DESAIN KONTROL KEAMANAN PADA CONTENT MANAGEMENT SYSTEM WORDPRESS BERDASAR ASPEK JARINGAN DENGAN PANDUAN OWASP

1st Adnan Nauli Harahap
Program Studi S1 Sistem Informasi
Universitas Telkom
Bandung, Indonesia
adnannh@student.telkomuniversity.ac.id

2nd Adityas Widjajarto
Program Studi S1 Sistem Informasi
Universitas Telkom
Bandung, Indonesia
adtwjrt@telkomuniversity.ac.id

3rd Avon Budiyono
Program Studi S1 Sistem Informasi
Universitas Telkom
Bandung, Indonesia
avonbudi@telkomuniversity.ac.id

***Abstrak* — WordPress adalah *Content Management System* (CMS) yang paling populer di dunia untuk membuat dan mengelola situs web. Dengan kepopulerannya, membuat WordPress menjadi target serangan para *hacker* untuk menemukan celah keamanan dan melancarkan serangan yang berdampak kepada penggunanya. Penelitian ini bertujuan untuk mendesain sebuah prioritas kontrol keamanan pada WordPress dari eksploitasi-eksploitasi yang diujikan, terutama yang berhubungan dengan jaringan. Eksploitasi yang dilakukan yaitu eksploitasi terhadap XML-RPC dengan *Brute Force*, DDoS, *Packet Sniffing*, *Packet Data Manipulation*, dan *Session Hijacking* dengan target utama eksploitasi yaitu WordPress. Hasil dari eksploitasi dianalisis menggunakan pendekatan ancaman terhadap keamanan data yang terdiri dari *Disclosure*, *Alteration*, dan *Denial* serta berdasarkan OWASP *Top Ten*. Lalu, Setiap eksploitasi dievaluasi tingkat keparahan kerentanannya berdasarkan kategori yang diperoleh dari skor CVSS. Hasil dari penelitian ini berupa desain kontrol keamanan berdasarkan standar OWASP untuk prioritas mitigasi di CMS WordPress dengan urutan prioritas pertamanya yaitu eksploitasi *Packet Sniffing* yang termasuk ke dalam kategori *Cryptographic Failures* dengan tingkat keparahan di level *High*, tipe ancamannya berupa *Disclosure* dan mekanisme keamanan yang diterapkan dapat berupa penggunaan sertifikat SSL/TLS pada *server* WordPress, *Force* HTTPS, dan HTTP *Strict Transport Security* (HSTS). Kelanjutan penelitian ini dapat berupa penambahan variasi eksploitasi atau analisis terhadap sumber daya yang digunakan selama proses eksploitasi.**

***Kata kunci* — desain kontrol, eksploitasi, wordpress, jaringan**

I. PENDAHULUAN

Tidak bisa dipungkiri, keamanan adalah salah satu hal yang penting dan sering dibahas ketika berbicara mengenai teknologi di masa sekarang ini. Teknologi memainkan peranan penting di semua lini kehidupan, mulai dari penggunaan pribadi hingga bisnis yang bernilai milyaran rupiah. Keamanan menjadi aspek penting untuk melindungi data, sistem, layanan, dan semua jenis produk digital dari berbagai risiko yang mengancam. Salah satu bentuk produk digital tersebut adalah *Content Management System* atau biasa disingkat dengan CMS.

CMS adalah sistem yang memungkinkan pengguna untuk bisa membuat, mengelola, dan menyimpan konten digital seperti teks, gambar, video, dan audio tanpa harus memiliki pengetahuan teknis yang mendalam tentang pemrograman web. Banyak keuntungan yang bisa didapatkan ketika menggunakan CMS di antaranya mudah digunakan, memiliki banyak fitur tambahan yang bisa digunakan secara gratis, dan dapat digunakan untuk berbagai kebutuhan. Salah satu CMS yang paling populer dan banyak digunakan di dunia adalah WordPress.

WordPress adalah *Content Management System* (CMS) untuk membuat dan mengelola *website* atau *blog*. WordPress dibangun menggunakan bahasa pemrograman PHP dan basis data MySQL. WordPress digunakan hingga hampir 43,4% situs yang ada di dunia pada 2024 [1]. WordPress disukai oleh banyak pengguna karena WordPress memiliki tampilan antarmuka platform yang *user-friendly*, memiliki hingga 60 ribu *plugin* gratis yang bisa digunakan, dan yang terpenting WordPress bersifat *open source* yang artinya WordPress bisa digunakan, dimanipulasi, dan disebarkan tanpa perlu khawatir mengenai pelanggaran hak cipta.

Namun, bukan berarti WordPress tidak memiliki kekurangan. Sebagai salah satu CMS paling populer di dunia, WordPress menjadi sasaran serangan siber oleh para *hacker* untuk menemukan celah dan melancarkan peretasan yang bisa berdampak signifikan untuk penggunanya. Sebagian besar kerentanan disebabkan oleh kerentanan pada *plugin*, sedangkan faktor lainnya seperti serangan-serangan yang dapat dilakukan melalui jaringan atau internet, sehingga memungkinkan para *hacker* untuk memanfaatkan celah-celah tersebut.

Penelitian ini bertujuan untuk mengembangkan desain kontrol pada CMS untuk platform WordPress dengan meningkatkan keamanannya berdasarkan standar keamanan dunia seperti *Open Web Application Security Project* (OWASP). Desain kontrol yang diusulkan bertujuan untuk memberikan rekomendasi dan prioritas mekanisme keamanan ketika ingin menggunakan CMS WordPress, serta eksploitasi yang diujikan pada penelitian ini berfokus pada eksploitasi-eksploitasi yang berbasis pada aspek jaringannya.

II. KAJIAN TEORI

A. *Content Management System* (CMS)

Content Management System (CMS) adalah jenis perangkat lunak yang berfungsi untuk mengelola konten. Konten yang dimaksud mencakup berbagai bentuk informasi digital, seperti contohnya teks, gambar, audio, dan video. CMS ini merupakan aplikasi berbasis web yang diimplementasikan dengan menggunakan bahasa pemrograman yang mendukung pengembangan web [2]. Salah satu tujuan dari CMS adalah memudahkan orang yang tidak memiliki latar belakang teknis dalam pengembangan web untuk dapat mengedit dan menyesuaikan konten pada aplikasi web [3].

B. WordPress

WordPress adalah aplikasi CMS yang siap digunakan untuk membuat *website* dengan mudah, dilengkapi dengan berbagai *plugin* dan tema dasar yang dapat dimodifikasi dan dikembangkan lebih lanjut. WordPress bersifat *open-source* yang artinya tersedia secara gratis dan dapat dikembangkan secara mandiri. *Plugin* yang tersedia memiliki keunggulan masing-masing dan dikembangkan oleh pengembang dari seluruh dunia, menjadikannya salah satu kekuatan utama WordPress. Selain itu, WordPress juga memiliki beragam tema yang responsif untuk berbagai jenis perangkat [4].

C. *Threat*

Threat atau ancaman dalam konteks keamanan siber didefinisikan sebagai segala potensi bahaya yang dapat menyebabkan kerusakan atau mengganggu keamanan sistem informasi, sehingga ancaman tersebut dapat merusak kerahasiaan, integritas dan ketersediaan data atau informasi [5]. Ancaman dalam keamanan siber juga dapat diartikan sebagai tindakan oleh pelaku jahat (*malicious actor*) yang berhasil mendapatkan akses tidak sah ke jaringan komputer milik individu atau organisasi lain dengan tujuan untuk mencuri data, merusak, atau mengganggu [6].

D. *Vulnerability*

Vulnerability atau kerentanan pada sistem jaringan komputer adalah kelemahan, kekurangan, atau celah yang bisa dieksploitasi oleh satu atau lebih penyerang untuk melancarkan serangan. Serangan ini dapat mengancam kerahasiaan, integritas, atau ketersediaan suatu sistem [7].

E. OWASP

Open Web Application Security Project (OWASP) adalah organisasi nirlaba yang berfokus pada peningkatan keamanan di perangkat lunak. OWASP berfungsi sebagai kerangka kerja yang digunakan oleh pengembang dan profesional teknologi untuk melindungi situs web. Organisasi ini menyediakan sumber daya yang memungkinkan para pengembang untuk meningkatkan keamanan sistem melalui proyek *open-source* dan alat bantu dari OWASP yang digunakan dalam pengujian keamanan sistem [8]. Salah satu sumber daya tersebut adalah OWASP *Top Ten* yaitu daftar dari sepuluh risiko keamanan aplikasi web yang paling signifikan dan diperbarui secara berkala oleh OWASP. OWASP *Top Ten* ini dirancang untuk menyoroti masalah keamanan yang perlu diperhatikan oleh pengembang aplikasi web dalam proyek mereka [9].

F. CVE dan CVSS

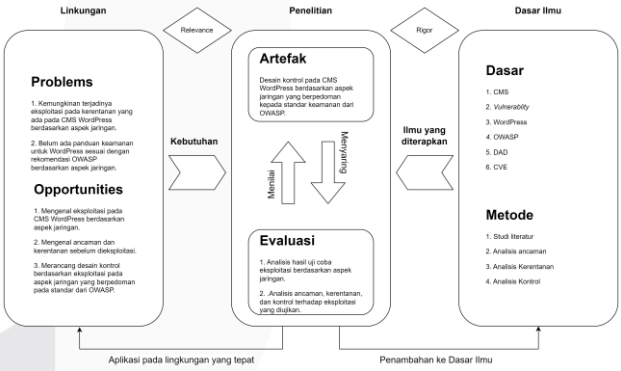
Common Vulnerabilities and Exposures (CVE) adalah sistem yang memberikan metode referensi untuk kerentanan (*vulnerability*) dan paparan (*exposure*) mengenai keamanan informasi yang dapat diketahui secara publik [10]. CVE juga berfungsi sebagai dokumentasi resmi terkait kerentanan yang terdeteksi dalam sebuah sistem keamanan informasi. Dokumentasi ini diterbitkan secara resmi oleh perusahaan Mitre [11]. Sedangkan, *Common Vulnerability Scoring System* (CVSS) adalah metode penilaian yang digunakan untuk mengukur tingkat kerentanan dalam suatu sistem. Skor CVSS dapat digunakan sebagai acuan untuk menentukan tingkat keparahan kerentanan yang ditemukan, dengan kategori penilaian yang meliputi *Low*, *Medium*, *High*, dan *Critical*. CVSS mengevaluasi beberapa aspek dalam menilai kerentanan, seperti *Attack Vector*, *Attack Complexity*, *Privilege Required*, *User Interaction*, *Scope*, *Confidentiality*, *Integrity*, dan *Availability* [12].

III. METODE

Gambaran rancangan penelitian yang dilakukan dijelaskan menggunakan model konseptual penelitian dan sistematika penyelesaian masalah seperti yang diuraikan sebagai berikut:

A. Model Konseptual Penelitian

Model konseptual penelitian merupakan kerangka berpikir yang bertujuan untuk memudahkan dalam mengidentifikasi permasalahan pada penelitian. Berikut adalah model konseptual penelitian ini:

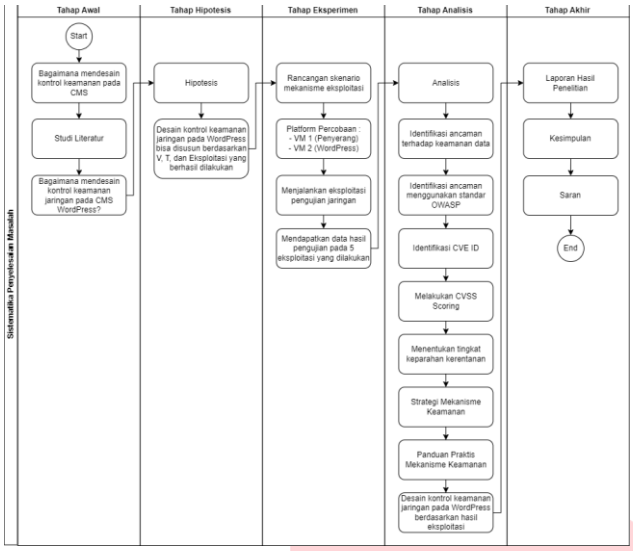


GAMBAR 1

(Model Konseptual Penelitian)

B. Sistematika Penyelesaian Masalah

Sistematika penyelesaian masalah adalah tahapan yang dilakukan pada pengerjaan penelitian dari tahap awal sampai tahap terakhir. Penyelesaian masalah pada penelitian ini mencakup 6 tahapan, yaitu: Tahap Awal, Tahap Hipotesis, Tahap Eksperimen, Tahap Analisis, dan Tahap Akhir. Berikut adalah sistematika penyelesaian masalah pada penelitian ini:



GAMBAR 2

(Sistematika Penyelesaian Masalah)

IV. HASIL DAN PEMBAHASAN

Bagian hasil dan pembahasan berisi analisis-analisis terhadap hasil data eksperimen eksploitasi yang diujikan. Analisis diawali dengan analisis terhadap ancaman pada keamanan data dan berdasar pada standar OWASP. Analisis selanjutnya adalah mengenai analisis kerentanan untuk mengukur tingkat keparahan masing-masing pengujian eksploitasi. Berikutnya, melakukan analisis kontrol pada eksploitasi berdasarkan hasil analisis-analisis sebelumnya dengan memodelkan desain kontrol berdasarkan kerentanan yang dieksploitasi keamanan sebagai bentuk prioritas kontrol berdasarkan hasil eksploitasi pengujian.

A. Analisis Ancaman Terhadap Keamanan Data

Pada analisis ancaman terhadap keamanan data terdapat tiga kategori jenis ancaman terhadap keamanan data yaitu Pengungkapan (*Disclosure*), Perubahan (*Alteration*), dan Penolakan (*Denial*). Berikut penjelasannya per eksploitasi:

TABEL 1

(Analisis Ancaman Terhadap Keamanan Data)

Eksploitasi	**Tipe Ancaman**	**Sebelum Eksploitasi**	**Setelah Eskploitasi**
XML-RPC / *Brute Force*	*Disclosure*	Informasi *login* semua pengguna dapat dijaga kerahasiaannya dan web WordPress terlindungi dari akses yang tidak sah.	Pihak tidak berwenang mendapatkan detail informasi *login* terutama *username* dan *password*, sehingga bisa mengakses WordPress.
DDoS	*Denial*	Semua layanan dan sistem pada *server* WordPress berjalan sebagaimana mestinya dan dapat merespons semua permintaan pengguna.	Penyerang menyebabkan layanan dan sistem pada *server* WordPress mengalami *down* dan tidak dapat diakses oleh pengguna sampai sistem diaktifkan kembali.
Packet Sniffing	*Disclosure*	Informasi mengenai paket data dan isinya tidak diketahui oleh pihak ketiga yang tidak berwenang.	Penyerang mendapatkan informasi detail mengenai isi paket data pada komunikasi yang tidak aman di *server* WordPress target.
Packet Data Manipulation	*Alteration*	Informasi pada paket data yang dikirimkan dari *server* WordPress masih utuh tanpa adanya perubahan apa pun ketika diterima pengguna.	Penyerang dapat mengubah isi paket data yang dikirimkan oleh *server* WordPress dengan menyisipkan skrip pada paket data tersebut.
Session Hijacking	*Disclosure*	Informasi mengenai *session cookie* pada akun pengguna dijaga kerahasiaannya pada WordPress.	Penyerang mendapatkan informasi *session cookie* yang bisa digunakan untuk menyusup masuk pada WordPress.

B. Analisis Ancaman Menggunakan Standar Dari OWASP

Pada analisis ancaman ini menggunakan daftar dari OWASP *Top Ten* edisi 2021 yang melakukan pemeringkatan terhadap ancaman keamanan paling signifikan dan diperbarui secara berkala oleh organisasi OWASP. Berikut penjelasannya per eksploitasi:

TABEL 2

(Analisis Ancaman Menggunakan Standar dari OWASP)

Eksploitasi	**Kategori OWASP *Top Ten***	**Alasan**
XML-RPC / *Brute Force*	*Identification and Authentication Failures* (A07:2021)	Karena pada eksploitasi ini tidak terdapat mekanisme yang mencegah serangan *brute force* yang bertujuan untuk mendapatkan informasi *login* pengguna WordPress.
DDoS	*Security Logging and Monitoring Failures* (A09:2021)	Karena pada eksploitasi ini terdapat ketidakmampuan dalam mendeteksi aktivitas yang mencurigakan dan merespons serangan DDoS pada *server* WordPress.
Packet Sniffing	*Cryptographic Failures* (A02:2021)	Karena pada eksploitasi ini data sensitif di dalam paket data tidak terenkripsi dengan benar sehingga penyerang dapat melihat data tersebut melalui lalu lintas jaringan yang telah dimanipulasi antara pengguna dan *server* WordPress.
Packet Data Manipulation	*Software and Data Integrity Failures* (A08:2021)	Karena pada eksploitasi ini penyerang memanipulasi paket data dengan injeksi skrip pada paket data yang diterima oleh pengguna dari web WordPress.
Session Hijacking	*Identification and Authentication Failures* (A07:2021)	Karena eksploitasi ini mendapatkan informasi sensitif berupa *session cookie* pengguna yang bisa digunakan untuk masuk sebagai pengguna tersebut di web WordPress.

C. Analisis Kerentanan Menggunakan CVSS

Analisis kerentanan bertujuan untuk mengetahui tingkat keparahan dari setiap eksploitasi yang diujikan. Analisis yang dilakukan adalah dengan mengidentifikasi CVE (*Common Vulnerabilities and Exposures*) dari masing-masing eksploitasi. Untuk beberapa eksploitasi pengujian yang spesifik dan tidak memiliki CVE ID tersendiri, maka akan dicarikan CVE yang lebih umum yang sekiranya memberikan dampak, hasil, atau proses yang mirip seperti yang dilakukan selama pengujian. Berikut penjelasannya per eksploitasi:

TABEL 3

(Identifikasi CVE ID dari Eksploitasi yang Diujikan)

Eksploitasi	Kerentanan	CVE ID
XML-RPC / *Brute Force*	*Gain Privileges via XML-RPC Method*.	CVE-2020-28035
DDoS	*Server Overload*	CVE-2023-44487
Packet Sniffing	*Unsecured* HTTP	CVE-2021-4161
Packet Data Manipulation	Inject Script to HTTP Response Packet	CVE-2021-21390
Session Hijacking	Session Cookie Stealing	CVE-2022-38846

Analisis berikutnya adalah menetapkan skor CVSS (*Common Vulnerability Scoring System*) dari CVSS *Vector* untuk mengevaluasi tingkat keparahan dari setiap eksploitasi dan menentukan kategori tingkat keparahannya. Berikut penjelasannya per eksploitasi:

TABEL 4

(Penentuan Tingkat Keparahan Berdasarkan Skor dari CVSS)

Eksploitasi	CVSS Vector	Skor	Level
XML-RPC / *Brute Force*	AV:N/AC:L/PR:N/UI:N/S:U/ C:H/I:H/A:H	9.8	*Critical*
DDoS	AV:N/AC:L/PR:N/UI:N/S:U/ C:N/I:N/A:H	7.5	*High*
Packet Sniffing	AV:N/AC:L/PR:N/UI:N/S:U/ C:H/I:N/A:N	7.5	*High*
Packet Data Manipulation	AV:N/AC:H/PR:N/UI:N/S:U/ C:N/I:H/A:N	5.9	*Medium*
Session Hijacking	AV:N/AC:H/PR:N/UI:N/S:U/ C:H/I:N/A:N	5.9	*Medium*

D. Desain Kontrol Keamanan

Pada bagian desain kontrol keamanan berdasarkan kerentanan yang dieksploitasi oleh ancaman ini bertujuan untuk melakukan prioritasi mekanisme keamanan agar memastikan keamanan WordPress secara menyeluruh. Desain kontrol ini didapatkan dari hasil analisis ancaman dan analisis kerentanan serta memberikan rekomendasi mekanisme keamanan pada setiap eksploitasinya. Berikut hasil desain kontrol untuk WordPress berdasarkan eksploitasi yang diujikan:

TABEL 5

(Desain Kontrol Keamanan Berdasarkan Kerentanan yang Diujikan)

Kategori OWASP *Top Ten*	Eksploitasi	Level	Tipe Ancaman	Mekanisme Keamanan
Cryptographic Failures (A02:2021)	*Packet Sniffing*	*High*	*Disclosure*	Gunakan sertifikat SSL/TLS pada *server* WordPress, *Force* HTTPS, dan HTTP *Strict Transport Security* (HSTS).
Identification and Authentication Failures (A07:2021)	XML-RPC / *Brute Force*	*Critical*	*Disclosure*	Menonaktifkan XML-RPC, membatasi akses ke berkas *xmlrpc.php*, atau memblokir metode tertentu di XML-RPC.
	Session Hijacking	*Medium*	*Disclosure*	Gunakan atribut "*Secure*" dan "*HttpOnly*" pada pengaturan *cookie* serta mengatur *timeout cookie*.
Software and Data Integrity Failures (A08:2021)	*Packet Data Manipulation*	*Medium*	*Alteration*	Gunakan HTTPS dengan sertifikat SSL/TLS dan *Hash-based Message Authentication Code* (HMAC).
Security Logging and Monitoring Failures (A09:2021)	DDoS	*High*	*Denial*	Gunakan *Web Application Firewall* (WAF) dan memasang *plugin* keamanan pada WordPress.

V. KESIMPULAN

Berdasarkan pengujian dan analisis yang telah dilakukan, penelitian ini menyimpulkan bahwa eksploitasi berdasar aspek jaringan terhadap WordPress dapat dilakukan melalui berbagai macam eksploitasi seperti eksploitasi XML-RPC dengan *Brute Force*, DDoS, *Packet Sniffing*, *Packet Data Manipulation*, dan *Session Hijacking*. Eksploitasi tersebut memiliki berbagai tingkat keparahan masing-masing, seperti eksploitasi XML-RPC yang termasuk dalam kategori *Critical* dengan skor CVSS 9.8, DDoS dan *Packet Sniffing* termasuk kategori *High* dengan skor 7.5, sementara *Packet Data Manipulation* dan *Session Hijacking* berada di kategori *Medium* dengan skor 5.9. Selain itu, desain kontrol keamanan berdasarkan OWASP *Top Ten*, tipe ancaman, dan tingkat keparahan menunjukkan bahwa mitigasi harus diprioritaskan dari eksploitasi *Packet Sniffing* sebagai prioritas pertama dengan mekanisme keamanan yang disarankan seperti penggunaan sertifikat SSL/TLS pada *server* WordPress, *Force* HTTPS, dan HTTP *Strict Transport Security* (HSTS). Kemudian, ada eksploitasi XML-RPC dengan mekanisme

keamanan berupa penonaktifan XML-RPC, pembatasan akses ke berkas "xmlrpc.php", atau pemblokiran metode tertentu di XML-RPC. Lalu, eksploitasi *Session Hijacking* dengan mekanisme keamanan dapat berupa penggunaan atribut "*Secure*" dan "*HttpOnly*" pada pengaturan *cookie* serta mengatur *timeout* pada *session cookie*. Selanjutnya, eksploitasi *Packet Data Manipulation* dengan mekanisme keamanan yang direkomendasikan dapat berupa penggunaan HTTPS dengan sertifikat SSL/TLS dan *Hash-based Message Authentication Code* (HMAC). Terakhir, eksploitasi DDoS sebagai prioritas terakhir dari eksploitasi yang diujikan dengan mekanisme keamanan dapat berupa penggunaan *Web Application Firewall* (WAF) dan pemasangan *plugin* keamanan di WordPress. Hasil dari desain kontrol ini menyimpulkan bahwa semakin tinggi kategori eksploitasinya dengan standar dari OWASP maka akan semakin menjadi prioritas untuk dilakukan kontrol pada eksploitasi tersebut.

REFERENSI

[1] B. F. Mauladhika, "Top 23 WordPress Statistics: Defining Trends and Insights for 2024." Accessed: Aug. 23, 2024. [Online]. Available: https://www.hostinger.com/tutorials/wordpress-statistics

[2] M. Z. Siambaton and M. Fakhriza, "Aplikasi Content Management System (CMS) Pada Joomla Untuk Membuat Web Service," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 1, no. 1, pp. 11–13, 2016, doi: 10.30743/infotekjar.v1i1.32.

[3] Basorudin, Gunarso, Erni Rouza, Luth Fimawahib, and Asep Supriyanto, "Perancangan dan Implementasi Sistem Operasi Linux Debian untuk Konfigurasi Content Management System (CMS) Wordpress Dengan Winscp," *Bull. Comput. Sci. Res.*, vol. 3, no. 1, pp. 21–29, 2022, doi: 10.47065/bulletincsr.v3i1.188.

[4] R. Muliono, "Optimasi Website Berbasis CMS Pada Google Pegespeed," *CESSJournal Comput. Eng. Syst. Sci.*, vol. 1, no. 2, pp. 32–35, 2016.

[5] Achmad Mukhlis, Baiq Laila Alfila, and Aliya Zhafira Wastuyana, "Ancaman dan Langkah Pengamanan Sistem Informasi Menggunakan Metode Systematic Literature Review," *J. Ilm. Sist. Inf. dan Ilmu Komput.*, vol. 3, no. 2, pp. 143–152, 2023, doi: 10.55606/juisik.v3i2.496.

[6] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," *Electron.*, vol. 12, no. 6, 2023, doi: 10.3390/electronics12061333.

[7] B. W. Retna Mulya and A. Tarigan, "Pemeringkatan Risiko Keamanan Sistem Jaringan Komputer Politeknik Kota Malang Menggunakan Cvss Dan Fmea," *Ilk. J. Ilm.*, vol. 10, no. 2, pp. 190–200, 2018, doi: 10.33096/ilkom.v10i2.311.190-200.

[8] A. W. Kuncoro and F. Rahma, "Analisis Metode Open Web Application Security Project (OWASP) pada Pengujian Keamanan Website: Literature Review," *Automata*, vol. 3, no. 1, pp. 1–5, 2021, [Online]. Available: https://www.sciencedirect.com

[9] H. Poston, "Mapping the OWASP Top Ten to Blockchain," *Procedia Comput. Sci.*, vol. 177, no. 2019, pp. 613–617, 2020, doi: 10.1016/j.procs.2020.10.087.

[10] Y. Yudiana, A. Elanda, and R. L. Buana, "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma Dengan Menggunakan OWASP Top 10," *CESS (Journal Comput. Eng. Syst. Sci.*, vol. 6, no. 2, p. 185, 2021, doi: 10.24114/cess.v6i2.24777.

[11] J. S. Marbun, S. Siddiq, R. A. Giffari, and A. R. Kardian, "Remote Code Execution (RCE) pada Windows 10 dengan Berkas .docx Menggunakan Framework Metasploit (CVE-2021-40444)," vol. 9, no. 1, pp. 119–127, 2024.

[12] M. Aziz, "Vulnerability Assesment Untuk Mencari Celah Keamanan Web Aplikasi E-Learning Pada Universitas XYZ," *J. Eng. Comput. Sci. Inf. Technol.*, vol. 2, no. 1, pp. 101–109, 2023, doi: 10.33365/jecsit.v1i1.13.