SECURITY ASSESMENT MENGGUNAKAN *OPEN WEB APPLICATION SECURITY PROJECT ZED ATTACK PROXY* (OWASP ZAP) UNTUK MENCARI KERENTANAN KEAMANAN WEB KRS DARING (KARTU RENCANA STUDI DARING) DI INSTITUSI PENDIDIKAN

(Security Assessment by using Open Web Application Security Project Zed Attack Proxy (OWASP ZAP) for Finding Security Vulnerabilities Web Course Selection Form Online in Educational Institution)

Galih Satya Prihatmadi, Chayadi Oktomy Noto Susanto, Dwijoko Purbohadi

ABSTRACT

Artikel ini berisi informasi tentang hasil penelitian *security assessment* yang dilakukan di Institusi Pendidikan. Institusi pendidikan telah menggunakan teknologi informasi untuk mendukung proses bisnis serta proses akademik untuk itu aspek keamanan menjadi suatu hal yang penting untuk diperhatikan. Salah satu aset teknologi informasi yang penting untuk dilindungi adalah Web KRS Daring (Kartu Rencana Studi Daring). Aspek keamanan pada Web KRS Daring penting untuk diteliti karena web tersebut merupakan aset teknologi informasi yang mempunyai data sangat penting berupa data pribadi mahasiswa, mata kuliah yang diambil, transkrip nilai, data kehadiran, data kendaraan, dan data pembayaran. Pada penelitian ini dilakukan dengan metode VAPT (*Vulnerability Assessment and Penetration Testing*), VAPT merupakan metode yang dapat digunakan untuk melakukan penilaian serta pengujian terhadap kerentanan keamanan yang ada. *Security assessment* dilakukan untuk menemukan kerentanan keamanan dan mengetahui dampak yang diberikan pada aset teknologi informasi. Dari hasil penelitian ini ditemukan masih terdapat kerentanan keamanan yang bisa dieksploitasi dan dampaknya menimbulkan kerugian bagi Institusi Pendidikan. Penelitian ini digunakan sebagai laporan kepada pihak institusi pendidikan sebagai bahan untuk dilakukan proses evaluasi dan peningkatan keamanan terhadap web aplikasi yang dimilikinya. Penelitian ini hanya dilakukan didalam lingkungan Institusi Pendidikan, sehingga kegiatan ini belum sepenuhnya menggambarkan tentang kemungkinan serangan sebenarnya yang berasal dari luar lingkungan Institusi Pendidikan.

Keywords: *Security Assessment, Vulnerability Assessment, Penetration Testing, OWASP, VAPT*.

PENDAHULUAN

Informasi yang dikelola dan disebarkan harus memiliki integritas atau dapat dipercaya, oleh sebab itu keamanan terhadap informasi menjadi hal yang penting, karena dapat mempengaruhi citra institusi pendidikan tersebut. Ancaman pada informasi dapat bersumber dari mana saja. Untuk mengetahui dan meminimalisir ancaman keamanan yang dapat menyebabkan risiko, perlu dilakukan kegiatan untuk mengukur risiko tersebut. *Security Assessment* adalah serangkaian kegiatan yang ditempuh untuk menilai sebuah keamanan pada web [1]. Tujuan dari kegiatan ini adalah mengetahui kerentanan keamanan dan risiko yang ditimbulkan atas percobaan serangan pada sebuah web. Risiko yang dihasilkan dapat berupa pengambilan informasi penting atau upaya untuk menggagalkan proses teknologi informasi yang berjalan.

Kegiatan tersebut dinilai perlu untuk meningkatkan mekanisme pelindung keamanan informasi yang bersifat rahasia. Langkah yang dilakukan berupa tindakan pencegahan, deteksi, dan respons [2]. Merujuk pada penelitian sebelumnya [3] terdapat daftar urutan aset kritis milik Institusi Pendidikan. Salah satu aset terpenting milik Institusi Pendidikan adalah Web KRS Daring (Kartu Rencana Studi Daring).

Namun diketahui bahwa, Web KRS Daring tersebut belum pernah dilakukan upaya untuk pengukuran kerentanan keamanan yang dapat menimbulkan risiko atau bisa disebut sebagai *security assessment*. Hal ini menjadi kekhawatiran tersendiri bagi organisasi jika

sewaktu waktu terjadi penyerangan, karena web tersebut berisi data sangat penting berupa data pribadi mahasiswa, mata kuliah yang diambil, transkrip nilai, data kehadiran, data kendaraan, dan data pembayaran.

Oleh sebab itu perlu adanya penilaian keamanan atau *security assessment* pada Web KRS Daring milik Institusi Pendidikan. Kegiatan tersebut dilakukan dengan kerangka kerja VAPT (*Vulnerability Assessment and Penetration Testing*). Kerangka kerja tersebut digunakan untuk melakukan kegiatan *security assessment*. Kerangka kerja VAPT terdiri atas dua kegiatan utama, yaitu *Vulnerability Assessment* dan *Penetration Testing* yang tujuannya adalah untuk mendapatkan informasi penting pada sebuah web aplikasi [4].

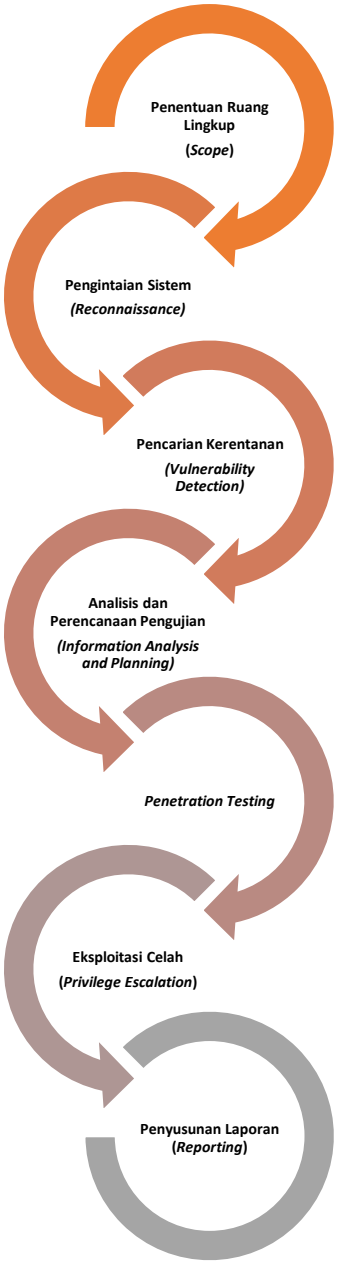
Vulnerability Assessment adalah pencarian kerentanan keamanan sistem yang dapat menyebabkan kegagalan proses teknologi informasi. Setelah penyerang menemukan kerentanan, penyerang menentukan cara untuk mengaksesnya. Dengan demikian ancaman terhadap kerahasiaan yang dimiliki oleh aplikasi meningkat. Penyerang menggunakan *tool* atau aplikasi untuk mengidentifikasi kerentanan aplikasi [5]. Aplikasi yang digunakan untuk mengetahui kerentanan keamanan pada aset sistem informasi adalah OWASP ZAP (*Open Web Application Security Project Zed Attack Proxy*). OWASP ZAP adalah aplikasi untuk menemukan *vulnerabilities* dalam suatu *web application* [6]. Setelah diketahui hasil dari *vulnerabilities* dari *web application* maka tahap selanjutnya adalah dilakukan *penetration testing*.

Penetration Testing adalah sebuah cara untuk mengidentifikasi celah keamanan pada penerapan mekanisme keamanan sebuah sistem. Kegiatan ini dilakukan dengan cara menyerang terhadap sistem komputer dengan tujuan menemukan kelemahan keamanan, berpotensi mendapatkan akses ke sana, fungsi dan datanya [7].

Hasil simulasi serangan ini kemudian didokumentasikan dan disajikan sebagai laporan kepada Institusi Pendidikan. Institusi Pendidikan dapat menjadikan artikel ini sebagai bahan evaluasi untuk meningkatkan keamanan pada Web KRS Daring.

METODE

Penelitian ini menggunakan kerangka kerja VAPT (*Vulnerability Assessment and Penetration Testing*) digunakan untuk menguji keamanan pada Web KRS Daring (Kartu Rencana Studi Daring) milik Institusi Pendidikan XYZ, untuk prosesnya bisa dilihat pada **Gambar 1**. Pada gambar tersebut terdapat 7 proses dan akan dijelaskan sebagai berikut.



***Gambar 1** Proses VAPT*

a. Penentuan Ruang Lingkup (*Scope*)

Pada tahap ini telah ditentukan Ruang Lingkup (*Scope*) seperti yang tertera pada subbab Batasan Masalah. Pengujian akan berfokus pada Web Aplikasi milik Institusi

Pendidikan yaitu KRS Daring (Kartu Rencana Studi Daring).

b. Pengintaian Sistem (*Reconnaissance*)

Pada tahap ini penulis akan mencari informasi dasar target dan mengumpulkan informasi terkait sistem seperti *IP Address* dan Port dengan menggunakan *tool software Nmap Version 7.70* pada sistem operasi *Parrot*.

c. Pencarian Kerentanan Keamanan (*Vulnerability Detection*)

Pada tahap ini penulis akan melakukan proses pencarian kerentanan keamanan dengan menggunakan *tool software* yaitu OWASP ZAP 2.7.0, nantinya digunakan untuk mendeteksi berbagai kerentanan dari Web KRS Daring. Dari hasil pencarian tersebut akan didapatkan daftar kerentanan yang nantinya akan digunakan sebagai bahan untuk perencanaan pengujian ke tahap berikutnya.

d. Analisis Perencanaan dan Perencanaan Pengujian (*Information Analysis and Planning*)

Pada tahap ini peneliti melakukan analisis untuk menentukan celah yang akan diuji dari hasil pencarian kerentanan pada Web KRS Daring. Peneliti memilih satu celah yang digunakan untuk bahan *penetration testing* yaitu *Secure Pages Include Mixed Content* yang memiliki kerentanan *level Low*, alasan memilih kerentanan ini karena bisa dimanfaatkan untuk mendapatkan akun nama pengguna dan kata sandi KRS Daring. *Tools* yang digunakan untuk *penetration testing* adalah *Arpspoof* dan *SSLStrip*, untuk pendekatannya menggunakan metode *Social Engineering*.

e. Penetration Testing

Pada tahap ini penulis akan melakukan simulasi penyerangan terhadap target yang diuji yaitu Web KRS Daring. Simulasi penyerangan akan dilakukan sesuai hasil rencana pengujian dari tahap sebelumnya.

f. Eksploitasi Kerentanan (*Privilege Escalation*)

Setelah selesai melakukan tahap *penetration testing* selanjutnya adalah tahap Eksploitasi Kerentanan (*Privilege Escalation*) yaitu pemanfaatan kerentanan dari hasil *penetration testing*. Pemanfaatan yang dimaksud adalah untuk mengambil informasi, merubah informasi, dan merubah hak akses.

g. Penyusunan Laporan (*Reporting*)

Pada tahap ini penulis menyusun laporan hasil dari pengujian yang sudah dilakukan pada Web KRS Daring.

Alat Penelitian

a. OWASP ZAP

Aplikasi *open source* untuk melakukan pencarian kerentanan pada *website* dengan cara *scanner* otomatis pada aplikasi ZAP.

b. Nmap

Tool open source untuk eksplorasi jaringan. *Nmap* melakukan *scanning* terhadap satu host untuk mengetahui layanan yang digunakan (nama dan versi aplikasi), sistem operasi dan jenis *filter firewall* yang digunakan. *Nmap* berjalan di semua sistem operasi komputer, seperti *Linux*, *Windows*, dan *Mac OS X*. *Nmap* menjalankan setiap baris perintah menggunakan *command prompt* atau terminal. *Nmap* juga tersedia dalam versi *GUI* dengan nama *Zenmap* [8].

c. Arpspoof

Tool untuk memanipulasi paket ARP (*Address Resolution Protocol*) dari *client* target agar semua paket – paket data dari *client* dialihkan ke *hacker* terlebih dahulu, ARP merupakan *protocol* yang bertugas memetakan *IP Address* menjadi *MAC Address* melalui penghubung antara *datalink layer* dan *IP layer* pada *TCP/IP* dan bekerja pada *layer* 2 [9].

d. SSLStrip

Tool untuk menyerang web yang dilindungi oleh https, cara kerjanya mencegah peralihan web dari http ke https dengan secara aktif mengubah *response* dari server sehingga pengunjung web akan tetap pada di *protocol* http.

HASIL DAN PEMBAHASAN

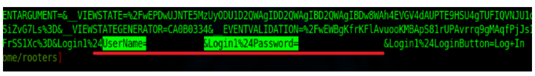
Tujuan penulisan artikel ini adalah untuk laporan yang ditujukan kepada institusi pendidikan sebagai bahan evaluasi pada Web KRS Daring. Institusi Pendidikan dapat melakukan evaluasi berdasarkan tolak ukur kegiatan *security assessment* dengan tolak ukur yang dijadikan sebagai bahan perbaikan adalah temuan kerentanan keamanan yang berhasil

dilakukan penetrasi. *Security Assessment* menggunakan metode VAPT.

Secure Pages Include Mixed Content memiliki kerentanan *level Low*. Kerentanan tersebut memanfaatkan kelemahan sistem dari web KRS Daring yang kebanyakan web dirancang memakai https melalui *request http* (*port* 80) atau *https* (*port* 443). Web *port* 80 biasanya hanya sebagai jembatan untuk menuju web yang sebenarnya pada *port* 443, dengan kata lain http sebagai gerbang menuju https. Maka dari itu kerentanan tersebut bisa dimanfaatkan untuk mendapatkan akun nama pengguna dan kata sandi Web KRS Daring.

SSLStrip adalah *tool* untuk menyerang web yang dilindungi oleh https, cara kerjanya mencegah peralihan web dari http ke https dengan secara aktif mengubah *response* dari server sehingga pengunjung web akan tetap pada di *protocol* http. Sedangkan *Arpspoo*f adalah *tools* untuk memanipulasi paket ARP (*Address Resolution Protocol*) dari *client* target agar semua paket – paket data dari *client* dialihkan ke *hacker* terlebih dahulu, ARP merupakan *protocol* yang bertugas memetakan *IP Address* menjadi *MAC Address* melalui penghubung antara datalink layer dan *IP Layer* pada *TCP/IP* dan bekerja pada *layer* 2 [10]. Pendekatan *Social Engineering* adalah salah satu metode yang biasa digunakan oleh seorang *hacke*r untuk memperoleh informasi tentang targetnya dengan cara menipu secara halus tanpa disadari sampai bisa meyakinkan si targetnya [11].

Setelah melakukan pendekatan *Social Engineering* kepada Mahasiswa maka hasilnya pada **Gambar 2** adalah mendapatkan akun pengguna dan kata sandi KRS Daring milik Mahasiswa . Karena pada saat Mahasiswa login ke KRS Daring nama pengguna dan kata sandi terekam masuk ke *log* SSLStrip di laptop milik peneliti.



***Gambar 2** Hasil SSLStrip pada perangkat Mahasiswa*

Hasil eksploitasi Web KRS Daring yang didapat adalah hak akses dari hasil *Social Engineering* pada target mahasiswa Institusi Pendidikan. Ketika diakses peneliti mendapatkan hak akses berupa mengganti data kendaraan mahasiswa dan mereset kata sandi akun Web KRS Daring

KESIMPULAN

Berdasarkan hasil *security assessment* pada Web KRS Daring milik Institusi Pendidikan XYZ, maka kesimpulan yang diambil yaitu berupa daftar hasil kerentanan keamanan menggunakan kerangka kerja VAPT (*Vulnerability Assessment and Penetration Testing*). Selanjutnya temuan tersebut akan dibuatkan laporan yang ditujukan kepada pihak Institusi Pendidikan.

REFERENSI

[1] Russ Miles, G. Rogers, E. Fuller, and T. Dykstra, *Security Assessment: Case Studies for Implementing the NSA IAM*. United States of America: Syngress, 2004.

[2] 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.

[3] A. M. A. Yuhaz, "Risk Management Aset 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.

[4] 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.

[5] 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.

[6] OWASP (Open Web Application Security Project), "Open Web Application Security Project," 2001. [Online]. Available: www.owasp.org.

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

[8] Nmap, "Nmap," 1997. [Online]. Available: https://nmap.org/man/id/index.html#man-description.

[9] S. Puangpronpitag and N. Masusai, "An Efficient and Feasible Solution to ARP Spoof Problem," *2009 6th Int. Conf. Electr. Eng. Comput. Telecommun. Inf. Technol.*, vol. 02, pp. 910–913, 2009.

[10] R. Wicaksono, "MITM Attack on Mandiri Internet Banking using SSLStrip," 2009. [Online]. Available: http://www.ilmuhacking.com/web-security/mitm-attack-mandiri-internet-banking-using-sslstrip/.

[11] A. Koyun and E. Al Janabi, "Social Engineering Attacks," *J. Multidiscip. Eng. Sci. Technol.*, vol. 4, no. 6, pp. 2458–9403, 2017.