TELCOMATICS, Vol.7 No.2, December 2022, pp. 53-60
e-ISSN: 2541-5867
DOI: 10.37253/telcomatics.v7i2.7357

Pengujian Keamanan *Learning Management System* TutorLMS terhadap Kerentanan *Insecure Design* dan *Broken Access Control*

Stefanus Eko Prasetyo*, Nafisatul Hasanah, Gautama Wijaya
Program Sarjana Teknologi Informasi, Fakultas Ilmu Komputer, Universtas Internasional Batam, Jl. Gajah Mada, Baloi Sei Ladi, Batam
*e-mail: *stefanus@uib.ac.id*

Abstrak

Menjual kursus digital merupakan ide kreatif yang dapat dilakukan dimasa pandemi COVID-19. Melalui video yang interaktif maka peluang untuk mendapatkan penghasilan lebih besar. Untuk menjual kursus digital seseorang atau perusahaan memerlukan sebuah sistem informasi yang dapat mengelolah administrasi, pendaftaran keanggotaan, pembayaran dan manajemen isi pembelajaran. Learning Management System (LMS) terintegrasi dapat digunakan untuk menjual kursus digital. Salah satu LMS yang dapat digunakan adalah TutorLMS, saat ini TutorLMS sudah digunakan lebih dari 60.000 pengguna. Pengujian Insecure Design dan Broken Access Control digunakan untuk mengetahui seberapa aman penggunaan TutorLMS dalam menjual kursus online. Dengan pengujian ini diharapkan penjual bisa berjualan kursus online dengan aman. Pengujian dilakukan menggunakan metode action research dimana langsung melakukan pengujian pada objek, disini penulis menggunakan demo website TutorLMS untuk melakukan pengujian. Dari hasil pengujian kursus online berbayar dapat diakses dengan mudah oleh pengunjung yang tidak melakukan pembelian bahkan pendaftaran. Desain REST API yang ada pada dokumentasi, tidak memerlukan autentikasi untuk membaca isi dari kursus online, menyebabkan pengunjung dapat dengan mudah untuk mengambil isi pembelajaran, video dan lainnya. Pengunjung juga dapat mendapatkan pertanyaan quiz dan jawaban, serta mendapatkan informasi author pembuat kursus.
Kata Kunci*: Learning Management System, Insecure Design, Broken Access Control, REST API, TutorLMS*

Abstract

Selling digital courses is a creative idea that can be done during the COVID-19 pandemic. Through interactive videos, the opportunity to earn greater income. To sell digital courses, a person or company needs an information system that can manage administration, membership registration, payment and learning content management. An integrated Learning Management System (LMS) can be used to sell digital courses. One of the LMS that can be used is TutorLMS, currently TutorLMS has been used by more than 60,000 users. The Insecure Design and Broken Access Control tests are used to find out how safe it is to use TutorLMS in selling online courses. With this test, it is hoped that sellers can sell online courses safely. Testing is carried out using the action research method which directly tests the object, here the author uses the TutorLMS demo website to do the testing. From the test results, paid online courses can be accessed easily by visitors who do not make purchases or even register. The REST API design in the documentation does not require authentication to read the contents of online courses, so that visitors can easily retrieve learning content, videos and more. Visitors can also get quiz questions and answers, as well as get information on the author of the course.

Keywords*: Learning Management System, Insecure Design, Broken Access Control, REST API, TutorLMS*

I. PENDAHULUAN

Pandemi Covid-19 membuat pemerintah mengeluarkan aturan pembatasan kegiatan masyarakat, melakukan jaga jarak dikeramaian dan berkegiatan segalanya dari rumah [1]. Dengan adanya waktu luang dirumah menyebabkan munculnya ide kreatif berbasis multimedia dan teknologi [2]. Menjual kursus digital merupakan salah satu ide kreatif yang bisa dilakukan. Melalui multimedia yang

TELCOMATICS, Vol.7 No. 2, December 2022, pp. 53-60
e-ISSN: 2541-5867
DOI: 10.37253/telcomatics.v7i2.7357

interaktif maka peluang untuk mendapatkan penghasilan lebih besar [3].

Untuk menjual kursus digital seseorang atau perusahaan memerlukan sebuah sistem informasi yang dapat mengelolah administrasi, pendaftaran keanggotaan, pembayaran dan manajemen isi pembelajaran. Learning Management System (LMS) dapat digunakan untuk memenuhi kebutuhan sistem penjualan kursus digital. Salah satu LMS yang banyak digunakan adalah TutorLMS, saat ini TutorLMS sudah digunakan lebih dari 60.000 pengguna [4].

TutorLMS adalah plugin WordPress gratis yang memiliki fitur LMS lengkap untuk membuat dan menjual kursus online dengan mudah. TutorLMS dilengkapi dengan fitur drag and drop yang mempermudah dalam pembuatan situs penjualan kursus online dengan mudah tanpa mengetahui bahasa program. Ini adalah salah satu penyebab kenapa TutorLMS banyak digunakan untuk menjual kursus online [5].

Berdasarkan latar belakang tersebut, penelitian ini akan melakukan pengujian kerentanan Insecure Design dan Broken Access Control terhadap TutorLMS. Insecure Design dan Broken Access Control merupakan kategori kerentanan yang dikeluarkan oleh Open Web Application Security Project (OWASP). OWASP adalah yayasan nirlaba yang bekerja untuk meningkatkan keamanan perangkat lunak [6].

Insecure Design diartikan sebagai desain kontrol yang tidak efektif. Salah satu faktor yang berkontribusi terhadap Insecure Design adalah kurangnya profil risiko bisnis yang melekat pada perangkat lunak atau sistem yang sedang dikembangkan, dan dengan demikian kegagalan untuk menentukan tingkat desain keamanan apa yang diperlukan.

Kontrol akses memberlakukan kebijakan sedemikian rupa sehingga pengguna tidak dapat bertindak di luar izin yang diberikan. Kegagalan biasanya mengarah pada pengungkapan informasi yang tidak sah, modifikasi, atau penghancuran semua data atau menjalankan fungsi bisnis di luar batas pengguna [7]. Kelemahan dalam kontrol akses terjadi karena kurangnya pengujian fungsional oleh pengembang aplikasi. [8].

Pengujian Insecure Design dan Broken Access Control digunakan untuk mengetahui seberapa aman penggunaan TutorLMS dalam menjual kursus online. Dengan pengujian ini diharapkan penjual bisa berjualan kursus online dengan aman dan pengguna hanya bisa mengakses kursus yang dibeli.

II. TINJAUAN PUSTAKA

Penelitian terkait keamanan Sistem Informasi dan LMS telah dilakukan oleh beberapa peneliti, diantaranya Studi Pustaka Tentang Kerentanan Keamanan E-Learning dan Penanganannya [9]. Penelitian ini merupakan jenis penelitian kajian pustaka yang dikaji dari sumber terpercaya. penelitian ini diawali dari minimnya literatur yang merangkum tentang penanganan dari berbagai jenis serangan yang terjadi pada sistem E-learning. Kemudian peneliti melakukan review yang fokus pada serangan E-Learning kemudian melakukan taksonomi penanganan E-learning yang terindikasi mendapatkan serangan dari peretas. Hasil dari penelitian ini menyimpulkan bahwa beberapa sisi pada sistem e-learning sering mengalami kerentanan keamanan, diantaranya adalah berhubungan dengan sisi privasi user atau bocornya privasi individu. Selanjutnya yaitu kerentanan integritas data pada konten, dan yang terakhir kerentanan pada sisi aplikasi website karena umumnya sistem e-learning merupakan aplikasi berbasis website.

Pengujian Kerentanan Website Wordpress Dengan Menggunakan Penetration Testing Untuk Menghasilkan Website Yang Aman [10]. Penelitian ini menggunakan metode defense in depth untuk meningkatkan sebuah sistem web yang tidak aman menjadi lebih aman. Pada tahapan pengujian serangan menggunakan penetration testing peneliti memastikan wordpress 5.6.7 yang digunakan terdapat kerentanan admin page yang bisa di akses public, percobaan login yang tidak terbatas, dan versi aplikasi tidak terupdate. Dengan pemanfaatan Defense in depth, peneliti menyarankan untuk membatasi akses login page hanya bisa dilakukan menggunakan VPN, membatasi login dengan menggunakan multi faktor otentikasi dan kode captcha dan, melakukan update versi secara berkala.

Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating [11]. Penelitian ini menggunakan metode penelitian tindakan menggunakan penilaian risiko OWASP.

e-ISSN: 2541-5867
DOI: 10.37253/telcomatics.v7i2.7357

Penilaian risiko digunakan untuk memutuskan tindakan apa yang harus dilakukan terhadap risiko tersebut. Peneliti mendeteksi kerentanan menggunakan aplikasi Acunetix dimana aplikasi website yang akan diuji membandingkan penggunaan PHP Native dan Framework CodeIgniter. Hasil dari penelitian menunjukkan bahwa platform aplikasi web yang menggunakan PHP Native dan CodeIgniter memiliki tingkat kerentanan likelihood dilevel medium, dan tingkat kerentanan impact berada dilevel low. Degnan melihat hasil akhir secara keseluruhan tidak ada jaminan aplikasi web yang dibuat menggunakan PHP Native ataupun CodeIgniter terhindar dari celah keamanan.

Pengujian Kerentanan Dan Penetrasi Keamanan Pada Aplikasi Web Manajemen Skripsi Prodi XYZ [12]. Penelitian ini mengevaluasi kerentanan aplikasi web Thesis Management yang dibuat menggunakan laravel, menggunakan aplikasi scanner burp suite yang tersedia untuk menilai dan mengevaluasi keamanan aplikasi web. Peneliti menggunakan Automation Scan dan Manual Scan. Proses ini menilai kerentanan yang ditemukan saat pengujian apakah dapat dieksploitasi. Hasil dari penelitian ini mendapatkan beberapa kerentanan yang diklasifikasikan dari rendah hingga tinggi.

Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi [8]. Penelitian ini melakukan pengujian ketentanan terhadap aplikasi web Absensi menggunakan metode OWASP Top 10 2017 dilakukan dengan pendekatan box testing. Terdapat 10 parameter yang di uji yaitu Cross-Site scripting, Injection, Broken Access Control, Broken Authentication, Sensitive Data Exposure, Using Components with Known Vulnerabilities, XML External Entities, insecure Deserialization, dan Insufficient Logging and Monitoring. Pengujian menggunakan aplikasi Netsparker, menunjukkan bahwa aplikasi memiliki kerentanan Using Component with Known Vulnerabilities, Security Misconfiguration, dan Sensitive Data Exposure, rekomendasi dari hasil penelitian diharapkan dapat membantu developer memperbaiki dan menutup celah kerentanan.

Penetration Testing Untuk Deteksi Vulnerability Sistem Informasi Kampus [13]. Penelitian ini dilakukan menggunakan metode sistematik agar hasil yang diinginkan tidak menyimpang dan tujuan yang diharapkan bisa terlaksana dengan baik, dan benar. Dalam mendeteksi kerentanan, peneliti menggunakan software Acunetix untuk mengetahui celah keamanan yang ada. Objek serangan adalah website informasi kampus. Pengembangan website pada sistem inforamasi kampus dikembangkan menggunakan menggunakan PHP dan Wordpress. Pada pengujian ini di temukan beberapa celah kelemahan atau kerentanan pada sistem informasi kampus yang dapat digunakan oleh orang yang tidak bertanggung jawab untuk memanipulasi file lokal, mengganggu kenerja dari server itu sendiri dengan teknik Denial of Servoce , melakukan clickjacking serta melakukan Cross-site request forgery.

Sistem Keamanan Database Berbasis Restfull Pada Content Management System Wordpress (Studi Kasus: STIKI Malang) [14]. Penelitian ini melakukan percobaan pentest dengan berbagai teknik serangan yang akan difokuskan ke salah satu target yaitu database dan pengujian akan dilakukan secara otomatis. Hasil yang diharapkan dari penelitian ini adalah Wordpress dapat diambil alih oleh pihak peretas. Berdasarkan hasil penelitian yang berupa pengembangan keamanan sistem database berbasis restfull pada wordpress content management system, dapat diambil sebuah kesimpulan yaitu sistem keamanan tambahan dapat menetralisir pembacaan konfigurasi pada file konfigurasi wordpress, sehingga attacker tidak mudah untuk melakukan pengambil alihan database.

Analisis Kemanan Website Menggunakan Metode Penetration Testing [15]. Penelitian ini menggunakan metode Zero Entry Hacking pada website Pengadilan Tinggi Bengkulu. Metode ini merupakan suatu metodologi yang digunakan dalam penetration testing yang terdiri dari pengumpulan informasi dan pengintaian sistem, yang bertujuan untuk mencari informasi dari website yang tersedia di internet. Kemudian scanning kerentanan yaitu tahap peneliti menggunakan berbagai macam tools dan mencoba berusaha mencari kerentanan yang terdapat pada website. Berikutnya melakukan eksploitasi kelemahan dan kerentanan, merupakan tahapan dimana peneliti menguji kerentanan yang didapatkan

TELCOMATICS, Vol.7 No. 2, December 2022, pp. 53-60
e-ISSN: 2541-5867
DOI: 10.37253/telcomatics.v7i2.7357

pada tahapan sebelumnya. Tahapan Terakhir yaitu paska eksploitasi, merupakan tahap melaporkan hasil pengujian yang telah dilakukan dan memberikan rekomendasi untuk mengatasi kerentanan yang ditemukan. Hasil dari penelitian ini adalah kerentanan pada website Pengadilan Tinggi Bengkulu dapat diketahui dengan meggunakan metode Zero Entry Hacking yang menggunakan 4 tahap dalam pengujiannya.

Learning Management System (LMS) adalah sebuah sistem informasi atau aplikasi yang komprehensif dan saling terintegrasi serta dapat dimanfaatkan sebagai platform penjualan kursus digital. LMS memiliki beberapa fungsi, di antaranya manajemen isi pelajaran apakah video, text maupun dokumen, proses pembelajaran, evaluasi, quiz dan ujian yang dilakukan secara online. Berdasarkan hal tersebut maka penggunaan LMS untuk kursus digital harus memiliki proses manajemen isi mata pelajaran dan manajemen aktivitas pembelajaran. Kedua hal ini harus disiapkan berdasarkan persyaratan dan kebutuhan pengguna [16].

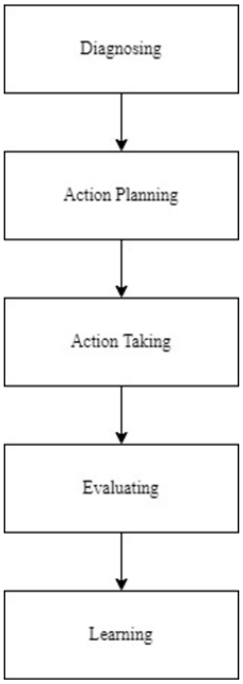
Insecure Design merupakan kategori baru pada OWASP Top 10 tahun 2021-2022 yang berfokus pada risiko terkait dengan cacat desain dan arsitektur, pola desain yang aman, dan referensi arsitektur. Perangkat lunak yang aman memerlukan siklus hidup pengembangan yang aman, beberapa bentuk pola desain yang aman, metodologi paved road, komponen yang aman, dan pemodelan ancaman [17].

Broken Access Control merupakan kategori kerentanan yang Naik dari peringkat kelima tahun 2017 menjadi posisi pertama tahun 2021. Access Control memberlakukan kebijakan supaya pengguna tidak dapat bertindak di luar izin yang diberikan. Pelanggaran prinsip izin ini adalah dimana akses yang benar hanya boleh diberikan untuk peran, akses pengguna tertentu, tetapi tersedia untuk siapa saja [18].

III. METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini menggunakan metode penelitan tindakan atau *action research*, ada lima tahapan dalam penelitian yang merupakan siklus dari action research seperti pada Gambar 1.

Tahap pertama adalah melakukan diagnosa (Diagnosing) Pada tahapan ini peneliti akan melakukan identifikasi masalah-masalah yaitu diagnosa sistem keamanan pada LMS yang dibuat menggunakan TutorLMS dengan cara melakukan studi literatur, penentuan ruang lingkup serta pengumpulan data dari observasi dan dokumentasi dari TutorLMS.



Gambar 1. Alur Penelitian

Tahap kedua adalah membuat rencana tindakan (*Action Planning*) tahapan ini peneliti melakukan pemahaman pokok masalah yang ada dan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada. Peneliti akan mulai menyusun rencana pengujian yang akan dilakukan pada LMS yang dibuat menggunakan TutorLMS.

Tahap ketiga adalah melakukan tindakan (*Action Taking*) mengimplementasikan rencana tindakan yang telah disusun. Pada langkah ini peneliti mulai melakukan tahapan-tahapan investigasi guna mendapatkan informasi kelemahan sistem dan mengujinya secara langsung dengan menggunakan tipe-tipe ancaman terhadap LMS yang dibuat menggunakan TutorLMS.

Tahap keempat adalah melakukan evaluasi (*Evaluating*) setelah tahapan *Action Taking* dilaksanakan peneliti mulai melakukan evaluasi pada hasil dari implementasi sebelumnya dan mulai menyimpulkan hasil dari langkah sebelumnya.

e-ISSN: 2541-5867
DOI: 10.37253/telcomatics.v7i2.7357

Tahap kelima adalah pembelajaran (Learning) langkah ini merupakan tahap akhir dari penelitian yaitu melakukan review terhadap hasil dari tahapan-tahapan yang telah dilalui.

Tabel 1. List REST API TutorLMS

Menampilkan List Kursus **http://yourwebsiteaddress/wp-json/tutor/v1/courses?order=desc&orderby=ID&paged=1** **Type: get** **Parameters: optional** **Pagination: true**
Menampilkan Detail Kursus **http://yourwebsiteaddress/wp-json/tutor/v1/course-detail/** **Type: get** **Parameter: required(number)**
Menampilkan Topik dari Kelas Kursus **http://yourwebsiteaddress/wp-json/tutor/v1/course-topic/** **Type: get** **Parameter: required (number)**
Menampilkan Pembelajaran dari Topik **http://yourwebsiteaddress/wp-json/tutor/v1/lesson/** **Type: get** **Parameter: required(number)**
Menampilkan Pengumuman Kursus **http://yourwebsiteaddress/wp-json/tutor/v1/course-annoucement/** **Type: get** **Parameter: required(number)**
Menampilkan Quiz dari Topik **http://yourwebsiteaddress/wp-json/tutor/v1/quiz/** **Type: get** **Parameter: required(number)**
Menampilkan Pertanyaan dari Quiz **http://yourwebsiteaddress/wp-json/tutor/v1/quiz-question-answer/** **Type: get** **Parameter: required(number)**
Menampilkan Informasi Author Kelas **http://yourwebsiteaddress/wp-json/tutor/v1/author-information/** **Type: get** **Parameter: required(number)**

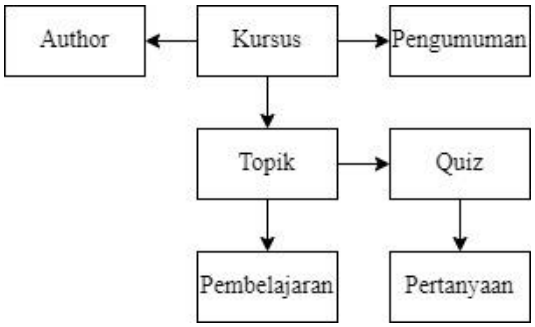
I. HASIL DAN PEMBAHASAN

Pada tahapan diagnosing peneliti membaca dokumentasi yang tersedia secara resmi pada website TutorLMS [19]. Hasil diagnosa peneliti menemukan bahwa TutorLMS mendukung penuh WordPress REST API dan multiple endpoint yang dapat digunakan untuk membaca data melalui permintaan HTTP dalam format JSON. Saat ini TutorLMS REST API v1 hanya menyediakan fasilitas read-only. REST API ini bersifat Publik dan tidak diperlukan otentikasi [20]. Daftar REST API yang didapatkan dapat dilihat pada Tabel 1.

Pada Tabel 1, dapat digambarkan sebuah kursus pada TutorLMS memiliki struktur yang sederhana. Sebuah Kursus memiliki beberapa topik, topik memiliki pembelajaran atau quiz, quiz memiliki pertanyaan, kursus memiliki pengumuman dan author kelas. Detail struktur dapat dilihat pada Gambar 2.

Hasil diagnosis diatas, digunakan untuk tahapan action planning peneliti merencanakan pengujian kerentanan insecure design dan *broken access control* pada REST API TutorLMS yang akan dilakukan secara manual menggunakan web browser pada sistem demo TutorLMS yang sudah di install oleh developer beralamat di preview.themeum.com/tutor.

Rencana pengujian kerentanan akan menargetkan salah satu kelas kursus yang berbayar, dan membaca semua isi pembelajaran dan quiz yang ada seperti pada Tabel 2 tanpa melakukan registrasi atau pendaftaran pada sistem TutorLMS.



Gambar 2. Struktur TutorLMS

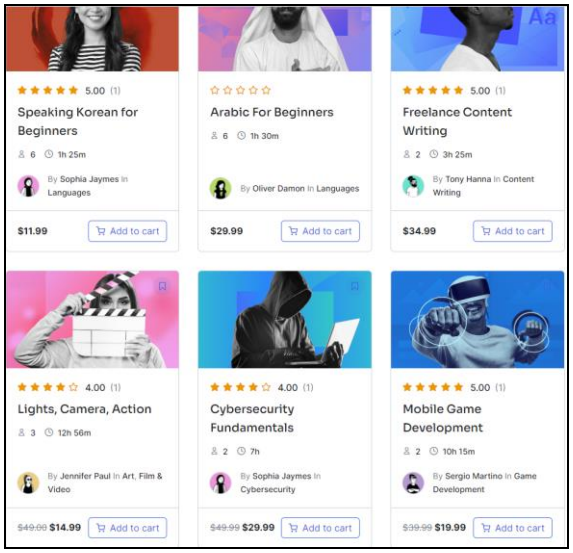
Tabel 2. Daftar Pengujian Kerentanan

No	Pengujian Kerentanan
1	Membaca Topik Kursus Berbayar
2	Membaca Pembelajaran dari Topik Berbayar
3	Membaca Quiz dari Topik Berbayar
4	Membaca Pertanyaan dari Quiz Berbayar
5	Membaca Pengumuman Kelas Berbayar
6	Membaca Author Kelas

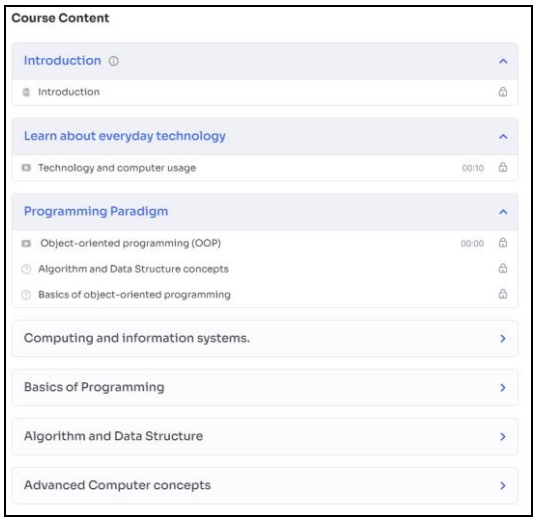
Action Taking diawali dengan mencari target kelas berbayar yang ingin dilakukan pengujian, dari hasil penelusuran web demo TutorLMS ditemukan kursus yang berbayar seperti Speaking Korean for Beginners, Arabic for Beginners, Freelance Content Writing, Light Camera Action, Cybersecurity Fundamentals

TELCOMATICS, Vol.7 No. 2, December 2022, pp. 53-60
e-ISSN: 2541-5867
DOI: 10.37253/telcomatics.v7i2.7357

dan Mobile Game Development, detail dapat dilihat pada Gambar 3.



Gambar 3. Daftar Kursus Berbayar



Gambar 4. Isi Kursus Cybersecurity Fundamentals

Untuk pengujian peneliti akan menargetkan kursus Cybersecurity Fundamentals untuk menjadi bahan pengujian. Detail Kursus Cybersecurity Fundamentals dilihat dari tampilan frontend memiliki 7 topik, didalam topik terdapat beberapa pembelajaran berupa video dan quiz. Video dan quiz pada tampilan frontend tidak bisa diakses atau terkunci karena peneliti tidak melakukan pembelian kursus seperti pada Gambar 4.

Setelah mendapatkan target kelas kursus, tahapan berikutnya peneliti menggunakan REST API yang diberikan dari Tabel 1 untuk melakukan pengujian sesuai daftar Tabel 2.

Peneliti mencari id kursus Cybersecurity Fundamentals dengan mengakses alamat web https://preview.themeum.com/tutor/wp-json/tutor/v1/courses. Hasil penelusuran API mendapatkan id kursus target adalah 109 dan id author adalah 2 seperti pada Gambar 5.


```
ID: 109,
post_author: "2",
post_date: "2022-02-18 06:21:27",
post_date_gmt: "2022-02-18 06:21:27",
post_content: "<p class=\"tutor-course-content\">Over this course's dur
is delivered. We will delve into its various subtopics and discuss each
but not least, we will compare some of the platforms and discuss the fu
content\">The number of well-paying jobs in this industry is slowly gro
Unfortunately, this branch of computer science severely lacks talented
content\">Throughout this course, you will learn concepts around the sp
also gain knowledge on other important topics.</p>",
post_title: "Cybersecurity Fundamentals",
post_excerpt: "",
post_status: "publish",
comment_status: "closed",
ping_status: "closed",
post_password: "",
post_name: "cybersecurity-fundamentals",
to_ping: "",
pinged: "",
post_modified: "2022-03-13 06:09:55",
post_modified_gmt: "2022-03-13 06:09:55",
post_content_filtered: "",
post_parent: 0,
guid: https://preview.themeum.com/tutor/?post_type=courses&#038;p=109,
menu_order: 0,
post_type: "courses",
post_mime_type: "",
comment_count: "0",
```


Gambar 5. Respon API Membaca Kursus

Id kursus yang didapatkan, akan digunakan untuk pengujian pembacaan topik https://preview.themeum.com/tutor/wp-json/tutor/v1/course-topic/109. Hasil pengujian menampilkan daftar topik beserta id topik seperti pada Gambar 6.


```
status_code: "success",
message: "Quiz retrieved successfully",
data: [
  ▾ {
      ID: "876",
      post_title: "Algorithm and Data Structure concepts",
      post_content: "",
      post_name: "algorithm-and-data-structure-concepts-3",
    ▾ quiz_settings: [
        ▾ {
          ▾ time_limit: {
              time_value: "30",
              time_type: "minutes"
            },
            attempts_allowed: "10",
            passing_grade: "80",
            max_questions_for_answer: "10",
            question_layout_view: "",
            questions_order: "rand",
            short_answer_characters_limit: "200",
            hide_quiz_time_display: 0,
            quiz_auto_start: 0,
            hide_question_number_overview: 0
```


Gambar 6. Respon API Membaca Topik

Id topik yang didapatkan, digunakan untuk pengujian pembacaan pembelajaran dan quiz. Pengujiaan pembacaan pembelajaran https://preview.themeum.com/tutor/wp-json/tutor/v1/lesson/709 mendapatkan detail isi

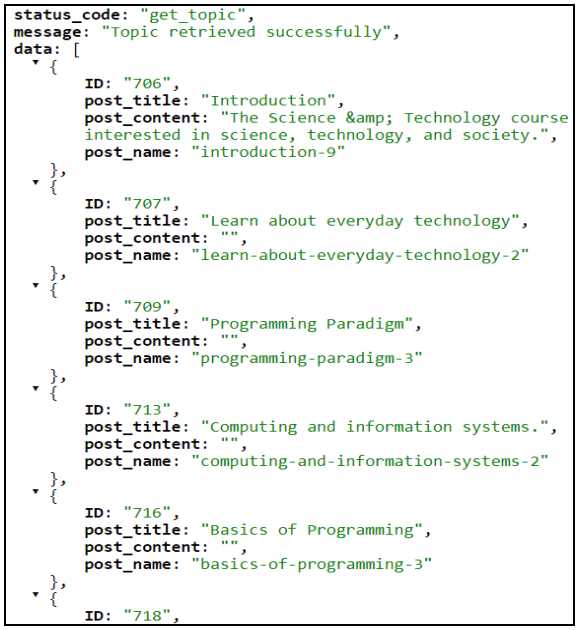
e-ISSN: 2541-5867
DOI: 10.37253/telcomatics.v7i2.7357

topik dan video pembelajaran seperti pada Gambar 7. Pengujiaan pembacaan quiz https://preview.themeum.com/tutor/wp-json/tutor/v1/quiz/709 mendapatkan id quiz dan detail quiz seperti pada Gambar 8.

Id quiz yang didapatkan, digunakan untuk pengujian pembacaan pertanyaan quiz https://preview.themeum.com/tutor/wp-json/tutor/v1/quiz-question-answer/876, respon API menampilkan keseluruhan isi pertanyaan, daftar jawaban dan jawaban yang benar dari quiz tersebut seperti pada Gambar 9.

Id kursus yang didapatkan akan digunakan untuk melakukan pengujian membaca pengumuman kelas kursus https://preview.themeum.com/tutor/wp-json/tutor/v1/course-annoucement/109

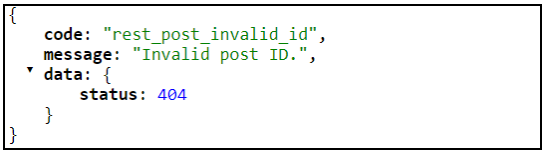
Hasil pengujian mendapatkan respon not found seperti pada Gambar 10 yang berarti pengujian memberikan hasil positif tetapi tidak ada pengumuman pada kelas kursus. Pengujian terakhir menggunakan id author pada kursus untuk menguji pembacaan data author kelas https://preview.themeum.com/tutor/wp-json/tutor/v1/author-information/2, pengujian memberikan data nama, email, id kelas yang pernah dibuat dan kapan melakukan pendaftaran pada sistem TutorLMS seperti pada Gambar 11.



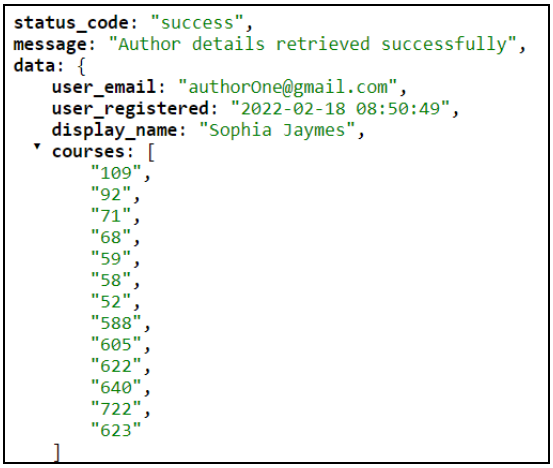
Gambar 7. Respon API Membaca Pembelajaran

Gambar 8. Respon API Membaca Quiz

Gambar 9. Respon API Membaca Pertanyaan Quiz



Gambar 10. `Respon API Membaca Pengumuman



Gambar 11. Respon API Membaca Author

TELCOMATICS, Vol.7 No. 2, December 2022, pp. 53-60
e-ISSN: 2541-5867
DOI: 10.37253/telcomatics.v7i2.7357

II. KESIMPULAN

Pengujian keamanan pada sistem TutorLMS menunjukkan bahwa plugin TutorLMS memiliki kerentanan pada insecure design dan broken access control. Kursus online berbayar dapat diakses dengan mudah oleh pengunjung yang tidak melakukan pembelian bahkan pendaftaran. Desain REST API yang ada pada dokumentasi, tidak memerlukan autentikasi untuk membaca isi dari kursus online, menyebabkan pengunjung dapat dengan mudah untuk mengambil isi pembelajaran, video dan lainnya. Pengunjung juga dapat mendapatkan pertanyaan quiz dan jawaban, serta mendapatkan informasi author pembuat kursus.

III. DAFTAR PUSTAKA

[1] F. A. Utami and R. N. Nurwati, "Dampak Pandemi Covid-19 Terhadap Pemutusan Hubungan Kerja (Phk) Pada Karyawan Fun World (Tempat Bermain Anak) Di Kota Cirebon," *Focus J. Pekerj. Sos.*, vol. 5, no. 1, p. 1, 2022, doi: 10.24198/focus.v5i1.28124.

[2] Aprillia Indah Pangestu and S. Ratnawati, "Pengembangan Ekonomi Kreatif Pada Masa Pandemi Covid-19 Dalam Perspektif Social Entrepreneurship," *Entrep. J. Bisnis Manaj. dan Kewirausahaan*, vol. 3, no. 1, pp. 469–479, 2022, doi: 10.31949/entrepreneur.v3i1.1489.

[3] A. P. Raneo, K. M. H. Thamrin, D. Yunita, and A. Nurullah, "Peluang Bisnis Multimedia di Era Pandemi Covid-19," *Sricommerce J. Sriwij. Community Serv.*, vol. 2, no. 2, pp. 105–112, 2021, doi: 10.29259/jscs.v2i2.43.

[4] Themeum, "Tutor LMS – eLearning and online course solution," *Wordpress Org*, 2022. https://wordpress.org/plugins/tutor/.

[5] Wordpress.Org, "Tutor LMS - Most Powerful WordPress LMS Plugin," 2022. https://www.themeum.com/product/tutor-lms/.

[6] T. Hardiani, D. Wijayanto, and N. Latifah, "Data Security Analysis With OWASP Framework on Website XYZ," *Cybernetics*, vol. 6, no. 01, pp. 10–20, 2022.

[7] M. M. Hassan, M. A. Ali, T. Bhuiyan, M. H. Sharif, and S. Biswas, "Quantitative Assessment on Broken Access Control Vulnerability in Web Applications," *Int. Conf. Cyber Secur. Comput. Sci. (ICONCS'18), Oct 18-20, 2018 Safranbolu, Turkey*, no. October, pp. 1–7, 2018.

[8] I. O. Riandhanu, "Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing pada Keamanan Website Absensi," *J. Inf. dan Teknol.*, vol. 4, no. 3, pp. 160–165, 2022, doi: 10.37034/jidt.v4i3.236.

[9] R. Pramudita, S. Fuada, and N. W. A. Majid, "Studi Pustaka Tentang Kerentanan Keamanan E-Learning dan Penanganannya," *J. Media Inform. Budidarma*, vol. 4, no. 2, p. 309, 2020, doi: 10.30865/mib.v4i2.1934.

[10] R. Azis and S. Yazid, "Pengujian Kerentanan Website WordPress Dengan Menggunakan Penetration Testing Untuk Menghasilkan Website Yang Aman," *J. Restikom Ris. Tek. Inform. dan Komput.*, vol. 3, no. 3, pp. 93–105, 2021.

[11] B. Ghozali, K. Kusrini, and S. Sudarmawan, "Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating," *Creat. Inf. Technol. J.*, vol. 4, no. 4, p. 264, 2019, doi: 10.24076/citec.2017v4i4.119.

[12] E. Listartha, G. Arna, J. Saskara, D. Gede, and S. Santyadiputra, "Vulnerability Testing and Security Penetration on Prodi XYZ Thesis Management Web Applications," *Sci. Comput. Sci. Informatics J.*, vol. 4, no. 2, pp. 1–14, 2021.

[13] S. Sahren, R. A. Dalimuthe, and M. Amin, "Penetration Testing Untuk Deteksi Vulnerability Sistem Informasi Kampus," *Pros. Semin. Nas. Ris. Inf. Sci.*, vol. 1, no. September, pp. 994–1001, 2019, doi: 10.30645/senaris.v1i0.109.

[14] R. Valentin, "Sistem Keamanan Database Berbasis Restfull Pada Content Management System Wordpress (Studi Kasus: STIKI Malang)," *J. Inf. Technol.*, vol. 06, no. 01, pp. 78–89, 2018.

[15] T. Rahmadi, Khairil, and R. Supardi, "Analisis Kemanan Website Menggunakan Metode Penetration Testing," *GATOTKACA J. (Teknik Sipil, Inform. Mesin dan Arsitektur)*, vol. 2, no. 2, pp. 147–152, 2021.

[16] Andria and R. K. Setyansah, "Pemanfaatan Learning Management System (Lms) Berbasis E-Front," *Indones. J. Netw. Secur.*, vol. 9, no. 1, pp. 7–11, 2020.

[17] The OWASP® Foundation, "A04:2021 – Insecure Design," 2021. https://owasp.org/Top10/A04_2021-Insecure_Design/.

[18] The OWASP® Foundation, "A01:2021 – Broken Access Control," 2021. https://owasp.org/Top10/A01_2021-Broken_Access_Control/.

[19] Themeum, "Documentation | Tutor LMS," 2022. https://docs.themeum.com/tutor-lms/.

[20] Themeum, "Documentation | REST API," 2022. https://docs.themeum.com/tutor-lms/developers/rest-api/.