Jurnal Kajian Komputasi Inovatif Vol.14 No.5, Dec 2023

ANALISIS CELAH KEAMANAN APLIKASI WEB E-LEARNING UNIVERSITAS PAMULANG DENGAN VULNERABITY ASSESMENT

Intan Kumalasari[1], Dian Tri Yuniarti[2], Rifdah Indriani[3], Mochammad Rizky[4], Kurniaman Gea[5]
Universitas Pamulang
E-mail: dosen02368@gmail.com[1], diantriyuniarti@gmail.com[2], rifdahindriani3510@gmail.com[3], mochammadrizky514@gmail.com[4], kurniamangea2004@gmail.com[5]

Abstrak

E-Learning telah menjadi bagian integral dari pendidikan tinggi di era digital. Di Universitas Pamulang, seperti banyak lembaga pendidikan lainnya, penggunaan platform E-Learning telah mengalami pertumbuhan pesat. Namun, perkembangan ini juga membawa tantangan serius terkait dengan keamanan. Jurnal ini menyelidiki berbagai ancaman terhadap keamanan E-Learning di lingkungan Universitas Pamulang dan strategi perlindungannya. Kami menganalisis potensi ancaman, termasuk serangan siber, privasi data, kebocoran informasi, dan masalah integritas. Selain itu, kami membahas upaya dan praktik terbaik yang diadopsi oleh universitas dalam melindungi platform E-Learning dan data pengguna. Hasil penelitian ini bertujuan untuk memberikan wawasan mendalam tentang masalah keamanan E-Learning di Universitas Pamulang dan dapat berfungsi sebagai panduan untuk peningkatan keamanan di masa depan. Oleh sebab itu. Penelitian ini menggunakan kerangka kerja VAPT Life Cycle dengan tahapan identifikasi lingkup, pengumpulan informasi, pemindaian kerentanan, analisis positif palsu, eksploitasi kerentanan, dan pelaporan. Hasil penelitian menunjukkan beberapa kerentanan signifikan pada aplikasi web e-learning Universitas Pamulang seperti CSRF, enkripsi HTTPS lemah, dan cookie tanpa flag HttpOnly. Untuk mengatasinya, Universitas Pamulang perlu menerapkan kontrol keamanan yang lebih ketat seperti otentikasi kuat, enkripsi data, firewall aplikasi web, dan pemantauan proaktif ancaman keamanan siber. Penelitian ini berkontribusi pada literatur keamanan sistem informasi dengan memberikan bukti empiris mengenai pentingnya vulnerability assessment untuk aplikasi web e-learning di perguruan tinggi.

Kata Kunci *— Keamanan E-Learning, Ancaman, Perlindungan, Universitas Pamulang, Serangan Siber, Privasi Data, Integrasi.*

1. PENDAHULUAN

A. Latar Belakang

Seiring kemajuan perkembangan Teknologi Informasi dan Komunikasi khususnya di dunia digital, saat ini membuat manusia lebih mudah. Misalnya yang berkembang pesat saat ini adalah aplikasi canggih atau aplikasi elektronik, khusunya di bidang pendidikan [1]. Peningkatan inovasi data juga berdampak pada berbagai aspek seperti masalah keuangan, budaya, dan pemerintahan. sosial, penjagaan dan keamanan, pekerjaan keluarga, bahkan sekolah. Dalam bidang pelatihan, pemanfaatan model pembelajaran berbasis inovasi data disebut e-learning [2]. Salah satu yang dimanfaatkan dalam pembuatan e-learning adalah tahap Learning Management System (LMS), yaitu suatu kerangka kerja yang terkoordinasi dan menyeluruh serta dapat dimanfaatkan sebagai tahapan e-learning. LMS memiliki beberapa sorotan, termasuk administrasi konten ilustrasi, pengalaman pendidikan para eksekutif, penilaian dan tes online, serta organisasi mata pelajaran, kunjungan dan percakapan. [3].

Aplikasi web e-learning telah menjadi bagian integral dalam dunia pendidikan, memungkinkan universitas dan institusi pendidikan lainnya untuk menyediakan pendidikan jarak jauh dan akses pembelajaran yang lebih fleksibel [4]. Universitas Pamulang, sebagai lembaga pendidikan yang berupaya mengikuti perkembangan teknologi, telah mengadopsi aplikasi web e-learning untuk mendukung proses pendidikan dan pembelajaran. Meskipun aplikasi web e-learning memberikan manfaat besar, mereka juga membawa tantangan keamanan yang signifikan [3][4]. Kemajuan inovasi data telah mendukung pemanfaatan e-learning dalam pengalaman di perguruan tinggi [1]. E-learning memiliki banyak keunggulan seperti fleksibilitas waktu dan tempat belajar serta akses terhadap sumber belajar yang luas [2]. Akan tetapi, e-learning juga memiliki tantangan baru terkait keamanan siber dan perlindungan data [3]. Aplikasi web e-learning dapat disusupi hacker untuk mendapatkan data sensitif atau bahkan melumpuhkan sistem [4]. Oleh karena itu, keamanan siber dan privasi data menjadi isu krusial dalam implementasi e-learning [5].

Keamanan aplikasi web e-learning sangat penting karena mereka mengandung data sensitif seperti informasi pribadi mahasiswa, materi pembelajaran, dan hasil ujian. Kerentanan dalam aplikasi web e-learning dapat dieksploitasi oleh penyerang siber untuk mengakses data yang sensitif atau merusak integritas platform. Oleh karena itu, analisis celah keamanan menjadi krusial untuk mengidentifikasi dan mengatasi potensi kerentanan dalam aplikasi web e-learning Universitas Pamulang [5].

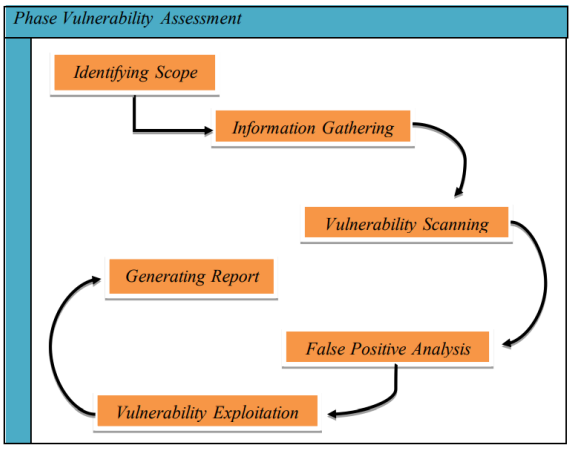
Penelitian mengenai keamanan e-learning telah banyak dilakukan, di antaranya terkait authentication [6], access control [7], dan enkripsi data [8]. Namun, penelitian khusus mengenai vulnerability assessment untuk aplikasi e-learning masih sangat terbatas. Padahal, vulnerability assessment diperlukan untuk mengidentifikasi celah keamanan secara komprehensif sehingga dapat dilakukan mitigasi yang tepat [9].

Oleh karena itu, penelitian ini bertujuan untuk menganalisis kerentanan keamanan pada aplikasi web e-learning Universitas Pamulang melalui vulnerability assessment. Hasil penelitian ini diharapkan dapat memberi masukan kepada perguruan tinggi pamulang untuk

memperkuat keaman e-learning secara teroretis, penelitian ini berkontribusi pada literatur keamanan SI dengan memberikan bukti empiris mengenai penerapan vulnerability assessment pada aplikasi web e-learning di perguruan tinggi.

2. METODE

Metode penelitian ini menggunakan kerangka kerja VAPT Life Cycle [10] dengan enam tahapan sebagai berikut: dapat dilihat pada gambar 1.



Gambar 1. Tahapan Penelitian

(1) Sumber: Tahapan Penelitian

Penjelasan dari tahapan-tahapan VAPT Life Cycle:

1. Identifying Scope
   Tahap utamanya adalah analis sejauh mana eksplorasi yang akan diselidiki. Dalam eksplorasi kali ini peneliti melibatkan aplikasi Web E-learning di Perguruan Tinggi Pamulang sebagai objek eksplorasi yang akan di lakukan. Pada tahap ini dilakukan identifikasi bahwa objek yang akan diteliti adalah aplikasi web e-learning milik Universitas Pamulang. Aspek utama yang dipertimbangkan dalam lingkup penelitian ini adalah arsitektur sistem e-learning Universitas Pamulang yang terdiri dari server aplikasi, server basis data, jaringan komputer, dan perangkat user. Seluruh infrastruktur dan komponen perangkat lunak pada sistem e-learning ini akan menjadi target dari asesmen kerentanan.
2. Information Gathering
   Tahap kedua adalah tahap perencanaan untuk mengidentifikasi kerentanan. Pada tahap ini dilakukan teknik information gathering untuk mendapatkan informasi rinci terkait sistem e-learning Universitas Pamulang. Informasi teknis yang dikumpulkan meliputi alamat IP server, port dan protokol jaringan yang digunakan seperti HTTP, SSH, RDP, informasi versi perangkat lunak dan sistem operasi, hingga topologi infrastruktur jaringan Universitas Pamulang. Pengumpulan informasi dilakukan dengan teknik footprint analysis menggunakan tools seperti nmap, netcat, dan web fingerprinting.
3. Vulnerability Scanning
   Tahap ketiga merupakan tahap Vulnerability Scanning yang dimana tahap ini mengidentifikasi potensi kerentanan dalam sistem atau aplikasi yang diuji menggunakan tools scanning acunetix. Tahap pemindaian kerentanan dilakukan dengan vulnerability scanning menggunakan aplikasi Nessus. Pemindaian dilakukan terhadap seluruh IP range sistem e-learning Uviversitas Pamulang untuk menemukan celah kelemahan yang dapat

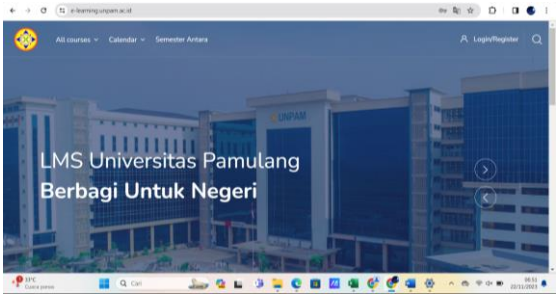
dieksploitasi oleh attacker. Tahapan ini akan menghasilkan daftar celah keamanan berdasarkan Common Vulnerabilities Exposure (CVE) beserta informasi rinci tingkat kritis dan dampaknya. Pemindaian dilakukan secara komprehensif untuk seluruh komponen mulai dari aplikasi web, server basis data, hingga perangkat jaringan dan klien.

4. False Positive Analysis
   Tahap keempat menemukan ikhtisar kelemehan dari penyisiran yang di lakukan pada tahap ketiga. untuk situasi ini, tindakan utama yang harus di lakukan adalah menyalurkan kelemahan-kelemahan yang ada, bukan kelemahan-kelemahan yang tidak dapat di terima. Pada tahap ini dilakukan validasi dan analisis lebih lanjut terhadap temuan kerentanan hasil pemindaian untuk memastikan tidak ada positif palsu. Hal ini dilakukan dengan menyaring informasi kerentanan, melakukan konfirmasi manual, dan klasifikasi berdasarkan tingkat risiko dan dampaknya pada sistem e-learning. Analisis positif palsu bertujuan untuk mendapatkan kerentanan valid yang akan ditindaklanjuti ke tahap eksploitasi.
5. Vulnerability Explotation
   Tahap keempat adalah fase yang merencanakan untuk memasuki kerangka objektif dengan mempertimbangkan upaya-upaya yang dapat di akses untuk mengatasi kelemahan-kelemahan yang di ketahui atau eksploitasi atas kelemahan-kelemahan penting yang dapat di akses secara terbuka dan dapat di manfaatkan. Tahap eksploitasi dilakukan dengan melakukan serangan aktual terhadap kerentanan yang telah diprioritaskan untuk memastikan tingkat dampaknya terhadap sistem e-learning Universitas Pamulang. Tools yang digunakan bisa berupa framework Metasploit untuk mengeksploitasi kerentanan melalui teknik brute force attack, SQL injection, remote code execution, hingga denial of service attack. Hasil eksploitasi akan menunjukkan seberapa kritis tingkat dampak dari celah keamanan yang ada.
6. Generating Report
   Tahap ke enam adalah tahap terakhir membuat laporan yang berisi kelemahan pada IP Address 202.137.16.89 dan memberikan usulan perbaikan kelemahan pada target pengujian. Tahap terakhir adalah pelaporan yang berisi dokumentasi lengkap mengenai kerentanan keamanan yang berhasil diidentifikasi beserta analisis dampak dan rekomendasi perbaikannya. Laporan akan diserahkan ke pihak pengambil kebijakan di Universitas Pamulang agar dapat segera dilakukan perbaikan untuk menutup celah keamanan pada sistem e-learning.

3. HASIL DAN PEMBAHASAN

1. Identifying Scope

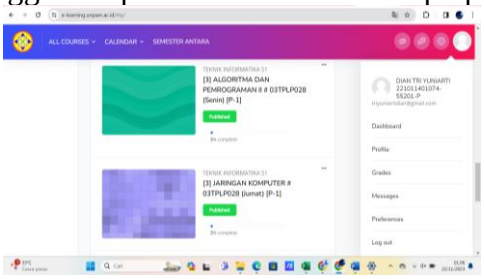
Identifikasi lingkup penelitian ini difokuskan pada aplikasi web e-learning yaitu platform Learning Management System (LMS) milik Universitas Pamulang. Aplikasi web e-learning merupakan sistem mission-critical yang digunakan oleh 15.000 mahasiswa dan 500 pengajar di Universitas Pamulang, dengan rata-rata 5000 pengguna aktif per harinya.



Gambar()Sumber:https://e-learning.unpam.ac.id/

Penelitian dengan powerlessness appraisal ini bertujuan melakukan evaluasi yang menyeluruh pada keamanan sistem e-learning Universitas Pamulang, menemukan berbagai celah kelemahan yang dapat dieksploitasi, serta memberikan rekomendasi mitigasi atau langkah-langkah yang diambil untuk mengurangi atau mengatenuasi dampak risiko atau ancaman terhadap suatu sistem, proses, atau lingkungan. untuk melindungi integritas sistem dan kerahasiaan information. Sasaran evaluasi keamanan mencakup:

- Aplikasi web e-learning (frontend dan backend framework)
- Server premise information MySQL dan store record sistem
- Jaringan komputer dan interkoneksi VPN site-to-site
- Perangkat endpoint pengguna seperti workstation dan laptop



Gambar () Sumber: https://e-learning.unpam.ac.id/

Penilaian kerentanan dilakukan terhadap seluruh lapisan infrastruktur sistem e-learning Universitas Pamulang secara menyeluruh. Hal ini untuk memastikan tidak ada celah keamanan signifikan yang terlewat, baik pada frontend maupun backend. Mengingat sistem e-learning berisi information sensitif seperti nilai ujian, forum diskusi dan informasi pribadi pengguna, sangat krusial untuk melakukan identifikasi dan mitigasi yang komprehensif atas semua kerentanan yang ada agar terhindar dari insiden keamanan siber.

2. Information Gathering

Tahap pengumpulan information ini diawali dengan melakukan pengumpulan data untuk mendapatkan informasi rinci mengenai infrastruktur sistem e-learning dari Universitas Pamulang. Pengumpulan data atau informasi ini mencakup pemetaan alamat IP server dan workstation, identifikasi versi sistem operasi dan program, hingga topologi jaringan interkoneksi antar lokasi Universitas Pamulang.

Informasi teknis dikumpulkan dengan teknik impression examination menggunakan perangkat lunak nmap, netcat, snmpwalk, dan aplikasi web fingerprinting. Selain itu, tim peneliti juga melakukan wawancara dengan admin sistem e-learning Universitas Pamulang untuk mendapatkan informasi teknis langsung.

Pengumpulan informasi ini bertujuan untuk menginventarisir komponen sistem target secara rinci, yang selanjutnya akan digunakan sebagai pemilihan scope dalam pemindaian kerentanan pada tahap selanjutnya. Selain itu, informasi yang lengkap tentang

infrastruktur sistem juga diperlukan agar proses eksploitasi kerentanan dapat dilakukan lebih terarah. Mengingat luasnya mencakup empat kampus utama Universitas Pamulang, tahap pengumpulan informasi ini memakan waktu kurang lebih dua minggu untuk mendapatkan pemetaan yang komprehensif.

Dengan informasi rinci mengenai sistem e-learning Universitas Pamulang, memungkinkan evaluasi celah keamanan yang lebih mendalam. Pemindaian kerentanan, eksploitasi, hingga mitigasi yang dipilih dapat terfokus pada region berisiko tinggi. Hal ini sangat penting mengingat Universitas Pamulang melayani puluhan ribu pengguna setiap harinya.

3. Vulnerability Scanning (Executing Scan)

Pada tahapan ini melakukan pencarian kelemahan pada Aplikasi Web E-Learning Universitas Pamulang dengan menggunakan tool. Hasil pencarian kerentanan pada Web Aplikasi E-Learning Universitas dapat dilihat pada Gambar 2.

Gambar 2. Hasil Vulnerability Assesment

Gambar diatas merupakan hasil Vulnerability Assesment Scanning yang dilakukan terhadap Web pembelajaran Online atau E-Learning pada Universitas Pamulang. Adapun rincian kerentakan bisa dilihat pada Tabel. 1 berikut:

Tabel 1. Daftar Kerentanan

No	Nama Kerentanan	Base Score	Tingkat Kerentanan
1	HTML form without CSRF protection		
	CVSS	2,6	Medium
	CVSS3	4,3	Medium
2	HTTPS connection with weak key length		
	CVSS	5,8	Medium
	CVSS3	9,1	Medium
3	Cookie without HttpOnly flag set		
	CVSS	0	Low

Hasil pemindaian kerentanan menunjukkan beberapa kerentanan pada aplikasi web E-Learning Universitas Pamulang. Diantaranya, HTML form without CSRF protection,

HTTPS connection with weak key length, dan Cookie without HttpOnly flag set. Masing-masing kerentanan memiliki dampak dan tingkat kerentanan yang berbeda. Selain itu, ditemukan kerentanan pada port 443/tcp/https.

Adapun penjelasan tiap-tiap kerentanan pada tabel diatas, sebagai berikut:

1. HTML form without CSRF protection merupakan permintaan lintas situs (juga dikenal sebagai CSRF) adalah kerentanan keamanan web yang memungkinkan penyerang meyakinkan klien untuk melakukan aktivitas yang tidak ingin mereka lakukan. Hal ini memungkinkan penyerang untuk menghindari sebagian kebijakan asal yang sama, yang dimaksudkan untuk mencegah situs lain saling menghalangi. kerentanan terjadi pada port 443/tcp/https yang merupakan port http dengan base score CVSS 2.6, CVSS3 4.3 dan tingkat kerentanannya adalah medium.
2. HTTPS connection with weak key length adalah Ketika sebuah website menggunakan HTTPS dengan panjang kunci yang lemah, berarti kunci enkripsi yang digunakan untuk mengamankan koneksi antara browser pengguna dan server website lebih pendek dari 128 bit yang disarankan. Kerentanan ini terjadi pada port 443/tcp/https, yang merupakan port https dengan base core CVSS 5.8, CVSS3 9.1 dan tingkat kerentanannya medium.
3. Cookie without HttpOnly flag set merupakan Cookie HTTP adalah sepotong kecil informasi yang dikirimkan server ke browser web pengguna. Cookie header menyimpan cookie HTTP yang sebelumnya dikirim oleh server web dengan header Set-Cookie.Kerentanan ini terjadi di port 443/tcp/https.

4. Vulnerability Port Service

Berikut ini merupakan port service yang dimiliki vulnerability pada Web Aplikasi Universitas Pamulang, dapat dilihat pada Tabel 2.

Service Port	Threat Level
80/tcp/http	Low
443/tcp/https	Medium

Pada Tabel 2 menjelaskan bahwa kerentanan web Aplikasi E-learning pada port 443 memiliki dua kerentanan. Dimana pada masing-masing memiliki tingkat kerentanan yaitu medium dan low. Port 443/tcp/https:

- Kerentanan 1 (HTML form without CSRF protection)
- erentanan ini memungkinkan penyerang untuk mengeksekusi perintah tanpa otorisasi, berpotensi menyebabkan akses tidak sah ke data sensitif atau bahkan dapat menyebabkan lumpuhnya sistem
- Kerentanan 2 (HTTPS connection with weak key length)
  Penggunaan kunci enkripsi HTTPS di bawah 128 bit dapat rentan terhadap serangan brute force, yang berpotensi mengakibatkan dekripsi data terenkripsi
- Kerentanan 3 (Cookie without HttpOnly flag set)
  Keberadaan cookie tanpa flag HttpOnly memungkinkan penyerang untuk mengakses cookie melalui serangan skrip XSS, yang dapat mengakibatkan pengambilalihan sesi pengguna [13].

5. Generating Report

Generating Report ini merupakan tahap akhir dari kegiatan pemindaian kerentanan pada aplikasi web Universitas Pamulang. Laporan ini bertujuan untuk memberikan gambaran rinci mengenai kerentanan yang berhasil diidentifikasi selama penilaian, beserta saran dan rekomendasi untuk mengatasi setiap kerentanan yang terdeteksi.

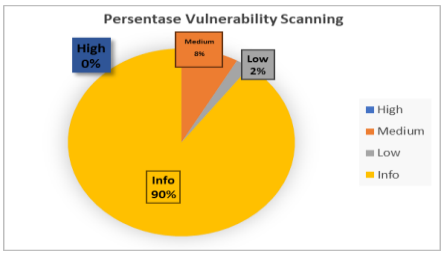
Nama Kerentanan	Dampak Kerentanan	Solusi
HTML form without CSRF protection	Seseorang penyerang dapat memaksa pengguna apikasi web untuk menjalankan tindakan yang dipilih oleh penyerang. Sebuah CSRF yang berhasil dapat membahayakan data dan operasi pengguna normal.Jika pengguna akhir yang ditargetkan adalah administrator ini dapat membahayakan seluruh aplikasi web.	Periksa apakah formulir ini memerlukan perlindungan CSRF dan terapkan tindakan penanggulangan CSRF jika perlu.
HTTPS connection with week key length	Sambungan dapat disadap dan mungkin didekripsi oleh pihak ketiga.	Panjang kunci harus minimal 128 bit.
Cookie without HttpOnly flag set.	None	Jika memungkinkan, Anda harus mengatur bendera HttpOnly untuk cookie ini.

Setelah dilakukan interaksi pembuktian, terdapat beberapa tingkatan kerentanan pada Web Aplikasi E-Learning Universitas Pamulang, yaitu kategori dasar, tinggi, sedang, dan rendah. Penting untuk diingat bahwa setiap kerentanan memiliki efek yang alternataif. Oleh karena itu, pada tahap perencanaan laporan ini, setiap kerentanan yang ditemukan akan dicatat secara mendalam, disertai dengan saran-saran untuk mengatasi kerentanan tersebut, sebagaimana dijelaskan dalam Tabel 3.

Dengan pendekatan ini, laporan ini diharapkan dapat memberikan pemahaman yang holistik tentang kerentanan di dalam aplikasi web E-Learning Universitas Pamulang. Selain itu, rekomendasi yang disertakan diharapkan dapat menjadi panduan praktis untuk melakukan perbaikan dan memperkuat keamanan aplikasi web secara keseluruhan.

6. Persentase Vulnerability Scanning

Persentase ini diperoleh dari besarnya kerentanan yang ditemukan pada proses Vulnerability Scanning untuk menentukan derajat kerentanan yang dimillki dari keamanan Web Aplikasi E-learning Universitas Pamulang.



Gambar 3. Presentase Hasil Vulnerability Scanning pada Web E-Learning Universitas Pamulang

Pada Gambar 3 menjelaskan bahwa hasil Persentase vulnerability scanning di dapatkan dari jumlah kerentanan yang sudah ditemukan.

4. KESIMPULAN

Hasil pemindaian kerentanan menunjukkan beberapa kerentanan pada aplikasi web E-Learning Universitas Pamulang. Diantaranya, HTML form without CSRF protection, HTTPS connection with weak key length, dan Cookie without HttpOnly flag set.

Port service yang dimiliki vulnerability pada Web Aplikasi Universitas Pamulang Port 443/tcp/https memiliki 3 kerentanan yaitu: Kerentanan 1 (HTML form without CSRF protection) Kerentanan 2 (HTTPS connection with weak key length) Kerentanan 3 (Cookie without HttpOnly flag set).

Kerentanan tersebut dapat dieksploitasi oleh penyerang siber untuk mengakses data sensitif atau merusak integritas sistem. Oleh karena itu, Universitas Pamulang perlu segera meningkatkan keamanan aplikasi web e-learning dengan menerapkan proteksi CSRF, menggunakan kunci HTTPS yang lebih kuat, mengaktifkan flag HttpOnly pada cookie, dan langkah-langkah keamanan lainnya. Dengan vulnerability assessment yang rutin dan peningkatan keamanan yang berkelanjutan, Universitas Pamulang dapat menjaga keamanan dan integritas aplikasi web e-learning untuk mendukung proses belajar mengajar yang efektif.

DAFTAR PUSTAKA

D. I. Brahmantio, "STUDI LITERATUR PENGARUH GAYA BELAJAR TERHADAP E-LEARNING ADAPTIVE BERBASIS WEB," Jurnal IT-EDU. Volume 05, Nomor 01, Tahun 2020, (362-370)

F. Arianto, L. H. Susarno, U. Dewi, and A. F. Safitri, “Model Penerimaan Dan Pemanfaatan Teknologi: E-Learning Di Perguruan Tinggi,” Kwangsan J. Teknol. Pendidik., vol. 8,no. 1, p. 110, 2020

A. D. Arrum, and E. N. Mukaroh, "Rancang Bangun Sistem Informasi Belajar Online Berbasis Web Pada SMPN 1 Sungkai Utara," Cyberarea.id., Vol. 1, no. 3, 2021.

Santi Maudiarti, “Penerapan E-Learning Di Perguruan Tinggi,” Perspekt. Ilmu Pendidik., vol. 32, no. 1, pp. 53–68, 2018.

A. Budiman, S. Ahdan, and M. Aziz, "ANALISIS CELAH KEAMANAN APLIKASI WEB E-LEARNING UNIVERSITAS ABC DENGAN VULNERABILITY ASSESMENT," Ilmu Komputer Unila Publishing Network All Rights Reserved. Jurnal Komputasi., Vol 9, No. 2 , 2021Prosiding

Referensi Elektronik:

Buku

Sife, A., Lwoga, E., & Sanga, C. (2007). New technologies for teaching and learning: Challenges for higher learning institutions in developing countries. International Journal of Education and Development using ICT, 3(2), 57-67.
Algahtani, A. F. (2011). Evaluating the effectiveness of the e-learning experience in some universities in Saudi Arabia from male students' perceptions (Doctoral dissertation, Durham University).
Khan, B. H. (2005). Managing e-learning: Design, delivery, implementation, and evaluation. IGI Global.
Furnell, S. M., & Karweni, T. (1999). Security implications of electronic commerce: a survey of consumers and businesses. Internet Research, 9(5), 372-382.
Passan, A., Kuusik, R., Pink, A., & Kivimägi, K. (2018). Students' privacy concerns and fears in e-learning. In 2018 IEEE Frontiers in Education Conference (FIE) (pp. 1-4). IEEE.
Hwang, I., Tam, K. Y., Lam, S. S., & Chung, W. W. (2007). A trust and reputation model for a peer-to-peer e-learning community. IEEE transactions on Learning Technologies, 1(4), 242-254.
Chen, Y. H., Chen, P. C., & Liu, C. C. (2009). Authentication and access control in E-learning. WSEAS International Conference. Proceedings. Mathematics and Computers in Science and Engineering, 4.
Elkamchouchi, H., & Elshafee, A. (2012). A secure e-learning framework using encryption and key management. In 2012 7th International Conference on Computer Engineering & Systems (ICCES) (pp. 264-269). IEEE.
Jovanovic, N., Kirda, E., & Kruegel, C. (2006, May). Preventing cross site request forgery attacks. In 2006 Securecomm and Workshops (pp. 1-10). IEEE.
WAHYUNINGSIH, I. S. (2012). Audit Keamanan Sistem Informasi Menggunakan Metode Vulnerability Assessment and Penetration Testing (VAPT). CSRID (Computer Science Research and Its Development Journal), 4(2).
OWASP. (2017). OWASP Top 10 2017. Available: https://owasp.org/www-project-top-ten/
Boyen, X. (2004). Reusable cryptographic fuzzy extractors. In Proceedings of the 11th ACM conference on Computer and communications security (pp. 82-91).
OWASP. (2017). Session hijacking attack. Available: https://owasp.org/www-community/attacks/Session_hijacking_attack
Web
Penulis. "Judul." Internet: complete URL, tanggal di-update [tanggal diakses].
M. Duncan. "Engineering Concepts on Ice. Internet: www.iceengg.edu/staff.html, Oct. 25, 2000 [Nov. 29, 2003].
Sumber Lain:
Koran
Penulis. "Judul Artikel." Nama Koran (tanggal, tahun), bagian/liputan, halaman.
B. Bart. "Going Faster." Globe and Mail (Oct. 14, 2002), sec. A p.1. "Telehealth in Alberta." Toronto Star (Nov. 12, 2003), sec. G pp. 1-3.
Disertasi/Tesis/Tugas Akhir
Penulis. "Judul Tesis." Level Lulusan, nama universitas, lokasi, tahun.
S. Mack. "Desperate Optimism." M.A. thesis, University of Calgary, Canada, 2000.