT merupakan metode yang dapat digunakan untuk melakukan penilaian serta pengujian terhadap kerentanan keamanan yang ada. Pencarian kerentanan yang terdapat pada web MoU menggunakan tool Nessus. *Security assessment* dilakukan untuk menemukan kerentanan keamanan dan mengetahui dampak yang diberikan pada aset teknologi informasi. Dari hasil penelitian ditemukan masih terdapat kerentanan keamanan yang bisa dieksploitasi dan dampaknya menimbulkan kerugian bagi institusi pendidikan.

Keyword : security assessment, vulnerability assessment and penetration testing,

Pendahuluan

Penggunaan web serta sumber daya online semakin meningkat beberapa decade belakangan ini, ancaman terhadap integritas dan keamanan informasi dan data telah meningkat. Setiap hari ditemukan kasus peretasan dan eksploitasi dengan cara yang baru. Untuk itu menemukan kerentanan pada sistem dan menginstal patch keamanan terbaru telah menjadi sesuatu yang penting bagi setiap organisasi yang terhubung ke internet [1]. Pada tahun 2018, Symantec Internet Security Threat Report (ISTR) menemukan bahwa deteksi malware pada coinminer meningkat sebanyak 8500 %, dan peretasan terhadap perangkat IoT meningkat sebanyak 600% [2]. Pembobolan keamanan ini seharusnya menjadi masalah yang serius tentang bagaimana seharusnya data dilindungi dari peretasan.

Untuk dapat megurangi jumlah peretasan yang terjadi serta mengurangi dampaknya organisasi dapat melakukan *security assessment*. *Security assessment* merupakan salah satu kegiatan yang bisa digunakan untuk meningkatkan keamanan sistem informasi. *Security assessment* sendiri merupakan sebuah penilaian keamanan terhadap sistem informasi yang diimplementasikan pada sebuah organisasi [3].

Kegiatan tersebut dinilai perlu untuk meningkatkan mekanisme pelindung keamanan informasi yang bersifat rahasia. Langkah yang dilakukan berupa tindakan pencegahan, deteksi, dan respons [4].

Di lokasi penelitian diketahui belum pernah dilakukan proses *security assessment*. Hal ini menjadi kekhawatiran tersendiri bagi organisasi jika sewaktu waktu terjadi penyerangan. Dengan belum dilakukannya *security assessment* maka belum diketahui pula jenis serangan yang mungkin terjadi pada web aplikasi MoU, seberapa parah dampak yang ditumbulkan, serta bagaimana cara mengatasi setiap serangan yang terjadi.

oleh sebab itu pada penelitian ini kan dilakukan *security assessment* untuk menemukan jenis kerentanan keamanan yang mungkin terjadi pada aplikasi web MoU dan dampak yang disebabkan oleh setiap kerentanan keamanan yang ditemukan. Penelitian ini dilakukan dengan metode VAPT (Vulnerability Assessment and Penetration Testing). Metode ini merupakan gabungan dari dua aktifitas yaitu vulnerability assessment dan penetration testing dengan tujuan untuk menilai keamanan pada

suatu sistem informasi [5]. Pada tahap vulnerability assessment digunakan untuk analisis dan menemukan kerentanan yang ada dan penetration testing merupakan tahap eksploitasi kerentanan keamanan yang ditemukan untuk mengevaluasi kerusakan serta dampak yang ditimbulkan terhadap sistem yang diuji. Dua aktifitas ini bisa dikombinasikan untuk mendapatkan hasil analisa keamanan yang lebih baik [6]. Tool yang digunakan untuk menemukan kerentanan keamanan adalah Nessus. Nessus adalah salah satu produk penilaian kerentanan keamanan yang paling banyak digunakaan pertama kali dirilis oleh Renaud Deraison pada tahun 1998. alat ini telah menjadi salah satu alat pemindaian kerentanan yang paling populer digunakan di seluruh industri selama 15 tahun terakhir [7]. Nessus menyediakan pemindaian kerentanan untuk perangkat jaringan, virtual host, sistem operasi, basis data, aplikasi web, dan jaringan hibrid IPv4 / IPv6 [8]. Nessus menggunakan Common Vulnerability and Exposure (CVE) sebagai standarnya. CVE adalah standar untuk penamaan kerentanan keamanan informasi [8]. Salah satu fitur yang menarik dari nessus adalah ini merupakan aplikasi open source dan banyak orang yang berkontribusi setiap hari. Akan ada plug-in untuk kerentanan baru dalam beberapa hari setelah kerentanan keamanan dirilis ke publik [9].

Manfaat: Hasil penelitian ini bisa digunakan sebagai bahan evaluasi untuk meningkatkan keamanan pada web aplikasi MoU milik institusi pendidikan.

Metode

A. Vulnerability Assessment

Pada bagian ini penguji bertujuan untuk menemukan informasi penting tentang target yang diuji dan melakukan scanning untuk menemukan kerentanan [10]. Vulnerability assessment adalah strategi yang menggunakan pendekatan sistematis dan proaktif untuk menemukan kerentanan. Ini digunakan untuk menemukan masalah baik yang diketahui atau yang tidak diketahui dalam sistem.

B. Penetration Testing

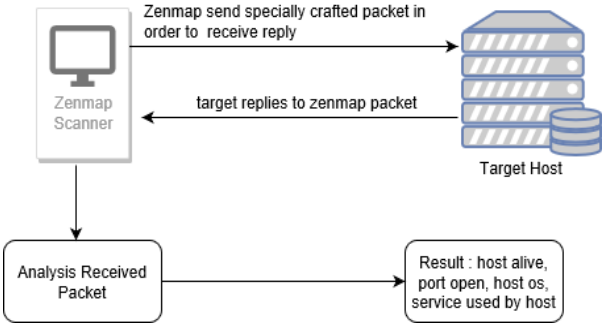
Penetration testing menguji keamanan pada sebuah jaringan atau sistem dengan melakukan serangan [10]. Tujuan penguji melakukan penetration testing adalah untuk mengecek tingkat kesulitan dalam mengeksploitasi kerentanan dan dampak yang ditimbulkan.

Scope

Scope adalah tahap untuk menentukan cakupan pada penelitian. Cakupan pada penelitian ini didasarkan pada penemuan asset kritis teknologi informasi yang telah dilkukan pada penelitian sebelumnya [11]. Salah satu asset kritis yang ada yaitu aplikasi web MoU.

Reconnaissance

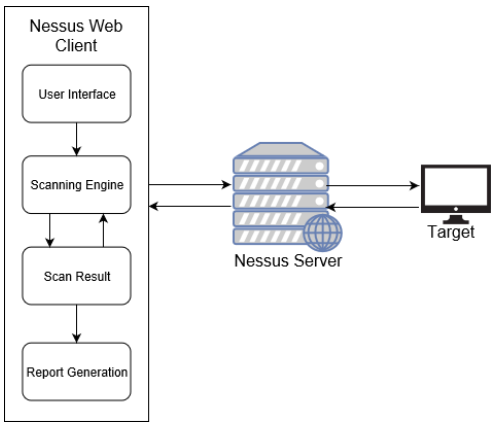
Reconnaisance adalah mencari informasi dasar seperti sistem operasi, alamat IP, port dan web server yang digunakan pada web aplikasi MoU. Reconnaisance dilakukan dengan menggunakan tool Nmap Version 7.70. Nmap menggunakan ip paket untuk menentukan apa host yang tersedia dan apa servis yang disediakan oleh host.



Gambar 1 Zenmap Work Flow

Vulnerability Detection

Vulnerability detection merupakan proses mencari celah keamanan pada web aplikasi MoU menggunakan tool Nessus Version 7.1.2 pada aplikasi peramban Microsoft Edge pada sistem operasi windows.



Gambar 2 Vulnerability Scanner Architecture

Information Analysis and Planning

Menganalisis informasi tentang temuan celah keamanan yang ditemukan pada tahap vulnerability detection. Dan membuat rencana penetration testing terhadap sistem yang diuji. Dari hasil *vulnerability detection* ditemukan bahwa aplikasi MoU memiliki beberapa kerentanan salah satunya SQL Injection

dengan tingkat dampak yang diberikan terhadap sistem yaitu *high*.

SQL Injection attack adalah salah satu Teknik *hacking* dimana penyerang menambahkan statemen SQL melalui *field* masukan yang terdapat pada aplikasi web untuk mendapatkan akses. Kurangnya validasi terhadap masukan yang terdapat pada aplikasi web bisa menyebabkan serangan ini berhasil [12].

dan juga dari hasil scan ditemukan bahwa aplikasi web dilindungi oleh firewall sehingga perlu melakukan upaya agar statement SQL yang dikirimkan tidak terkena filter. Firewall memiliki fungsi untuk melindungi data dan resource dari kerusakan akibat dari penyusup yang masuk kedalam jaringan komputer [13].

Penetration Testing

Simulasi serangan terhadap sistem yang sudah disebutkan diatas untuk mendapatkan informasi atau data yang terdapat pada sistem.

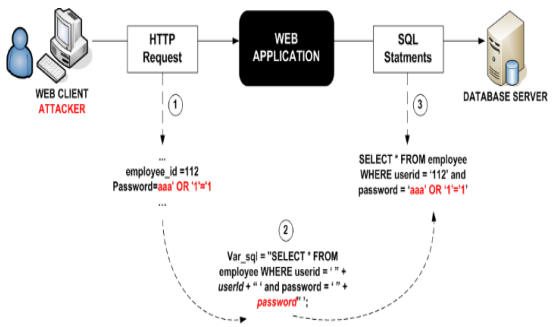
Privilege Escalation

kondisi dimana kita melakukan sebuah eksploitasi agar mendapatkan hak akses yang lebih tinggi.

Report

Tahap membuat laporan dari hasil setiap proses yang telah dilakukan.

Hasil



Gambar 3 SQL Injection Attack

Gambar 3 diatas merupakan gambar bagaimana serangan SQL Injection terjadi. Penyerang mengirimkan http request berisi SQL statemen yang telah dimodifikasi dari web client menuju server dengan tujuan menggati SQL statemen yang asli menjadi SQL statemen yang telah dimodifikasi untuk memperoleh data yang diinginkan dari database.

Pada proses penetration testing penguji melakukan serangan dengan metode SQL Injection, ini bertujuan untuk mendapatkan informasi seperti *user credential, Email,* dan informasi penting lain dari database. Penguji memasukkan SQL statemen yang telah dimodifikasi pada URL. Pada pengaturan default setiap website yang menggunakan database memiliki 3 kerentanan yang sangat umum yaitu:

1. Setiap website yang masih pada pengaturan default masih menggunakan database information_schema.
2. Dengan menggunakan information_schema.tables dapat melihat seluruh table yang terdapat pada website.
3. table_name adalah fungsi untuk melihat nama dari table yang terdapat pada information_schema.tables.

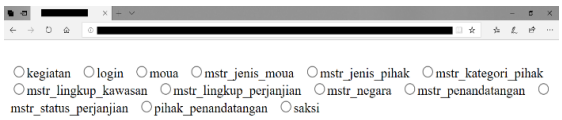
penguji menggunakan *Union Based SQL Queries* untuk mengeksploitasi database. Dengan menggunakan *Union Based SQL Queries* penguji menggabungkan query yang telah dimodifikasi dan query yang aman dengan menggunakan kata UNION untuk mendapatkan data tentang table lain [12]. Eksploitasi SQL Injection dilakukan dengan tahap berikut:

Gambar 4 SQL Injection Tahap I

Tahap 1: pada gambar 4 adalah hasil menemukan jumlah kolom yang terdapat pada tabel. Pada tahap ini SQL statemen yang dimasukkan bertujuan untuk mendapatkan jumlah kolom yang ada pada tabel database dengan menggunakan klausa SQL "*ORDER BY*". Penulisan SQL statemen secara lengkap adalah "$URL?parameter = 1' + ORDER\ BY + 3$". 3 merupakan jumlah kolom yang terdapat pada tabel.

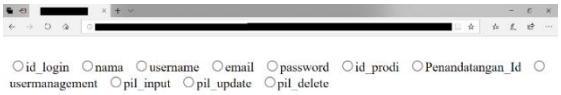
Gambar 5 SQL Injection Tahap II

Tahap 2: gambar 5 menunjukkan kolom yang rentan dan bisa disisipi oleh SQL statemen yang berbahaya. Pada tahap ini SQL statemen yang dimasukkan bertujuan untuk menemukan kolom yang bisa digunakan untuk memasukkan SQL statemen berbahaya untuk menemukan tabel atau kolom lain yang ada pada database. Penulisan SQL statemen secara lengkap adalah "URL?parameter=-1'+UNIOIN ALL SELECT+1,2,3".



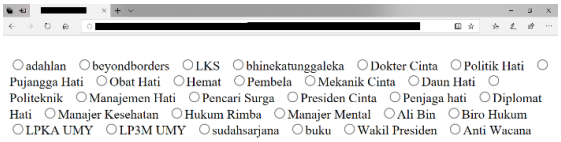
Gambar 6 SQL Injection Tahap III

Tahap 3: pada gambar 6 menunjukan nama tabel yang terdapat pada database. Pada tahap ini SQL statemen yang dimasukan bertujuan untuk mendapatkan semua nama tabel yang ada biasanya tabel pada website disimpan pada database information_schema. Penulisan SQL statemen secara lengkap adalah "URL?parameter=-1' + UNION ALL SELECT + 1, 2, table_name FROM information.schema.tables WHERE table_schema = database()".



Gambar 7 SQL Injection IV

Tahap 4: pada gambar 7 memperlihatkan nama kolom yang terdapat pada sebuah tabel. Pada tahap ini SQL statemen yang dimasukkan bertujuan untuk mendapatkan daftar kolom yang terdapat pada tabel tertentu. Penulisan SQL statemen secara lengkap adalah "URL?parameter=-1'+UNION ALL SELECT+ 1,2, column_name FROM information_schema.columns WHERE table_name ='TableName'".



Gambar 8 SQL Injection Tahap V

Tahap 5: gambar 8 memperlihatkan data yang terdapat pada kolom. Pada tahap ini SQL statemen yang dimasukkan bertujuan utnuk membaca data yang terdapat pada kolom disebuah tabel tertentu**.** Penulisan SQL statemen secara lengkap adalah "URL?parameter=-1'+UNION ALL SELECT+ 1,2,'ColumnName' FROM 'TableName'".

Kesimpulan

masih ada celah keamanan yang bisa dieksploitasi dan dapat mempengaruhi proses bisnis dari Perguruan Tinggi. Selanjutnya hasil penelitian dan temuan celah keamanan ini akan dibuatkan laporan yang ditujukan kepada pihak Perguruan Tinggi.

Daftar Pustaka

[1] J. Bau, E. Bursztein, D. Gupta, and J. Mitchell, "State of the art: Automated black-box web application vulnerability testing," *Proc. - IEEE Symp. Secur. Priv.*, pp. 332–345, 2010.

[2] P. Allisy-Roberts *et al.*, "Executive

Summary," *J. ICRU*, vol. 6, no. 2, pp. 7–8, 2006.

[3] A. A. Aziz, "Scoping Security Assessments - A Project Management Approach," *Security*, 2011.

[4] D. Dalalana Bertoglio and A. F. Zorzo, "Overview and open issues on penetration test," *J. Brazilian Comput. Soc.*, vol. 23, no. 1, pp. 1–16, 2017.

[5] J. N. Goel and B. M. Mehtre, "Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology," *Procedia Comput. Sci.*, vol. 57, pp. 710–715, 2015.

[6] P. S. Shinde and S. B. Ardhapurkar, "Cyber Security Analysis Using Vulnerability Assessment and Penetration Testing," *IEEE Spons. World Conf. Futur. Trends Res. Innov. Soc. Welf. (Startup Conclave)*, pp. 1–5, 2016.

[7] H. Kumar, *Learning Nessus for Penetration Testing*. 2014.

[8] H. C. Li, P. H. Liang, J. M. Yang, and S. J. Chen, "Analysis on cloud-based security vulnerability assessment," *Proc. - IEEE Int. Conf. E-bus. Eng. ICEBE 2010*, pp. 490–494, 2010.

[9] I. Mukhopadhyay, S. Goswami, and E. Mandal, "Web Penetration Testing using Nessus and Metasploit Tool," *IOSR J. Comput. Eng.*, vol. 16, no. 3, pp. 126–129, 2014.

[10] G. Buja, K. Bin Abd Jalil, F. Bt Hj Mohd Ali, and T. F. A. Rahman, "Detection model for SQL injection attack: An approach for preventing a web application from the SQL injection attack," *Comput. Appl. Ind. Electron. (ISCAIE), 2014 IEEE Symp.*, pp. 60–64, 2014.

[11] A. M. A. Yuhaz, "Risk Management Teknologi Informasi Menggunakan Framework OCTAVE (Operationally Critical Threat, Asset And Vulnerability Evaluation) Dan FMEA (Failure Mode And Effect Analysis) Di Institusi Pendidikan XYZ," Universitas Muhammadiyah Yogyakarta, 2018.

[12] A. Tajpour, S. Ibrahim, and M. Sharifi, "Web Application Security by SQL Injection DetectionTools," *IJCSI Int. J. Comput. Sci. Issues*, vol. 9, no. 2, pp. 332–339, 2012.

[13] P. E. Bell, "United States Patent," vol. 153, 1992.

PENULIS:

Firman Tito Widyantoro

Teknik Informatika, Teknik, Universitas Muhammadiyah Yogyakarta, Yogyakarta.

Email: firman.tito.2014@ft.umy.ac.id