ANALISIS KEAMANAN E-LEARNING MENGGUNAKAN OPEN WEB APPLICATION SECURITY PROJECT (OWASP) (STUDI KASUS: MOCA UNIMMA)

N Bagas Adinugroho[1], P Hendradi[2*], D Sasongko[3]

[1,2,3]Universitas Muhammadiyah Magelang

p_hendra@ummgl.ac.id[2]

ABSTRACT

Like other Higher Education Systems, e-learning at the University of Muhammadiyah Magelang (UNIMMA) known as My Online Class (MOCA) based on the Moodle Learning Management System (LMS) has become a learning tool in the pandemic era and continues to this day. Thus, the MOCA system stores important data from learning activities. So, the next challenge is the data security system. For this reason, in this study a security analysis was carried out which aims to provide an overview and recommendations for its development. In conducting security analysis, the Open Web Application Security Project (OWASP) and Red Hawk and OWASP Zap tools are used. The results obtained information about 13 vulnerabilities for MOCA and 2 of them are high-level vulnerabilities, namely Cross Site Scripting and SQL Injection vulnerabilities. For this reason, this study also provides recommendations for these 2 vulnerabilities

Keywords—*E-learning System, OWASP, Red hawk*

ABSTRAK

Seperti Pendidikan Tinggi lainnya sistem e-learning Universitas Muhammadiyah Magelang (UNIMMA) yang dikenal dengan *My Online Class* (MOCA) berbasis *Learning Management System* (LMS) Moodle menjadi sarana belajar saat pandemi dan berlanjut sampai saat ini. Konsekuensinya pada MOCA tersimpan data penting dari kegiatan pembelajaran. Sehinga tantangan berikutnya adalah sistem keamanan data. Untuk itulah dalam penelitian ini dilakukan analisa keamanan yang bertujuan untuk memberikan gambaran serta rekomendasi pengembangannya. Dalam melakukan analisa keamanan digunakan metode *Open Web Application Security Project* (OWASP) dan *Tool Red Hawk* dan OWASP Zap. Hasilnya diperoleh informasi 13 kerentanan atas MOCA dan 2 diantaranya berlevel high, yaitu kerentanan *Cross Site Scripting* dan *SQL Injection*. Dalam penelitian ini disajikan juga rekomendasi untuk 2 kerentanan tersebut.

Kata Kunci— *E-learning System, OWASP, Red hawk*

I. PENDAHULUAN

Seiring dengan perkembangan Teknologi Informasi yang merupakan salah satu pedukung utama pada era pendidikan 4.0 [1]. Hal ini dikarenakan Pendidikan 4.0 membutuhkan kemitraan

yang kuat antara industri dan lingkungan akademik dalam menciptakan sumber daya manusia [2]. Perkembangan teknologi informasi juga mempengaruhi beberapa aspek seperti aspek ekonomi, budaya, politik. sosial, pertahanan keamanan, pekerjaan rumah tangga bahkan dunia pendidikan sekalipun. Dalam pendidikan penerapan model pembelajaran yang berbasiskan teknologi informasi disebut e-learning [3][4].

Selain itu E-learning merupakan metode pembelajaran menggunakan media elektronik (audio-visual) dengan teknologi internet [5] yang proses kegiatan pembelajarannya dapat berlangsung dengan jarak jauh tanpa harus bertatap muka di dalam ruang kelas pendukung untuk menghadapi revolusi industri 4.0 [6]. Salah satu yang digunakan dalam pembuatan e-learning yaitu *platform* Learning Management System (LMS) Yang merupakan sebuah sistem yang terintegrasi dan komprehensif serta dapat digunakan sebagai platform e-learning. LMS memiliki beberapa fitur antara lain, yaitu manajemen isi pelajaran, manajemen proses pembelajaran, evaluasi dan ujian yang dilakukan secara *online*, serta administrasi mata pelajaran, *chatting*, dan diskusi [5].

Universitas Muhammadiyah Magelang (UNIMMA) menamai sistem e-learning nya dengan *MyOnline Class* (MOCA) yang bebasis LMS Moodle berperan sebagai sarana belajar yang utama saat pandemi covid-19 dan saat ini masih digunakan karena terbukti efektif untuk mengelola data perkuliahan. Tantangan selanjutnya adalah sistem keamanannya. Penelitian ini mengarah pada pengembangan sistem keamanan dari e-learning yang bertujuan untuk meningkatkan layanan sistem e-learning sebagai sistem pembelajaran dengan memanfaatkan *Open Web Application Security Project* (OWASP). Yaitu *framework* untuk mencari celah kelemahan dari sebuah website [7]. Informasi kerentanan yang dihasilkan akan menjadi bagian dari diskusi dan pembahasan mengacu pada tinjauan literatur yang akan menghasilkan usulan desain sistem keamanan e-learning.

II. METODE PENELITIAN

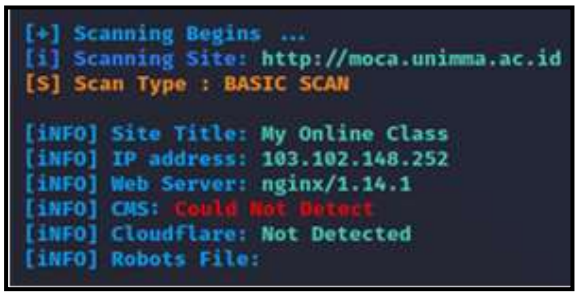
Dalam penulisan penelitian ini dilakukan dengan tahapan-tahapan yang akan mengarahkan langkah-langkah penelitian agar sesuai dengan perumusan masalah dan tujuan penelitian. Berikut ini adalah Langkah-langkahnya

a. Analisa Objek

Tahapan ini peneliti akan menentukan objek yang akan dianalisa keamanannya yaitu MOCA, dalam tahapan ini akan

dijelaskan lebih detail profil dari MOCA, baik profil pengelola dan juga profil teknis seperti aktivitas, aplikasi dan infrastruktur.

Dalam melakukan analisis objek dilakukan tahapan untuk menggali informasi (*Information Gathering*) yaitu proses evaluasi keamanan berdasarkan informasi yang tersedia untuk umum di internet yaitu alamat IP, pendaftar domain, server DNS, status server, sistem operasi yang digunakan, dan port terbuka [8]. *Tools* yang digunakan yaitu RedHawk.



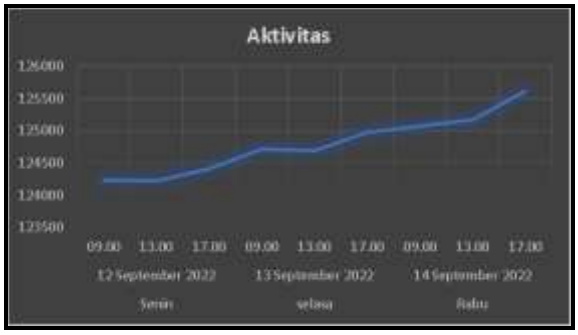
Gambar 1. Hasil scanning REDHAWK

Dari gambar 1 *scaning* menggunakan RedHawk diperoleh informasi *website title*, *ip address* dan *web server*. Ketiga informasi tersebut digunakan dalam langkah pengujian kerentanan.

Selanjutnya untuk mengetahui tingkat pengguna MOCA dapat diperoleh dari bagian kanan bawah, seperti gambar 2 ;

Gambar 2. Tampilan MOCA

Berikutnya untuk mengetahui tingkat aktivitas penggunaan MOCA peneliti melakukan pengecekan dengan pembagian waktu, yaitu pagi jam 09.00, siang jam 13.00, dan sore jam 17.00. Untuk hari yaitu senin, selasa, dan rabu. Berikut ini hasil dalam bentuk grafik aktifitas MOCA;



Gambar 3. Grafik aktivitas MOCA

b. Studi Literature

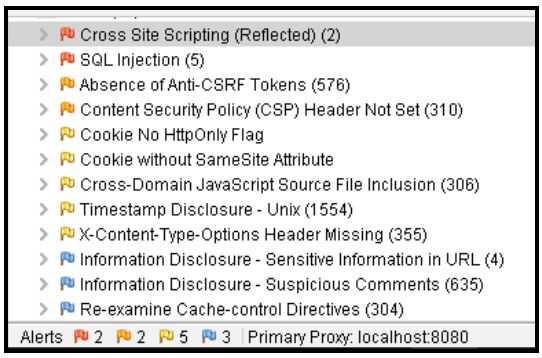
Tahapan ini peneliti akan melakukan literature review pada jurnal yang memiliki rentang waktu 5 tahun, dan memiliki tema yaitu security, e-learning, OWASP, Pontensi Serangan pada system, dan System Informasi. Untuk itu tahapan ini dilakukan dengan memasukan kata kunci ke dalam pencarian google scholar

(http://scholar.google). Pemilihan literatur selain rentang tahun, juga mempertimbangkan kualitas penerbit, yaitu minimal terindeks sinta 4.

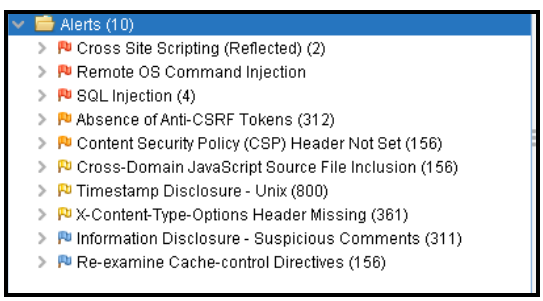
c. Uji kerentanan.

Pada tahapan ini peneliti dapat melakukan pengujian terhadap pontensi serangan yang terdapat pada *system.* Metode yang akan digunakan adalah *Open Web Application Security Project* (*OWASP*).

Dalam melakukan uji kerentanan peneliti menggunakan *tools scanning* yaitu *OWASP Zap* yang digunakan untuk mengetahui celah keamanan pada suatu website [9]. Pengujian dilakukan berdasarkan pembagian waktu, berikut hasil *scanning*;



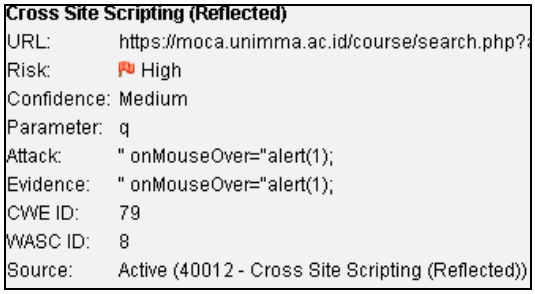
Gambar 4. Hasil *Scanning* Pagi



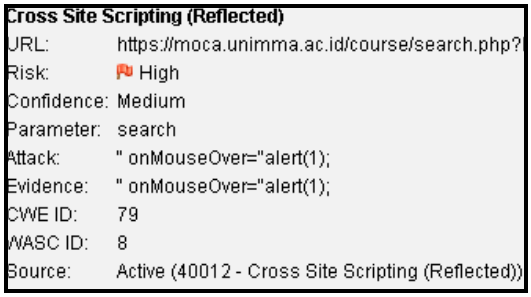
Gambar 5. Hasil *Scanning* Siang

Gambar 6. Hasil scanning sore

Dari gambar 4, 5 dan 6 untuk hasil kerentanan dengan jumlah terbanyak terdapat pada sore hari dengan masing-masing memiliki 13 kerentanan dengan 2 *level high*, 3 dengan *medium*, 5 dengan *level Low*, dan 3 dengan level *informational*. Selanjutnya dari beberapa kerentanan tersebut yang harus diperhatikan yaitu serangan *Cross Site Scripting* (XSS) dan SQL *Injection*, dikarenakan memiliki *level high*. Berikut detail kerentanan ;



Gambar 7. Detail Serangan XSS

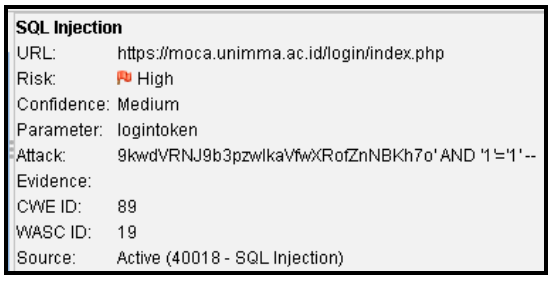


Gambar 8. Detail Serangan XSS 2

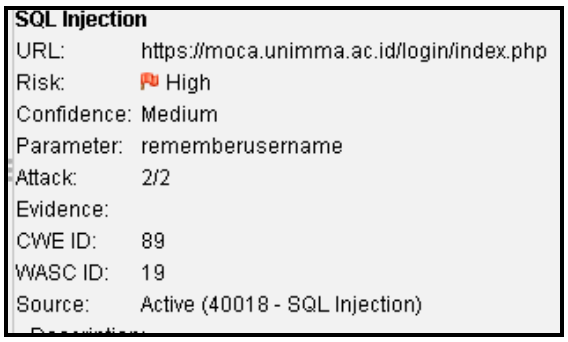
Serangan *Cross Site Scripting* adalah serangan berbahaya yang menyerang suatu website dengan memasukkan kode berbahaya berupa javascript melalui from input yang bertujuan untuk mengambil file yang digunakan untuk masuk ke *website* secara *illegal* [10]. Sedangkan untuk serangan SQL Injection merupakan teknik serangan yang bertujuan untuk mengetahui informasi database yang digunakan pada *system* [11].

Untuk serangan *Cross Site Scripting* pada kasus ini terdapat pada fitur pencarian pada MOCA. Serangan terjadi ketika melakukan input ke fitur pencarian yang kemudian inputan tersebut dibaca dalam bentuk *query string* html. Pada *query string* yang di *input* pencarian dapat dimodifikasi di dalam *query string* tersebut. Hal ini dapat menimbulkan ancaman kerentanan pada website karena *Hacker* dapat melihat *cookie* mereka sendiri dan dapat melakukan modifikasi di halaman dibuka mereka sendiri dengan menambahkan kode *javascript* [12].

Serangan SQL *Injection* dilakukan melaui halaman *login.* Penyerang melakukan penyisipan secara langsung ke dalam baris *parameter* yang digabungkan dengan baris perintah SQL dan dieksekusi [13].



Gambar 9. Detail Serangan SQL Injection



Gambar 10. Detail Serangan SQL Injection 2

d. Solusi Perbaikan

Pada tahapan ini peneliti akan memberikan solusi pada teknisi mengacu pada uji kerentanan dan berdasarkan literatur. Uraian dari solusi perbaikan menjadi bagian dari hasil dan pembahasan.

III. HASIL DAN PEMBAHASAN

Pertimbangan setelah dilakukan studi literature dan pengujian kerentanan dapat ditemukan beberapa solusi untuk mencegah serangan pada website tersebut. Berikut solusi pencegahan serangan pada website:

1. Cross Site Scripting

Dilakukan pengembangan pada website dengan menggunakan beberapa bentuk *Security Development Lifecycle* (SDL).

Tujuannya untuk mengurangi jumlah kesalahan *coding* dalam aplikasi yang terdeksi maupun tidak terdeteksi [12].

2. SQL Injection

Dengan memfilter kata dan karakter yang masuk karena selalu ada celah
untuk menyerang selama ada inputan – inputan dari user[13].

Memberikan pesan error dengan cara menonaktifkan atau merubah agar dapat mencegah penyerang untuk menelusuri alur database[14].

Melakukan penambahan fungsi mysql *real escape string* pada *website* agar dapat dilakukan pembersihan *queri* dengan menyeleksi karakter yang tidak dianggap sebagai bagian dari queri [13].

IV. KESIMPULAN

Bedasarkan hasil Analisa menggunakan OWASP ZAP menunjukkan bahwa system informasi MOCA memiliki 13 kerentanan dan memiliki 2 kerentanan dengan level high yaitu Cross Site Scripting dan SQL *Injection*, sehingga perlu dilakukan perbaikan lebih lanjut oleh pihak pengembang system informasi MOCA dengan mengikuti solusi perbaikan dari penulis.

V. PENELITIAN LANJUTAN

Bedasarkan kesimpulan sangat diperlukan untuk melakukan penelitian dengan menggunakan metode ISSAF *(Information System Security Assasment Framwork*) agar dapat mengetahui kerentanan dari sisi *web server*.

DAFTAR PUSTAKA

[1] A. Alwiyah and S. Sayyida, "Penerapan E-Learning untuk Meningkatkan Inovasi Creativepreneur Mahasiswa," *ADI Bisnis Digit. Interdisiplin J.*, vol. 1, no. 1, pp. 35–40, 2020.

[2] P. Hendradi, "Artificial Intelligence Influence in Education 4.0 To Architecture Cloud Based E-Learning System," *Int. J. Artif. Intell. Res.*, vol. 4, no. 1, pp. 30–38, 2020.

[3] Santi Maudiarti, "Penerapan E-Learning Di Perguruan Tinggi," *Perspekt. Ilmu Pendidik.*, vol. 32, no. 1, pp. 53–68, 2018.

[4] 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.

[5] N. A. Larasati and S. Andayani, "Pengaruh Penggunaan Learning Management System (LMS) Terhadap Tingkat Kepuasan

Mahasiswa Menggunakan Metode DeLone and McLean," *J. Tek. Inform. UNIKA St. Thomas*, vol. 4, no. 1, pp. 13–20, 2019.

[6] H. Dhika, F. Destiawati, S. Surajiyo, and M. Jaya, "Implementasi Learning Management System Dalam Media Pembelajaran Menggunakan Moodle," *Pros. Semin. Nas. Ris. Inf. Sci.*, vol. 2, no. 0, pp. 228–234, 2020.

[7] G. Guntoro, L. Costaner, and M. Musfawati, "Analisis Keamanan Web Server Open Journal System (Ojs) Menggunakan Metode Issaf Dan Owasp (Studi Kasus Ojs Universitas Lancang Kuning)," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 5, no. 1, p. 45, 2020.

[8] C. B. Setiawan, D. Hariyadi, A. Sholeh, and A. Wisnuaji, "Pengembangan Aplikasi Information Gathering Berbasis HybridApps," *J. INTEK*, vol. 5, no. 1, 2022.

[9] D. Hariyadi and F. E. Nastiti, "Analisis Keamanan Sistem Informasi Menggunakan Sudomy dan OWASP ZAP di Universitas Duta Bangsa Surakarta," *J. Komtika (Komputasi dan Inform.*, vol. 5, no. 1, pp. 35–42, 2021.

[10] D. Demhi, O. E. S. Liando, and J. R. Batmetan, "Cross-site Scripting Reflected as A Risk High-Level Attack on University Website," *Int. J. Inf. Technol. Educ.*, vol. 1, no. 3, pp. 103–111, 2022.

[11] Aufan Imron Rosadi, "Analisis Keamanan Sistem Informasi Akademik dengan Web Penetration Testing," 2018.

[12] S. Suroto and A. Asman, "Ancaman Terhadap Keamanan Informasi Oleh Serangan Cross-Site Scripting (Xss) Dan Metode Pencegahannya," *Zo. Komput.*, vol. 11, no. 1, pp. 11–19, 2021.

[13] H. Aliyasa Almaj Duddin and A. Senja Fitrani, "Pengamanan Proses Input Output Pada Web Untuk Meminimalisir Serangan SQL-Injection dan XSS Menggunakan Metode IDS dan IPS," *Network, Comput. Sci.* |, vol. 4, no. 1, pp. 6–12, 2021.

[14] M. S. Fathurrahman, Yupi Kuspandi Putra, "Jurnal Informatika dan Teknologi," *Teknol. infotek J. Inform. dan Teknol.*, vol. 3, no. 9, pp. 1689–1699, 2020.