JIKB Jurnal Ilmu Komputer dan Bisnis

Jurnal Ilmu Komputer dan Bisnis (JIKB)
Mei-2021, Vol.XII, No.1, hal.88-101
ISSN(P): 2087-3921; ISSN(E): 2598-9715

Keamanan Sistem Perangkat Lunak dengan Secure Software Development Lifecycle

[1]Muhammad Rizky Hasan*, [2]Suhermanto, [3]Suharmanto
[1,2]Magister Ilmu Komputer Universitas Budiluhur

Alamat Surat
Email: [1]kesatrianagaapi@gmail.com, [2]suher.yahmi@gmail.com, [3]suharmanto.java@gmail.com

Article History:
Diajukan: 30-03-2021; Direvisi: 14-04-2021; Diterima: 28-04-2021

ABSTRAK

Saat ini, pengembangan perangkat lunak lebih kompleks daripada sebelumnya di mana keamanan menjadi salah satu yang paling krusial. Masalah keamanan menjadi bagian penting untuk developer perangkat lunak.Kebutuhan keamanan dalam pengembangan perangkat lunak menghasilkanpenciptaan yang disebut *Secure Software Development Life Cycle* (SSDLC). Paper ini menyoroti kerentanan perangkat lunak dan pendekatan untuk mengatasinya. Untuk itu akan dibahas beberapa tool keamanan seperti OWASP dan ISSAF. Tujuannya agar dapat mengetahui sejauh mana tool-tool tersebut meminimalkan kerentanan dalam pengembangan perangkat lunak.

Kata Kunci : Keamanan; perangkat lunak; SSDLC

ABSTRACT

Software development is more complex than ever with security being one of the most crucial. Security issues are an important part for software developers. Security requirements in software development result in a creation called the Secure Software Development Life Cycle (SSDLC). This paper looks at software vulnerabilities and approaches to address them. For that we will discuss several security tools such as OWASP and ISSAF. The goal is to know the extent to which these tools minimize vulnerabilities in software development.

Keywords: Security; software; SSDLC

1. *INTRODUCTION*

Internet telah mengubah dunia, hari ini hampir semua orang yang terhubung ke Internet menunjukkan persentase penetrasi pengguna internet di dunia semakin meningkat. Kerentanan dari serangan dengan metode injeksi seperti *Cross Site Scripting* dan *SQL Injection* yang dapat digunakan oleh pihak tertentu untuk mencuri informasi atau untuk tujuan tertentu(Kurniawan, Riadi, & Luthfi, 2017). Saat ini, pengembangan perangkat lunak lebih kompleks daripada sebelumnya di mana keamanan menjadi salah satu yang paling krusial. Masalah keamanan menjadi bagian penting untuk developer perangkat lunak dan memahami kerentanan, risiko dan lain-lain menjadi makanan sehari-hari(Fujdiak et al., 2019).

Kebutuhan keamanan dalam pengembangan perangkat lunak menghasilkanpenciptaan yang disebut *Secure Software Development Life Cycle* (SSDLC). Ini adalah konsep metodologis yang termasuk dalam *Software Development Life Cycle*, yang dijelaskan oleh limafase utama - *analysis, design, implementation (building), testing,* dan *evaluation*

https://doi.org/10.47927/jikb.v12i1.95

(deployment dan maintenance)(Fujdiak et al., 2019). *Secure Software Development Life Cycle*, SSDLC, menekankan pada keamanan ke dalam *Software Development Life Cycle*. Perangkat lunak yang aman tidak mudah dicapai dan ditunjukkan bahwa peningkatan proses pengembangan perangkat lunak dapat membantu meminimalkan jumlah kerentanan dalam pengembangan perangkat lunak. Namun, proses SSDLC melibatkan banyak praktik dan kegiatan keamanan untuk mencapai tujuan keamanan. Cara mengadopsi kegiatan ini dengan baik untuk meningkatkan keamanan perangkat lunak merupakan masalah yang penting(Tung, Lo, Shih, & Lin, 2016).

Paper ini menyoroti kerentanan perangkat lunakdan pendekatan untuk mengatasinya. Untuk itu akan dibahas beberapa *tool* keamanan seperti OWASP dan ISSAF. Tujuannya agar dapat mengetahui sejauh mana *tool-tool* tersebut meminimalkan kerentanan dalam pengembangan perangkat lunak.

2. *RELATED WORKS*

Penyusunan paper ini mengambil beberapa referensi penelitian sebelumnya/jurnal-jurnal yang berhubungan dengan penelitian ini.

Tabel 1. Penelitan-Penelitian Sebelumnya

No.	Judul	Penulis	Jurnal/Konferensi	Tujuan Penelitian	Masalah	Metode	Hasil/Kesimpulan
1.	Forensic Analysis And Prevent Of Cross Site Scripting In Single Victim Attack Using Open Web Application Security Project (Owasp) Framework	Ade Kurniawan, Imam Riadi, Ahmad Luthfi	Journal of Theoretical and Applied Information Technology	Menawarkan metode proteksi kepada user	Cyberattack pada individual maupun website dengan menggunakan metode cross site scripting atau sql injection	Open Web Application Security Project (OWASP)	Forensic Analysis And Prevent Of Cross Site Scripting In Single Victim Attack Using Open Web Application Security Project (OWASP) Framework terbagi menjadi 3 tahap, yaitu: Tahap Attacking, Tahap Analisis, dan Tahap Patching.
2.	DLR Secure Software Engineering	Rohan Krishnamurthy, Michael Meinel, Carina	2018 ACM/IEEE 1st International	Meningkatkan software development	DLR adalah sebuah organisasi penelitian di Jerman	DLR Secure Software Engine	Untuk meningkatkan proses pengembangan perangkat

		Haupt, Andreas Schreiber, Patrick Mäder	Workshop on Security Awareness from Design to Deployment	process untuk menghasilkan software berkeamanan tinggi	yang mengharuskan untuk membagikan atau sharing software yang mereka buat kepada partner dan mempublikasinya secara terbuka. Karenanya sangat penting sekali untuk menguatkan software untuk mencegah penyerangan terbuka.	ering	lunak, kami memulai a kelompok penelitian baru. Tujuan kami adalah untuk mengoptimalkan properti proses menggunakan pendekatan dari ilmu data. Kami menyertakan dua sumber utama data: asal proses perangkat lunak dan skor untuk perangkat lunak keamanan artefak itu.
3.	An Application Security Framework for SOA-based Mission Data Systems	Daniel Fischer, Mehran Sarkarati, Mariella Spada, Thomas Michelbach, Wenzel Urban, Christian Tueffers	2011 Fourth IEEE International Conference on Space Mission Challenges for Information Technology 2011 Space Mission Challenges for Information Technology	Menjelaskan sebuah application security framework untuk Sistem data misi berbasis SOA (Service Oriented Architecture)	keamanan informasi adalah bidang yang semakin berkembang dalam ESA dan badan antariksa lainnya. Dalam beberapa tahun terakhir, ancaman yang dihasilkan dari kejahatan dunia maya telah berkembang di seluruh	Secure Software Development Cycle (SSDLC)	kami telah mempresentasikan kerangka kerja keamanan aplikasi untuk penyediaan sistem data misi SOA yang mampu meningkatkan secara signifikan ketahanan dan keamanan aplikasi layanan web.

					dunia.		
4.	Managing the Secure Software Development	Radek Fujdiak, Petr Mlynek, Pavel Mrnustik, Maros Barabas, Petr Blazek, Filip Borcik, Jiri Misurec.	2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)	fokus pada keamanan SDLC bersama dengan tantangan terkait dan masalah terkait.	Masalah keamanan menjadi bagian penting dari Software engineer dan memahami kerentanan, risiko, dan lainnya menjadi roti sehari-hari.	SSDLC	memperkenalkanpendekatan, menyoroti tantangan, dan memunculkan topik baru pendekatan manajemen di SSDLC bersama dengan pengenalan alat mSSDLC kami
5.	MENENTUKAN DAMPAK RESIKO KEAMANAN BERBASIS PENDEKATAN OWASP	Robertus Halomoan Hutagalung, Lukito Edi Nugroho, Risanuri Hidayat	Prosiding SNATIF Ke- 4 Tahun 2017	Asesmen keamanan pada aplikasi berbasis website .	Mengetahui celah keamanan pada aplikasi berbasis web saja belum cukup untuk meningkatkan keamanan pada aplikasi.	Open Web Application Security Project	Hasil kemungkinan dan dampak keseluruhan pada celah ***local file inclusion*** adalah 6.375 (High) pada tingkat overall likelihood, 9 (High) pada tingkat Overall Technical Impact, 4.75 (Medium) pada tingkat Overall Business Impact. Hasil kemungkinan dan dampak keseluruhan pada celah ***Sql Injection***

							adalah 6.375 (High) pada tingkat overall likelihood, 3.75 (Medium) pada tingkat Overall Technical Impact, 1.75 (Low) pada tingkat Overall Business Impact. Hasil kemungkinan dan dampak keseluruhan pada celah ***xss injection*** adalah 6.25 (High) pada tingkat overall likelihood, 3.25 (Medium) pada tingkat Overall Technical Impact, 1.75 (Low) pada tingkat Overall Business Impact.
6.	SQL Injection and Cross Site Scripting Prevention Using OWASP Web	Robinson, Memen Akbar, Muhammad Arif Fadhly Ridha	INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION	penelitian ini mengusulkan Open Web Application Security Project	Informasi yang disimpan oleh aplikasi web seringkali bersifat rahasia dan, jika	Open Web Application Security Project	OWASP ModSecurity berhasil mendeteksi dan mengamankan 100% aplikasi web dari SQL Injection

	Application Firewall			(OWASP) ModSecurity Core Rule Set yang dapat membantu administrator mengamankan server web	diperoleh oleh penyerang dapat mengakibatkan kerugian besar bagi konsumen dan perusahaan.		setelah 15 kali pengujian menggunakan 3 Sistem Operasi perbedaan.
7.	Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server	Dr. Raden Teduh Dirgahayu, S.T., M.Sc., Yudi Prayudi, S.Si., M.Kom., Adi Fajaryanto	Jurnal Ilmiah NERO Vol. 1 No. 3	pengujian terhadap webserver IKIP PGRI menggunakan penetration testing, agar dapat direkomendasikan upaya untuk meminimalisir tingkat kerentanan sistem yang ada.	webserver IKIP PGRI Madiun, sejak pertama webserver online sampai saat ini webserver berhasil dibobol oleh hacker beberapa kali dalam setahun dan belum pernah dilakukan penetrationtest pada webservernya.	ISSAF dan OWASP	Hasil pengujian dan analisa dengan metode ISSAF menunjukkan bahwa sistem web server IKIP PGRI Madiun masih dapat ditembus dan mengambil alih hak akses administrator, sedangkan dengan metode OWASP versi 4 menunjukkan bahwa manajemen otentifikasi, otorisasi dan manajemen sesi belum diimplementasikan

							dengan baik.
8.	Penerapan Pengujian Keamanan Web Server Menggunakan Metode OWASP versi 4 (Studi Kasus Web Server Ujian Online)	Mohmmad Muhsin, Adi Fajaryanto	Multitek Indonesia Vol. 9, No. 1 Juni 2015	menerapkan pengujian keamanan aplikasi Ujian Online menggunakan metode OWASP versi 4 agar dapat diketahui tingkat kerentanan yang ada.	Mengingat pentingnya data yang tersimpan maka perlu diterapkan pengujian keamanan dari aplikasi	OWASP	Hasil pengujian menggunakan OWASP versi 4 menunjukkan bahwa manajemen otentifikasi, otorisasi dan manajemen sesi belum diimplementasikan dengan baik sehingga perlu dilakukan perbaikan lebih lanjut oleh pihak stake holder Fakultas Teknik Universitas Muhammadiyah Ponorogo
9.	An integrated security testing framework for Secure Software Development Life Cycle	Yuan-Hsin Tung, Sheng-Chen Lo, Jen-Feng Shih, and Hung-Fu Lin	Asia-Pacific Network Operations and Management Symposium (APNOMS)	kami mengusulkan framework pengujian keamanan terintegrasi untuk siklus hidup pengembangan perangkat lunak yang aman. Dalam	Ratusan kerentanan dan cacat keamanan diungkapkan oleh peretas, pengembang, dan pengguna.	SSDLC	Hasil menunjukkan bahwa sistem prototipe kami dapat memberikan kualitas dan layanan yang stabil. Sistem prototipe menunjukkan bahwa pendekatan kami efisien untuk melakukan masalah keamanan di

				framework usulan kami, kami menerapkan kegiatan keamanan dan praktik SSDLC untuk menghasilkan pedoman keamanan			bawah pengembangan perangkat lunak. Dalam studi selanjutnya, kami akan terus menambahkan fitur ke kerangka kerja kami yang diusulkan untuk tujuan peningkatan keamanan perangkat lunak.
10.	Secure Coding in Software Development	Nor Harisah Zainuddin, Assoc.Prof.Dr.Normaziah Abd Aziz	Malaysian Conference in Software Engineering (MySEC)	Paper ini menyoroti kerentanan perangkat lunak dan pendekatan untuk mengatasinya. Selain kesadaran seperti itu yang telah berlangsung selama dekade terakhir, penelitian ini mengusulkan alat yang dapat meningkatkan	Seiring dengan meningkatnya jumlah pengguna dan aplikasi tidak sah, kerentanan sistem dapat memperlakukan individu dan organisasi.	SDLC and OWASP	Kesimpulannya, keamanan bukanlah sesuatu yang ada ditujukan pada akhir pengembangan perangkat lunak atau dimasukkan fase tertentu dari SDLC tetapi perlu diintegrasikan di seluruh SDLC untuk menghasilkan perangkat lunak yang aman. Itu pentingnya keamanan harus dimasukkan ke dalam pikiran pengembang perangkat

				keterampilan dan insinyur pengetahuan terhadap perangkat lunak yang aman dalam membangun sistem yang aman.			lunak, manajer proyek, pemrogram, pemilik sistem dan juga pengguna akhir selama persyaratan, fase desain, pengkodean, pengujian, dan penyebaran.

3. *RESEARCH METHOD*

A. *Systematic Literature Review*

Tinjauan literatur sistematis berarti laporan dari "pertanyaan yang dirumuskan dengan jelas yang menggunakan metode sistematis dan eksplisit untuk mengidentifikasi, memilih, dan menilai secara kritis penelitian yang relevan dan untuk mengumpulkan dan menganalisis data dari studi yang termasuk dalam ulasan" (Liberati et al., 2009; van Laar, van Deursen, van Dijk, & de Haan, 2017). Penelitian literatur ini dibuat sesuai dengan Item Pelaporan Pilihan untuk Tinjauan Sistematis dan pedoman Analisis-Meta atau juga dikenal sebagai pedoman PRISMA untuk metode tinjauan literatur sistematis (van Laar et al., 2017). Urutan penelitian ini ditulis sesuai dengan Daftar Periksa PRISMA(Liberati et al., 2009). Metode ini dipilih, karena membantu mensintesis literatur akademik dengan cara yang akurat dan dapat diandalkan (van Laar et al., 2017).

Pendekatan PRISMA menyajikan daftar berbasis temuan dari 27 komponen dan diagram alir terdiri dari empat fase(Liberati et al., 2009). Daftar komponen melibatkan evaluasi reabilitas penelitian sebelumnya (van Laar et al., 2017). PRISMA tidak diusulkan sebagai teknik penilaian, tetapi PRISMA diusulkan untuk memastikan ketepatan dan kejelasan saat menulis makalah literatur sistematis. Daftar PRISMA dari 27 komponen dan diagram alir terdiri dari empat fase digunakan untuk melaporkan hasil (Liberati et al., 2009).

B. *Research Question*

Karena kebutuhan untuk mengevaluasi secara efektif kegunaan dari domain aplikasi spesifik, beberapa penulis telah mengembangkan studi untuk membangun faktor penentu keberhasilan dalam mengembangkan kinerja proyek sistem informasi. Dalam hal ini, membangun faktor-faktor itu penting untuk mengetahui pendekatan mana yang digunakan penulis untuk mengembangkan faktor-faktor keberhasilan kritis baru dalam mengembangkan proyek sistem informasi dan jika pendekatan yang digunakan memungkinkan menciptakan dan memvalidasi faktor-faktor keberhasilan kritis dalam mengembangkan proyek sistem informasi dengan benar (Quiñones & Rusu, 2017).

Tinjauan literatur sistematis ini ditulis berdasarkan pengamatan pada faktor-faktor keberhasilan pengembangan sistem informasi. Studi ini perlu disesuaikan dengan baik di

setiap organisasi yang proses utamanya berjalan pada pengembangan sistem informasi. Ketidakpedulian pengembangan sistem informasi akan menyebabkan kerugian pada proses bisnis. Karena itu, para peneliti dalam penelitian ini merasa sangat penting. Oleh karena itu, pertanyaan penelitian terbaik untuk tinjauan literatur sistematis ini adalah "Apakah FrameworkSSDLCdapat mengurangi kerentanan keamanan pada sistem perangkat lunak? "

C. *Study Selection Criteria*

Makalah yang dipilih harus memenuhi kriteria tinjauan literatur sistematis ini untuk menghasilkan hasil yang sesuai. Karena itu, kriteria inklusi harus mencakup:

1. Makalah yang merupakan makalah penelitian.
2. Makalah yang menjelaskan tentang framework-framework SSDLC dan tools yang digunakan.
3. Makalah yang menjelaskan tentang tinjauan literatur sistematis PRISMA.
4. Makalah yang diterbitkan dari 2014 hingga 2019.
5. Makalah yang ditulis dalam bahasa Inggris dan bahasa Indonesia.
6. Makalah yang diterbitkan di ScienceDirect, Scopus, JSTOR, IEEE, atau SpringerLink.
7. Makalah yang diterbitkan pada konferensi internasional dan jurnal internasional.

Kriteria pengecualian yang tidak memenuhi persyaratan meliputi:

1. Tesis yang tidak dipublikasikan.
2. Makalah yang tidak fokus terutama pada pengembangan sistem informasi.

D. *Data extraction*

Item data yang diekstraksi dari setiap artikel review termasuk: tinjauan literatur sistematis tentang faktor-faktor keberhasilan kritis dalam pengembangan sistem informasi menggunakan daftar periksa PRISMA; penulis penelitian; jurnal; Tanggal penerbitan; kondisi yang ditangani oleh setiap ulasan, dan intervensi diperiksa. Setiap item daftar periksa PRISMA dinilai memadai, tidak memadai, tidak dijelaskan, atau tidak berlaku [8].

Penelitian sebelumnya yang terlibat dalam penelitian literatur sistematis ini terkait dengan framework-framework SSDLC dan *tools* yang digunakan. Informasi diidentifikasi dan diekstraksi mengenai elemen-elemen berikut:

1. Penulis dan tahun makalah.
2. Domain yang diusulkan dalam framework-framework SSDLC dan *tools* yang digunakan.

4. *RESULT*

Strategi pencarian termasuk 16 paper kandidat dari tinjauan literatur sistematis ini. Hanya 8 paper yang dipilih dalam analisis akhir yang teks lengkapnya mengalami ekstraksi data karena terkait dengan studi tinjauan literatur sistematis ini. 8 makalah dikeluarkan karena artikel berada di luar ruang lingkup penelitian literatur ini.

A. *Study results*

Penelitian literatur ini mengamati alasan mengapa framework SSDLC aman digunakan dan dapat mengurangi kerentanan keamanan. Faktor penentu keberhasilan dikumpulkan dari penelitian sebelumnya yang ditunjukkan pada tabel di bawah ini.

Penulis	Tools	Hasil
Robinson, Memen Akbar, Muhammad Arif	OWASP	SQL Injection Attack : Dari 7 jenis serangan, 6 berhasil mengamankan

Fadhly Ridha		dan mendeteksi serangan.
		SQLmap Exploitation : Dari 3 sistem operasi yang diserang, 3 berhasil mengamankan dan mendeteksi serangan.
		BeEF Exploitation : Dari 3 sistem operasi yang diserang, 3 gagal mengamankan dan mendeteksi serangan.
		XSSer Exploitation : Dari 3 sistem operasi yang diserang, 3 berhasil mengamankan dan mendeteksi serangan.
Radek Fujdiak, Petr Mlynek, Pavel Mrnustik, Maros Barabas, Petr Blazek, Filip Borcik, Jiri Misurec.	mSSDLC	Berkat analisis tahap awal melalui mSSDLC dan manajemen pendekatan tahap awal mendapatkan informasi yang cukup untuk resimulasi, yang memberikan informasi yang cukup valid untuk proses pengambilan keputusan dan menghemat waktu serta biaya.
Daniel Fischer, Mehran Sarkarati, Mariella Spada, Thomas Michelbach, Wenzel Urban, Christian Tueffers	Penggunaan SSDLC framework untuk COSIF-based web application development	Kerangka kerja keamanan aplikasi untuk penyediaan sistem data misi SOA yang mampu meningkatkan secara signifikan ketahanan dan keamanan aplikasi layanan web. At the same time, the framework provides a set of tools and templates that aim at reducing the effort related to the additional steps, introduced in the SSDLC.
Ade Kurniawan, Imam Riadi, Ahmad Luthfi	OWASP	berhasil mendeteksi, memfilter, memblokir, dan memberi tahu pengguna sehingga korban menjadi lebih waspada jika pengguna menjelajah bahwa telah ada muatan yang dimilikinya telah disuntikkan oleh penyerang ke situs web dengan bentuk skrip kait dari Cross Site Scripting
Dr. Raden Teduh Dirgahayu, S.T., M.Sc., Yudi Prayudi, S.Si., M.Kom., Adi Fajaryanto	ISSAF dan OWASP	metode ISSAF menunjukkan bahwa sistem web server IKIP PGRI Madiun masih dapat ditembus dan mengambil alih hak akses administrator,

		metode OWASP versi 4 menunjukkan bahwa manajemen otentifikasi, otorisasi dan manajemen sesi belum diimplementasikan dengan baik.
Mohmmad Muhsin, Adi Fajaryanto	OWASP	Hasil pengujian menggunakan OWASP versi 4 menunjukkan bahwa manajemen otentifikasi, otorisasi dan manajemen sesi belum diimplementasikan dengan baik
Robertus Halomoan Hutagalung, Lukito Edi Nugroho, Risanuri Hidayat	OWASP	celah Sql Injection terhadap server.te.ugm.ac.id dapat di generate dan menghasilkan penilaian kemungkinan dengan angka 6.375 dengan tingkat kemungkinan secara keseluruhan adalah High dan dampak teknis secara keseluruhan menghasilkan nilai 3.75 yang berarti tingkat dampak pada sisi teknis adalah Medium, sedangkan dampak bisnis secara keseluruhan menghasilkan nilai 1.75 yang mana berarti tingkat dampak pada sisi bisnis adalah Low
		celah Xss Injection terhadap server.te.ugm.ac.id dapat di generate dan menghasilkan penilaian kemungkinan dengan angka 6.25 dengan tingkat kemungkinan secara keseluruhan adalah High dan dampak teknis secara keseluruhan menghasilkan nilai 3.25 yang berarti tingkat dampak pada sisi teknis adalah Medium, sedangkan dampak bisnis secara keseluruhan menghasilkan nilai 1.75 yang mana berarti tingkat dampak pada sisi teknis adalah Low
Yuan-Hsin Tung, Sheng-Chen Lo, Jen-Feng Shih, and Hung-Fu Lin	SSDLC	Hasilnya menunjukkan bahwa sistem prototipe kami dapat memberikan layanan yang berkualitas dan stabil.

5. *CONCLUSION*

Kesimpulan dari penelitian ini adalah bahwasanya Framework-framework SSDLC dapat mengevaluasi kerentanan keamanan pada sistem perangkat lunak. Dengan demikian perancang/developer perangkat lunak dapat menerapkan secure coding agar sistem yang akan dibangun dapat lebih rentan dari ancaman penyerangan.

6. *REFERENCES*

Fujdiak, R., Mlynek, P., Mrnustik, P., Barabas, M., Blazek, P., Borcik, F., & Misurec, J. (2019). Managing the secure software development. *2019 10th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2019 - Proceedings and Workshop*, 1–4. https://doi.org/10.1109/NTMS.2019.8763845

Kurniawan, A., Riadi, I., & Luthfi, A. (2017). Forensic analysis and prevent of cross site scripting in single victim attack using open web application security project (OWASP) framework. *Journal of Theoretical and Applied Information Technology*, *95*(6), 1363–1371.

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P. A., … Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate healthcare interventions: explanation and elaboration. *BMJ (Clinical Research Ed.)*, *339*. https://doi.org/10.1136/bmj.b2700

Quiñones, D., & Rusu, C. (2017). How to develop usability heuristics: A systematic literature review. *Computer Standards and Interfaces*, *53*(September 2016), 89–122. https://doi.org/10.1016/j.csi.2017.03.009

Tung, Y. H., Lo, S. C., Shih, J. F., & Lin, H. F. (2016). An integrated security testing framework for Secure Software Development Life Cycle. *18th Asia-Pacific Network Operations and Management Symposium, APNOMS 2016: Management of Softwarized Infrastructure - Proceedings*. https://doi.org/10.1109/APNOMS.2016.7737238

van Laar, E., van Deursen, A. J. A. M., van Dijk, J. A. G. M., & de Haan, J. (2017). The relation between 21st-century skills and digital skills: A systematic literature review. *Computers in Human Behavior*, *72*, 577–588. https://doi.org/10.1016/j.chb.2017.03.010

Pidgeon, T. E., Wellstead, G., Sagoo, H., Jafree, D. J., Fowler, A. J., & Agha, R. A. (2016). An assessment of the compliance of systematic review articles published in craniofacial surgery with the PRISMA statement guidelines: A systematic review. *Journal of Cranio-Maxillofacial Surgery*, *44*(10), 1522–1530. https://doi.org/10.1016/j.jcms.2016.07.018

Krishnamurthy, R., Meinel, M., Haupt, C., Schreiber, A., & Mader, P. (2018). DLR secure software engineering. Proceedings - 2018 ACM/IEEE 1st International Workshop on Security Awareness from Design to Deployment, SEAD 2018, 49–50. https://doi.org/10.23919/SEAD.2018.8472854

Fischer, D., Sarkarati, M., Spada, M., Michelbach, T., Urban, W., & Tueffers, C. (2011). An application security framework for SOA-based mission data systems. Proceedings - 4th IEEE International Conference on Space Mission Challenges for Information Technology, SMC-IT 2011, 53–60. https://doi.org/10.1109/SMC-IT.2011.22

Kurniawan, A., Riadi, I., & Luthfi, A. (2017). Forensic analysis and prevent of cross site scripting in single victim attack using open web application security project (OWASP) framework. Journal of Theoretical and Applied Information Technology, 95(6), 1363–1371.

Mada, U. G. (2017). Menentukan Dampak Resiko Keamanan Berbasis Pendekatan Owasp. Prosiding SNATIF, 477–484.

Akbar, M., Arif, M., Ridha, F., & Scripting, A. C. S. (2018). INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION SQL Injection and Cross Site Scripting Prevention Using OWASP Web Application Firewall. Journal on Informatics Visualization Sql, 2, 286–292.

Dirgahayu, T., Prayudi, Y., & Fajaryanto, A. (2015). Penerapan Metode ISSAF dan OWASP versi 4 Untuk Uji Kerentanan Web Server. Jurnal Ilmiah NERO, 1(3), 190–197. Retrieved from http://nero.trunojoyo.ac.id/index.php/nero/article/download/29/27

M. Muhsin, A. Fajaryanto, "Penerapan Pengujian Keamanan Web Server Menggunakan Metode OWASP versi 4 (Studi Kasus Web Server Ujian Online)," Multitek Indonesia, Vol. 9, pp. 31-42, 2015.

Zenah, N. H. Z., & Aziz, N. A. (2011). Secure coding in software development. 2011 5th Malaysian Conference in Software Engineering, MySEC 2011, 458–464. https://doi.org/10.1109/MySEC.2011.6140716

Ghozali, B., Kusrini, K., & Sudarmawan, S. (2019). Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating. Creative Information Technology Journal, 4(4), 264. https://doi.org/10.24076/citec.2017v4i4.119

Yu, H., Jones, N., Bullock, G., & Yuan, X. Y. (2011). Teaching secure software engineering: Writing secure code. 2011 7th Central and Eastern European Software Engineering Conference, CEE-SECR 2011, 1–5. https://doi.org/10.1109/CEE-SECR.2011.6188473

Kao, T. C., Mao, C. H., Chang, C. Y., & Chang, K. C. (2012). Cloud SSDLC: Cloud security governance deployment framework in secure system development life cycle. Proc. of the 11th IEEE Int. Conference on Trust, Security and Privacy in Computing and Communications, TrustCom-2012 - 11th IEEE Int. Conference on Ubiquitous Computing and Communications, IUCC-2012, 1143–1148. https://doi.org/10.1109/TrustCom.2012.106.

Tung, Y. H., Lo, S. C., Shih, J. F., & Lin, H. F. (2016). An integrated security testing framework for Secure Software Development Life Cycle. 18th Asia-Pacific Network Operations and Management Symposium, APNOMS 2016: Management of Softwarized Infrastructure - Proceedings. https://doi.org/10.1109/APNOMS.2016.7737238

Yang, J., Lodgher, A., & Lee, Y. (2019). Secure modules for undergraduate software engineering courses. Proceedings - Frontiers in Education Conference, FIE, 2018-October, 1–5. https://doi.org/10.1109/FIE.2018.8658433