PENGEMBANGAN SISTEM INFORMASI PENILAIAN KEAMANAN APLIKASI BERDASARKAN APPLICATION SECURITY VERIFICATION STANDARD (ASVS)

Maharani[1], Icha Yolindasari[2], Eriene Dheanda Absharina[3]
kharismaputriancak2005@gmail.com[1], ichayolindasari@gmail.com[2],
erienedheanda@itsnusriwijaya.ac.id[3]
UIN Raden Fatah Palembang

ABSTRAK

Dalam rangka memenuhi tuntutan transformasi digital di setiap sektor bisnis, penggunaan sistem informasi elektronik berupa aplikasi meningkat dengan pesat. Aplikasi berbasis web dan mobile merupakan platform sistem informasi yang paling banyak digunakan karena sesuai dengan kebutuhan penggunaannya yang hanya memerlukan jaringan internet untuk dapat terhubung dengan server. Server tersebut tentu melayani banyakpengguna dan banyak permintaan dimana masih terdapat banyak kasus serangan siber yang mengganggu aspek kerahasiaan, keutuhan, dan ketersediaan data dan informasi. Oleh karena itu, peningkatan keamanan aplikasi dengan melakukan penilaian keamanan aplikasi diperlukan dan Application Security Verification Standard (ASVS) merupakan salah satu standar yang memiliki beberapa tingkatan persyaratan keamanan yang dapat disesuaikan dengan kebutuhan pengembangan aplikasi di Indonesia. Penelitian ini mengembangkan sistem informasi penilaian keamanan aplikasi berdasarkan ASVS dengan menerapkan metode pengembangan Software Development Life Cycle (SDLC) yang terdiri dari proses perencanaan, desain, pembangunan, pengujian, operasional, dan pemeliharaan aplikasi. Berdasarkan hasil pengujian, aplikasi yang dikembangkan mampu menyediakan instrumen penilaian keamanan aplikasi yang sesuai dengan kebutuhan persyaratan sehingga pemilik atau pengembang aplikasi dapat melakukan peningkatan keamanan aplikasi secara mandiri, baik untuk aplikasi berbasis web maupun mobile.

Kata Kunci: Aplikasi Mobile, Aplikasi Web, ASVS, Keamanan Aplikasi, SDLC.

ABSTRACT

In order to meet the needs of digital transformation in every business, the use of information systems in the form of electronic application sectors is increasing rapidly. Web-based and mobile applications are the platform systems that are most widely used because they suit usage needs, which only require an internet network to connect to the information server. This server serves many users and requests, but there are still many cases of cyber attacks that disrupt the confidentiality, integrity, and availability of data and information. Therefore, increasing application security by carrying out the necessary application security assessments and the Application Security Verification Standard (ASVS) is a standard with several levels of security requirements that can be adapted to the needs of application development in Indonesia. This research develops an application security assessment information system based on ASVS by applying the Software Development Life Cycle (SDLC) development method, which consists of planning, design, development, testing, operations, and application maintenance. Based on the test results, the application developed is able to provide application security assessment instruments that meet the requirements so that application owners or developers can improve application security independently, both for web-based and mobile applications.

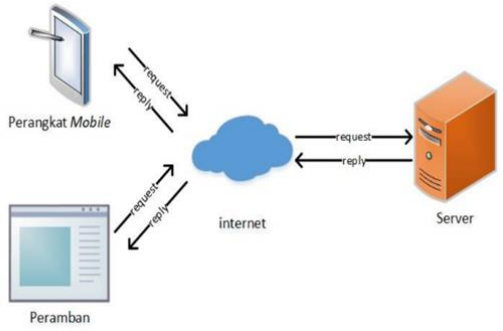
Keywords: *Mobile Application, Web-Based Application, ASVS, Application Security, SDLC.*

PENDAHULUAN

Transformasi digital yang berkembang pesat menjadi sebab perkembangan sistem informasi elektronik meningkat dengan signifikan di setiap sektor bisnis dan kehidupan. Beberapa pelayanan seperti keuangan, logistik, perdagangan, dan sebagainya menggunakan sistem informasi elektronik untuk meningkatkan kualitas layanannya. Selain itu, penerapan regulasi Sistem Pemerintahan Berbasis Elektronik (SPBE) juga menuntut setiap instansi pemerintahan melakukan digitalisasi pelayanan kepada warganya[1].

Salah satu faktor pendukung berhasilnya transformasi digital adalah perkembangan teknologi informasi dan komunikasi bidang internet yang sangat masif. Pada survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) [2], jumlah pengguna internet di Indonesia tahun 2023 sebesar 215 juta atau sekitar 78,19% dari populasi Indonesia yang sebesar 278 juta. Jumlah ini mengalami peningkatan sekitar 1,17% dari tahun sebelumnya. Peningkatan pengguna internet ini sebanding dengan peningkatan risiko serangan siber terhadap sistem informasi elektronik. Beberapa kasus serangan siber yakni kebocoran data, penipuan berupa phishing, serangan ransomware, dan sebagainya banyak terjadi sehingga diperlukan keseriusan terhadap peningkatan keamanan sistem informasi elektronik [3].

Aplikasi web dan mobile merupakan platform sistem informasi elektronik yang paling banyak digunakan dibandingkan dengan desktop [4]. Pada aplikasi web seperti pada Gambar 1, pengguna hanya perlu mengakses alamat aplikasi melalui peramban, seperti Chrome, Firefox, Safari, dan sebagainya. Sedangkan pada mobile, aplikasi dapat diakses setelah instalasi pada perangkat mobile. Persamaan dari kedua platform ini adalah setiap permintaan pengguna akan dikirimkan ke server yang akan mengolah permintaan tersebut.



Gambar 1. Cara kerja aplikasi berbasis web dan mobile

Untuk memastikan keamanan aplikasi, pemilik atau pengembang harus melakukan pengujian keamanan aplikasi sebelum diluncurkan [5]. Langkah awal pengujian yaitu penilaian identifikasi kerentanan dengan meninjau penerapan persyaratan minimum standar keamanan aplikasi. Dimas dkk. melakukan penilaian keamanan aplikasi kesehatan berbasis mobile menggunakan OWASP Top 10 [6]. OWASP Top 10 adalah 10 risiko tertinggi keamanan aplikasi paling sering ditemukan pada suatu tahun tertentu. Pada penelitian itu, 10 risiko yang digunakan yaitu penyimpanan data, komunikasi, otentikasi, dan sebagainya. Meskipun OWASP Top 10 berisi risiko yang populer, tapi masih banyak risiko yang menyebabkan kerentanan aplikasi hingga persyaratan keamanan aplikasi yang komprehensif lebih dibutuhkan.

Fernando dkk. melakukan uji keamanan aplikasi penerimaan mahasiswa baru dengan menggunakan Open Source Security Testing Methodology Model (OSSTMM) [7]. OSSTMM adalah model metodologi pengujian sistem keamanan jaringan dan aplikasi mencakup pengujian fisik, jaringan, aplikasi, lingkungan sistem, keamanan pengguna, dan

sebagainya yang bertujuan memberikan tingkat keamanan yang menyeluruh tidak hanya pada aplikasi, tapi juga lingkungan sistem dan karakteristik pengguna aplikasi.

Selain OWASP Top 10 dan OSSTMM, ada Application Security Verification Standard (ASVS) yang paling banyak digunakan karena memiliki persyaratan lebih komprehensif [8]. Seperti OWASP Top 10, ASVS diluncurkan oleh OWASP dan penelitian penilaian keamanan aplikasi menggunakan ASVS yang dilakukan oleh Tan dkk. di sektor keuangan [9]. Pada ASVS, penilaian keamanan aplikasi terdiri dari 3 tingkat berdasarkan kedalaman dari kebutuhan keamanan. Ini sesuai dengan karakteristik pengembang aplikasi Indonesia yang terdiri dari sektor UMKM hingga kritikal skala nasional. Masing-masing tingkat terdapat beberapa persyaratan yang terbagi 13 domain, yaitu autentikasi, manajemen sesi, manajemen akses, validasi input, kriptografi, penanganan eror dan pencatatan log, proteksi data, keamanan komunikasi, manajemen kode berbahaya, logika bisnis, file, keamanan API dan web service, serta keamanan konfigurasi. Setiap domain punya beberapa persyaratan keamanan aplikasi dengan total keseluruhan 286 persyaratan dipetakan pada acuan Common Weakness Enumeration (CWE) dan NIST 800-63 seperti yang ditunjukkan pada Tabel 1.1 [10].

Tabel 1. Contoh Persyaratan Keamanan Aplikasi ASVS

Domain 2. Autentikasi					
Persyaratan	**L1**	**L2**	**L3**	**CWE**	**NIST 800.63**
2.1.1. Kata sandi yang ditetapkan pengguna setidaknya terdiri dari 12 karakter, termasuk beberapa spasi yang digabungkan.	v	v	v	521	5.1.1.2
2.3.2. Pendaftaran dan penggunaan perangkat autentikasi yang disediakan pengguna didukung, seperti token FIDO.		v	v	308	6.1.3
2.2.4. Resistensi peniruan identitas terhadap phishing, seperti penggunaan Multi Factor Authentication (MFA), perangkat kriptografi, dan sebagainya.			v	308	5.2.5

METODE PENELITIAN

Sistem informasi penilaian keamanan aplikasi dikembangkan menggunakan kerangka kerja Software Development Life Cycle (SDLC) untuk memastikan kualitas dan kebutuhan pengembangan sistem informasi yang efektif, efisien, dan berkelanjutan [11].

Kerangka kerja SDLC terdiri dari 6 tahapan.

1) Analisis Kebutuhan

Tahap pertama adalah melakukan tinjauan terhadap ASVS yang meliputi domain persyaratan keamanan aplikasi dan metode penilaiannya. Kasus kerentanan dan tindakan respon terhadap kasus kerentanan yang sering terjadi juga dilakukan analisis untuk mengetahui kesesuaian antara persyaratan keamanan aplikasi yang tersedia dengan pelanggaran yang sering terjadi pada kasus kerentanan.

2) Desain

Berdasarkan kebutuhan yang telah dianalisis pada tahap sebelumnya, desain konseptual dan desain teknis dilakukan berupa diagram use-case dan diagram aktivitas. Sistem informasi yang akan dikembangkan adalah aplikasi berbasis web dan mobile untuk memudahkan penggunaannya yang tidak memerlukan instalasi dan menggunakan sumber daya perangkat.

3) Konstruksi

Konstruksi merupakan tahap yang melakukan pemrograman sistem informasi. Sistem informasi menggunakan bahasa pemrograman PHP versi 7.4 [12] dan database

MySQL versi 8.1.0 [13] dengan kerangka kerja pengembangan menggunakan Laravel versi 8 [14]. Penggunaan PHP, MySQL, dan Laravel yang bersifat open source dalam pengembangan sistem informasi punya keunggulan yaitu banyak digunakan oleh pengembang dan menyediakan fitur-fitu yang umum digunakan sehingga tidak perlu membangun sistem informasi dari awal [15].

4) Implementasi

Tahap ini melakukan instalasi program sistem informasi ke server pengujian untuk dilakukan pengujian. Server pengujian yang digunakan berbeda dengan server operasional karena hanya menggunakan server dengan sumber daya dan tingkat keamanan rendah [16].

5) Pengujian

Pengujian yang dilakukan yakni pengujian fungsional untuk mengetahui kesesuaian fungsi antara yang diharapkan dengan yang dikembangkan. Pengujian ini dilakukan di sisi pengguna dengan metode black box, yaitu penguji tidak perlu mengetahui kode program sistem informasi [17].

6) Pemeliharaan

Setelah sistem informasi dinyatakan sukses tahap pengujian, selanjutnya sistem informasi dapat digunakan secara masif di lingkungan operasional. Tahap pemeliharaan ini merupakan tahap melakukan pemantauan aplikasi, perbaikan jika terdapat masalah, dan peningkatan jika diperlukan.

Gambar 2. Tahap SDLC Pengembangan Sistem Informasi Penilaian Keamanan Aplikasi

Penggunaan enkripsi data tingkat tinggi, seperti Standar Enkripsi Tinggi (AES) dengan kunci 256-bit, memberikan perlindungan kuat terhadap data baik saat dikirim maupun disimpan. Selain itu, sistem deteksi dan pencegahan intrusi (IDS/IPS) berbasis pembelajaran mesin memungkinkan deteksi pola

serangan baru secara real-time, sementara autentikasi multifaktor (MFA) memastikan hanya pengguna sah yang dapat mengakses data perusahaan [18].

Dengan kemampuan belajar dari data, algoritma machine learning seperti Random Forest, Support Vector Machine (SVM), dan Neural Networks dapat otomatis mendeteksi pola serangan yang berpotensi membahayakan. Algoritma ini memproses data historis untuk mengidentifikasi pola anomali atau serangan yang sulit dideteksi metode konvensional, sehingga meningkatkan respons keamanan secara real-time [19].

HASIL DAN PEMBAHASAN

Desain Sistem Informasi

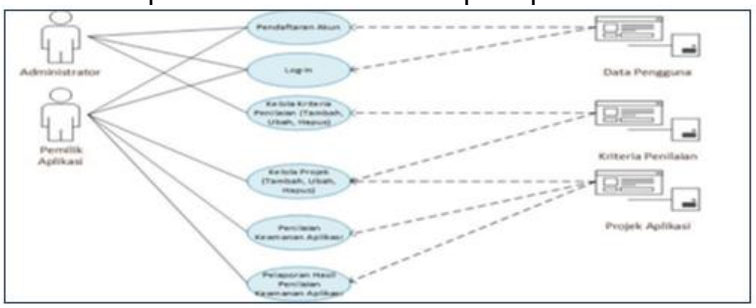
Dalam pengembangan sistem informasi ini ada 2 desain penilaian keamanan aplikasi, pertama diagram use-case adalah diagram yang mempresentasikakan hubungan

antara peran-peran pengguna dengan fitur-fitur yang dibutuhkan pada sistem informasi [20]. Dan kedua diagram aktivitas adalah diagram yang merepresentasikan keterkaitan antara proses-proses yang berjalan secara berurutan pada sistem informasi [21].

Desain diagram use-case dan diagram aktivitas dari sistem informasi penilaian keamanan aplikasi adalah sebagai berikut.

1) Diagram Use-Case

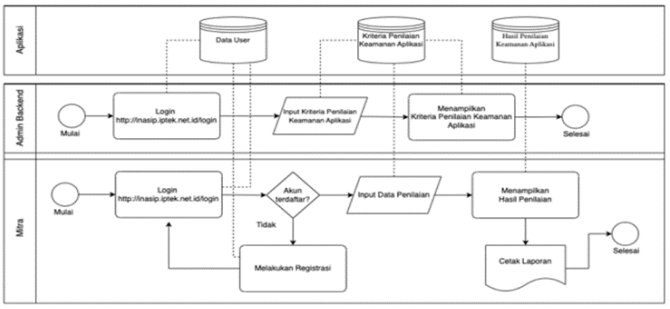
Terdapat dua peran pengguna pada sistem informasi penilaian keamanan aplikasi, yaitu administrator dan mitra. Administrator adalah peran yang memiliki kendali terhadap semua fitur aplikasi, seperti pengelolaan pengguna, persyaratan keamanan aplikasi, dan projek. Sedangkan mitra adalah pengembang atau pemilik aplikasi yang akan melakukan penilaian keamanan aplikasi.Selanjutnya, kedua peran ini dihubungkan dengan hak akses fitur-fitur yang dibutuhkan pada sistem informasi seperti pada Gambar 3.



Gambar 3. Diagram Use-Case Sistem Informasi Penilaian Keamanan Aplikasi

2) Diagram Aktivitas

Diagram aktivitas menggambarkan urutan hubungan proses antar fitur-fitur dari diagram use-case, yaitu modul autentikasi, modul projek, modul identifikasi, modul penilaian, dan modul pelaporan, seperti pada Gambar 4.



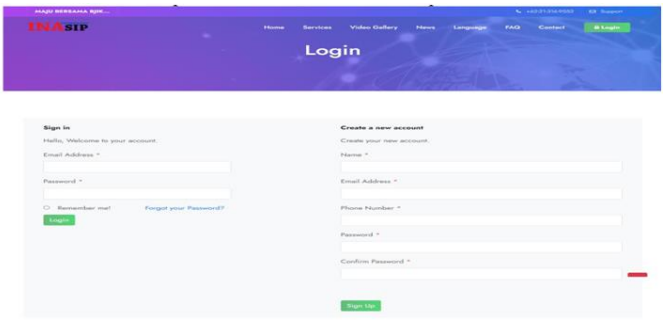
Gambar 4. Diagram Aktivitas Sistem Informasi Penilaian Keamanan Aplikasi

A. Implementasi

Berikut adalah modul-modul yang telah dilakukan implementasi

1) Modul Autentikasi

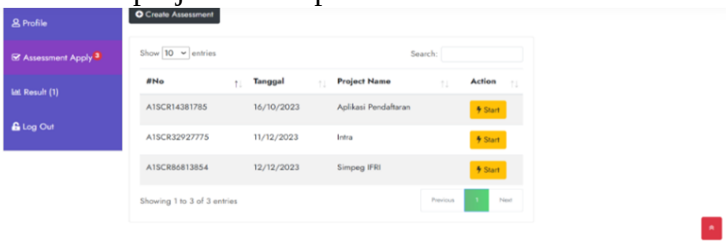
Modul melakukan verifikasi pada pengguna bahwa pengguna sah melakukan akses terhadap sistem informasi. Autentikasi yang digunakan berupa kombinasi antara alamat e-mail dengan password dan harus membuat akun baru jika pengguna baru pertama kali menggunakan sistem informasi, Berikut Tampilan modul autentikasi pada Gambar 5.



Gambar 5 Modul Autentikasi

2) Modul Projek

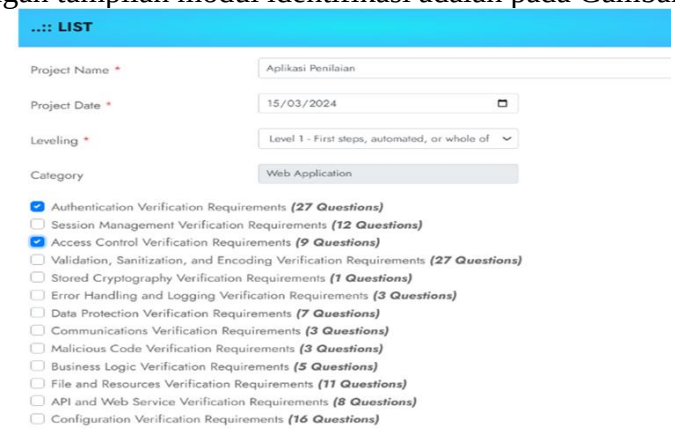
Modul yang berfungsi menampilkan riwayat penilaian aplikasi yang telah dibuat, baik yang telah selesai dilakukan penilaian ataupun yang belum selesai dilakukan penilaian. Tampilan modul projek adalah pada Gambar 6.



Gambar 6. Modul Projek

3) Modul Identifikasi

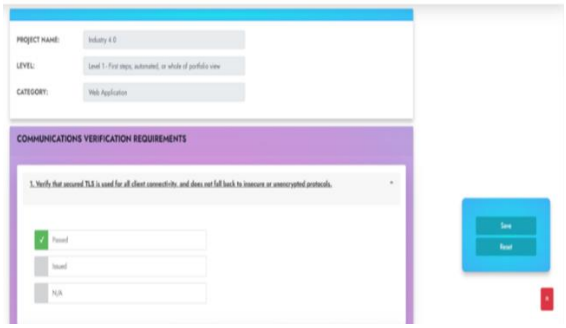
Modul yang tampil jika pengguna membuat penilaian aplikasi pertama dan berfungsi melakukan identifikasi aplikasi yang akan dilakukan penilaian, seperti nama aplikasi, tanggal pembuatan, tingkat keamanan, jenis aplikasi, dan domain persyaratan yang digunakan kali dengan tampilan modul identifikasi adalah pada Gambar 7.



Gambar 7 Modul Identifikasi

4) Modul Penilaian

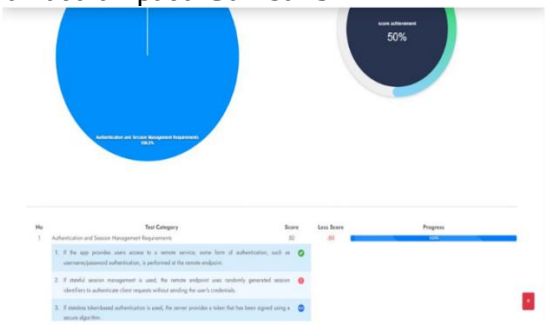
Modul yang berfungsi melakukan penyesuaian nilai terhadap persyaratan yang dibutuhkan. Penilaian terdiri dari 3 nilai, yaitu passed jika sesuai, issued jika tidak sesuai, dan N/A jika tidak dapat dilakukan penilaian. Tampilan modul penilaian adalah pada Gambar 8.



Gambar 8 Modul Penilaian

5) Modul Pelaporan

Berfungsi menampilkan nilai hasil penilaian keamanan aplikasi secara keseluruhan. Tampilan modul pelaporan adalah pada Gambar 9



Gambar 9 Modul Pelaporan

B. Pengujian Fungsional

Tahap yang berfokus dalam pengujian fungsional bertujuan memverifikasi apakah hasil yang diperoleh sesuai dengan apa yang diharapkan. Pengujian yang dilakukan merupakan metode black box, yaitu penguji tidak perlu mengetahui kode program sistem informasi [22]. Hasil pengujian fungsional pada masing-masing modul yang telah dibangun adalah seperti pada Tabel 2.

Tabel 2 Hasil Pengujian Fungsional

Nomor	Modul	Hasil yang Diharapkan	Hasil Pengujian	Keterangan
1	Autentikasi	1. Jika kombinasi alamat *e-mail* dan *password* sesuai, maka pengguna berhasil masuk ke dalam sistem. 2. Jika kombinasi alamat *e-mail* dan *password* tidak sesuai, maka pengguna tidak dapat masuk ke dalam sistem. 3. Sistem dapat melakukan pendaftaran akun.	1. Berhasil masuk ke dalam sistem ketika kombinasi alamat e-mail dan password sesuai. 2. Tidak dapat masuk ke dalam sistem ketika kombinasi alamat e-mail dan password tidak sesuai. 3. Sistem dapat melakukan pendaftaran akun.	sesuai

Nomor	Modul	Hasil yang Diharapkan	Hasil Pengujian	Keterangan
2	Projek	1. Sistem dapat menampilkan semua projek yang telah dibuat. 2. Sistem dapat membuat projek baru. 3. Sistem dapat membuka projek yang telah dibuat.	1. Sistem berhasil menampilkan semua projek yang telah dibuat. 2. Sistem berhasil membuat projek baru. 3. Sistem berhasil membuka projek yang telah dibuat.	sesuai
3	Identifikasi	1. Sistem dapat menuliskan nama projek. 2. Sistem dapat menentukan tanggal projek. 3. Sistem dapat menentukan tingkat dan domain persyaratan keamanan aplikasi. 4. Sistem dapat menyimpan projek baru.	1. Sistem berhasil menuliskan nama projek. 2. Sistem berhasil menentukan tanggal projek. 3. Sistem berhasil menentukan tingkat dan domain persyaratan keamanan aplikasi. 4. Sistem berhasil menyimpan projek baru	sesuai
4	Penilaian	1. Sistem dapat memilih pilihan jawaban yang sesuai. 2. Sistem dapat mengubah jawaban. 3. Sistem dapat menghapus jawaban. 4. Sistem dapat mengirim jawaban.	1. Sistem berhasil memilih jawaban yang sesuai. 2. Sistem berhasil mengubah jawaban. 3. Sistem berhasil menghapus jawaban. 4. Sistem berhasil mengirim jawaban.	sesuai
5	Pelaporan	1. Sistem dapat menampilkan nilai keamanan aplikasi. 2. Sistem dapat menampilkan grafik hasil penilaian. 3. Sistem dapat memberikan rekomendasi peningkatan keamanan aplikasi.	1. Sistem berhasil menampilkan nilai keamanan aplikasi. 2. Sistem berhasil menampilkan grafik hasil penilaian. 3. Sistem berhasil memberikan rekomendasi peningkatan keamanan aplikasi.	sesuai

Berdasarkan Tabel 2, Pengujian fungsional yang telah dilakukan semua modul aplikasi dengan metode black box maka diperoleh hasil semua modul telah sesuai antara kebutuhan dengan implementasinya. Oleh karena itu, sistem informasi penilaian keamanan aplikasi telah siap digunakan oleh para pemilik atau pengembang aplikasi untuk meningkatkan keamanannya.

KESIMPULAN

Pengembangan sistem informasi penilaian keamanan aplikasi menggunakan metode SDLC terdiri dari tahap analisis kebutuhan, desain, konstruksi, implementasi, pengujian, dan pemeliharaan. Persyaratan ini mengacu pada ASVS yang sesuai untuk aplikasi web dan mobile. Desain pengembangan ini berupa diagram use-case dan diagram aktivitas yang membangun 5 modul aplikasi, yaitu autentikasi, projek, identifikasi, penilaian, dan pelaporan. Kemudian pengujian fungsional di sisi pengguna dengan menggunakan metode black box akan dilakukan berdasarkan hasil pengujian sistem informasi dengan penilaian keamanan aplikasi yang telah dikembangkan sudah sesuai kebutuhan dan persyaratan, baik pengguna maupun regulasi. Maka dari itu, sistem informasi dapat digunakan pemilik atau pengembang aplikasi untuk meningkatkan keamanan aplikasi secara mandiri.

DAFTAR PUSTAKA

Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.

"Survei Pengguna Internet Indonesia Tahun 2023". Accessed: 3 May 2024. [Online]. Available:https://survei.apjii.or.id/.

Muhammad Lugas Pribady. "29 Juta Serangan Siber Diblokir di Indonesia Selama 2023". Accessed: 3May 2024. [Online]. Available: https://inet.detik.com/security/d-7214588/29-juta-serangan-siber-diblokir- di-indonesia-selama-2023.

Dwiyatno, Saleh, et al. "Aplikasi Sistem Informasi Akademik Berbasis Web". PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer, Vol. 9, No.2, (2022): 83-89.

Ghozali, Bahrun, Kusrini Kusrini, and Sudarmawan Sudarmawan. "Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp (Open Web Application Security Project) Untuk Penilaian Risk Rating". Creative Information Technology Journal 4.4 (2019): 264-275.

Dimas Febriyan Priambodo, Guntur Satria Ajie, Hendy Aulia Rahman, Aldi Cahya Fajar Nugraha, Aulia Rachmawati, dan Marcella Risky Avianti, "Mobile Health Application Security Assessment based on OWASP Top 10 Mobile", International Conference on Information

Technology System and Innovation (ICITSI), 8-9 November 2022, Bandung.
Yendri Ikhlas Fernando dan Rahmad Abdillah, “Security Testing Sistem Penerimaan Mahasiswa Baru Universitas XYZ Menggunakan Open Source Security Testing Methodology Model (OSSTMM)”, Jurnal CoreIT, Vol. 2, No. 1, Juni 2016, ISSN: 2460-738X.
“OWASP Application Security Verification Standard”. Accessed: 3 May 2024. [Online]. Available: https://owasp.org/www-project-application-security-verification-standard/ .
Vincent Tan, Carmen Cheh, dan Binbin Chen, “From Application Security Verification Standard to Regulation Compliance: A Case Study in Financial Services Sector”, International Symposium on Software Reliability Engineering Workshop (ISSREW), 2021.
Shao-Fang Wen dan Basel Katt, “A Quantitative Security Evaluation and Analysis Model for Web Applications based on OWASP Application Security Verification Standard”, Journal of Computers and Security, 2023.
Yoyok Seby Dwanoko, “Implementasi Software Development Life Cycle (SDLC) dalam Penerapan Pembangunan Aplikasi Perangkat Lunak”, Jurnal Teknologi Informasi: Teori, Konsep, dan Implementasi, Vol. 7, No. 2, 2016.
PHP: Hypertext Preprocessor. Available: https://www.php.net/.
MySQL. Available: https://www.mysql.com/.
Laravel. Available: https://laravel.com/
Alfin Adi Surya dan Imam Haromain, “Rancang Bangun Website Lelang Mobil Menggunakan Framework CodeIgniter 3 pada PT. ABC”, Jurnal Teknologi Terpadu, Vol. 9, No. 2, Tahun 2023.
Hermawan, Adam. “Sistem informasi manajemen dan tracking berkas (studi kasus: Ptsp kecamatan kebon jeruk)”. JUSIBI (Jurnal Sistem Informasi dan Bisnis) 1.2 (2019).
Fahrezi, Ahmad, et al. “Pengujian Black Box Testing pada Aplikasi Inventori Barang Berbasis Web di PT. AINO Indonesia”. LOGIC: Jurnal Ilmu Komputer dan Pendidikan 1.1 (2022): 1-5.
Mitigasi Risiko Cybercrime Terhadap Keamanan Sistem Komputasi Awan Pada Perusahaan D Aryani, ED Absharina - Jurnal Cakrawala Akademika, 2024 Related articles
IMPLEMENTASI AI-POWERED INTRUSION DETECTION SYSTEMS UNTUK MENDETEKSI ANCAMAN KEAMANAN PADA BIG DATA DP Amanda, ED Absharina - Simtek: jurnal sistem informasi dan teknik komputer, 2025 Related articles
Prima, Nadya, and Ahmaddul Hadi. “Rancang Bangun Sistem Informasi E-Commerce di UKM Aneka Kebaya Berbasis Web (Studi Kasus: Baju Kebaya dan Rok Batik di Koto Tangah Simalanggang)”. Jurnal Pendidikan Tambusai 6.1 (2022): 1029-1035.
Alyssa Walker. “Web Server vs Application Server – Difference Between Them”. Accessed: 19 May 2024. [Online]. Available: https://www.guru99.com/web-server-vs-application-server.html.
Riko Rinaldiansyah Nugraha, Giri Purnama, “Pengembangan Aplikasi Payroll Berbasis Web pada Institusi Perguruan Tinggi (Studi Kasus di Universitas XYZ)”, JTSI, Vol. 4, No. 2, September 2023: 335-345.