INDEXIA : Informatic and Computational Intelligent Journal
Vol.6, No.1, Mei 2024, hlm. 62-71
P-ISSN : 2657-0424
E-ISSN : 2657-0432

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

Samsudiat[1)], Hartanto Kurniawan[2,*)], Cahyono Nugroho[3)]
[1,2,3)]Pusat Riset Kecerdasan Artifisial dan Keamanan Siber, Badan Riset dan Inovasi Nasional
Gedung 254, KST BJ Habibie, Setu, Tangerang Selatan, Banten, 15314
e-mail: samsudiat@brin.go.id[1)], hartanto.kurniawan@brin.go.id[2)], cahyono.nugroho@brin.go.id[3)]
*corresponding author

(Naskah masuk : 7 April 2024 Diterima untuk diterbitkan : 21 Mei 2024)

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 banyak pengguna 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*

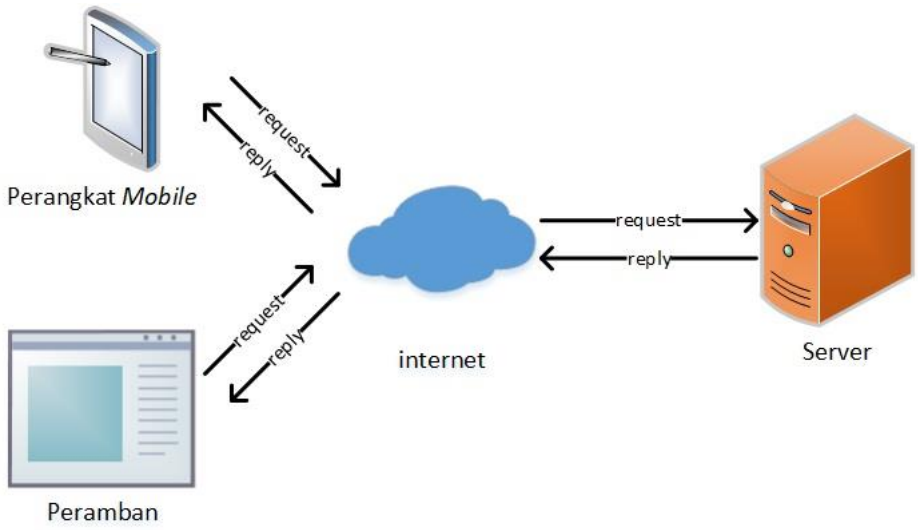
I. PENDAHULUAN

Pesatnya transformasi digital menyebabkan pengembangan sistem informasi elektronik mengalami peningkatan yang signifikan di setiap sektor bisnis dan kehidupan. Beberapa pelayanan seperti keuangan, logistik, perdagangan, dan sebagainya telah menggunakan sistem informasi elektronik untuk meningkatkan kualitas layanannya. Selain itu, penerapan regulasi terkait Sistem Pemerintahan Berbasis Elektronik (SPBE) juga menuntut setiap instansi pemerintahan untuk melakukan digitalisasi pelayanan

kepada warganya [1].

Salah satu faktor pendukung keberhasilan transformasi digital tersebut adalah perkembangan teknologi informasi dan komunikasi di bidang internet yang sangat masif. Berdasarkan survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) [2], jumlah pengguna internet di Indonesia pada tahun 2023 adalah 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 seperti kebocoran data, penipuan berupa phishing, serangan ransomware, dan sebagainya telah banyak terjadi sehingga diperlukan keseriusan terhadap peningkatan keamanan dari sistem informasi elektronik [3].

Aplikasi berbasis *web* dan *mobile* merupakan platform sistem informasi elektronik yang paling banyak digunakan dibandingkan dengan yang berbasis *desktop* [4]. Aplikasi tersebut banyak digunakan karena kemudahan penggunaannya dimana pengguna dapat mengakses aplikasi dimana pun dan kapan pun saat terhubung dengan internet. Pada aplikasi berbasis *web* seperti pada Gambar 1.1, pengguna hanya perlu mengakses alamat aplikasi melalui peramban, seperti Chrome, Firefox, Safari, dan sebagainya. Sedangkan pada aplikasi berbasis *mobile*, aplikasi dapat diakses setelah dilakukan instalasi pada perangkat mobile. Persamaan dari kedua *platform* ini adalah setiap permintaan pengguna akan dikirimkan ke server yang akan mengolah permintaan tersebut. Server tersebut tentu terhubung dengan banyak pengguna dan banyak permintaan sehingga keamanan dari aspek kerahasiaan, keutuhan, dan ketersediaan data dan informasi harus menjadi prioritas utama bagi pemilik dan pengembang aplikasi.



Gambar 1.1 Cara kerja aplikasi berbasis web dan mobile

Dalam rangka memastikan keamanan aplikasi, pemilik atau pengembang aplikasi perlu melakukan pengujian keamanan aplikasi sebelum aplikasi diluncurkan [5]. Langkah awal dari pengujian ini adalah melakukan penilaian identifikasi kerentanan dengan meninjau penerapan dari persyaratan minimum standar keamanan aplikasi. Beberapa penelitian terkait penilaian keamanan aplikasi ini telah dilakukan. Dimas dkk. melakukan penilaian keamanan aplikasi kesehatan berbasis mobile dengan menggunakan OWASP Top 10 [6]. OWASP Top 10 merupakan 10 risiko tertinggi keamanan aplikasi yang paling sering ditemukan pada suatu tahun tertentu. Pada penelitian tersebut, 10 risiko yang digunakan seperti, penyimpanan data, komunikasi, otentikasi, dan sebagainya. Meskipun OWASP Top 10 berisi risiko yang populer, tetapi masih terdapat banyak risiko yang dapat menyebabkan kerentanan pada aplikasi sehingga persyaratan keamanan aplikasi yang komprehensif lebih dibutuhkan.

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

keamanan pengguna, dan sebagainya yang bertujuan untuk memberikan tingkat keamanan yang menyeluruh tidak hanya aplikasi, tetapi juga lingkungan sistem dan karakteristik pengguna aplikasi. Pada pengembangan sistem informasi saat ini yang cepat dan tepat, kebanyakan pemilik aplikasi menggunakan server pihak ketiga atau tidak mencakup aspek fisik dan lingkungan sistem aplikasi sehingga menyebabkan OSSTMM tidak dapat diterapkan secara optimal sebagai standar keamanan aplikasi.

Selain OWASP Top 10 dan OSSTMM tersebut, terdapat *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 telah dilakukan oleh Tan dkk. di sektor keuangan [9]. Pada ASVS, penilaian keamanan aplikasi terdiri dari 3 tingkat berdasarkan kedalaman dari kebutuhan keamanan. Hal ini sesuai dengan karakteristik pengembang aplikasi di Indonesia yang terdiri dari sektor UMKM hingga sektor kritikal skala nasional. Masing-masing tingkat tersebut terdapat beberapa persyaratan yang terbagi menjadi 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 tersebut memiliki beberapa persyaratan keamanan aplikasi dengan total keseluruhan sebanyak 286 persyaratan yang juga dipetakan pada acuan *Common Weakness Enumeration* (CWE) dan NIST 800-63 seperti yang ditunjukkan pada Tabel 1.1 [10].

Tabel 1.1 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

Berdasarkan tinjauan penelitian sebelumnya, terdapat beberapa standar keamanan aplikasi yang tersedia dan *Application Security Verification Standard* (ASVS) yang diterbitkan oleh OWASP merupakan standar yang paling banyak digunakan karena memiliki tingkatan persyaratan keamanan aplikasi yang dapat disesuaikan dengan kebutuhan dari pengembangan aplikasi. Selain itu, ASVS dapat digunakan berbeda pada aplikasi berbasis *web* dan berbasis *mobile* dengan persyaratan-persyaratan yang sesuai dengan platform yang digunakan. Oleh karena itu, penelitian ini bertujuan untuk membangun sistem informasi penilaian keamanan aplikasi untuk aplikasi baik berbasis *web* maupun berbasis *mobile*.

II. METODE PENELITIAN

Sistem informasi penilaian keamanan aplikasi dikembangkan dengan 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 sebagai berikut.

1) Tahap Analisis Kebutuhan
   Tahap pertama pengembangan sistem informasi penilaian keamanan aplikasi adalah melakukan tinjauan terhadap ASVS yang meliputi domain persyaratan keamanan aplikasi dan metode penilaiannya. Selain itu, 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) Tahap Desain

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

3) Tahap Konstruksi
Selanjutnya, tahap konstruksi merupakan tahap yang melakukan pemrograman sistem informasi. Sistem informasi menggunakan bahasa pemrograman PHP versi 7.4 [18] dan database MySQL versi 8.1.0 [19] dengan kerangka kerja pengembangan menggunakan Laravel versi 8 [20]. Penggunaan PHP, MySQL, dan Laravel yang bersifat *open source* dalam pengembangan sistem informasi memiliki keunggulan yaitu banyak digunakan oleh pengembang dan menyediakan fitur-fitur yang umum digunakan sehingga tidak perlu membangun sistem informasi dari awal [12].

4) Tahap Implementasi
Tahap implementasi merupakan tahap yang melakukan instalasi program sistem informasi ke server pengujian untuk dilakukan pengujian. Server pengujian yang digunakan adalah berbeda dengan server operasional karena hanya menggunakan server dengan sumber daya dan tingkat keamanan yang rendah [13].

5) Tahap Pengujian
Pengujian yang dilakukan adalah pengujian fungsional yang merupakan pengujian untuk mengetahui kesesuaian fungsi antara yang diharapkan dengan yang telah dikembangkan. Pengujian ini merupakan pengujian yang dilakukan di sisi pengguna dengan metode *black box*, yaitu penguji tidak perlu mengetahui kode program sistem informasi [14].

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

Gambar 2.1 Tahap *SDLC* Pengembangan Sistem Informasi Penilaian Keamanan Aplikasi

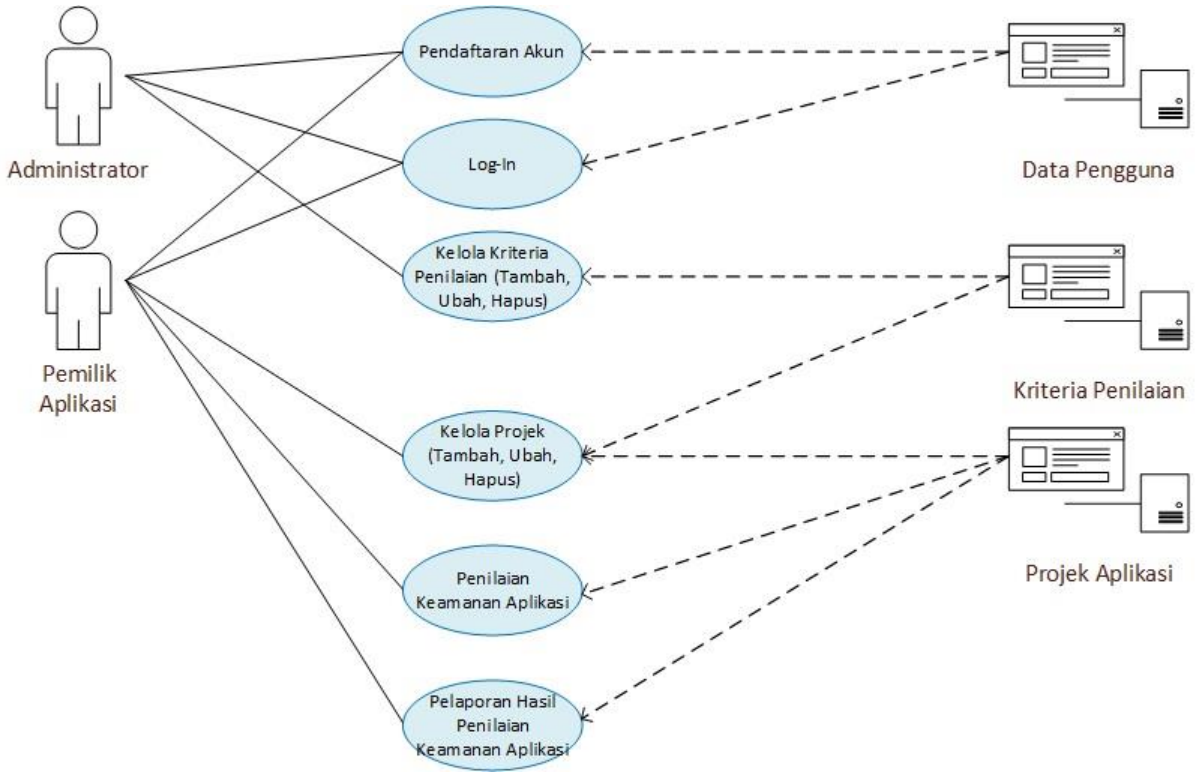
III. HASIL DAN PEMBAHASAN

3.1 Desain Sistem Informasi

Terdapat 2 desain dalam pengembangan sistem informasi penilaian keamanan aplikasi, yaitu diagram *use-case* dan diagram aktivitas. Diagram *use-case* merepresentasikan hubungan antara peran-peran pengguna dengan fitur-fitur yang dibutuhkan pada sistem informasi [15]. Sedangkan diagram aktivitas merepresentasikan keterkaitan antara proses-proses yang berjalan secara berurutan pada sistem informasi [16]. Desain diagram *use-case* dan diagram aktivitas dari sistem informasi penilaian keamanan aplikasi adalah sebagai berikut.

1) Diagram *Use-Case*

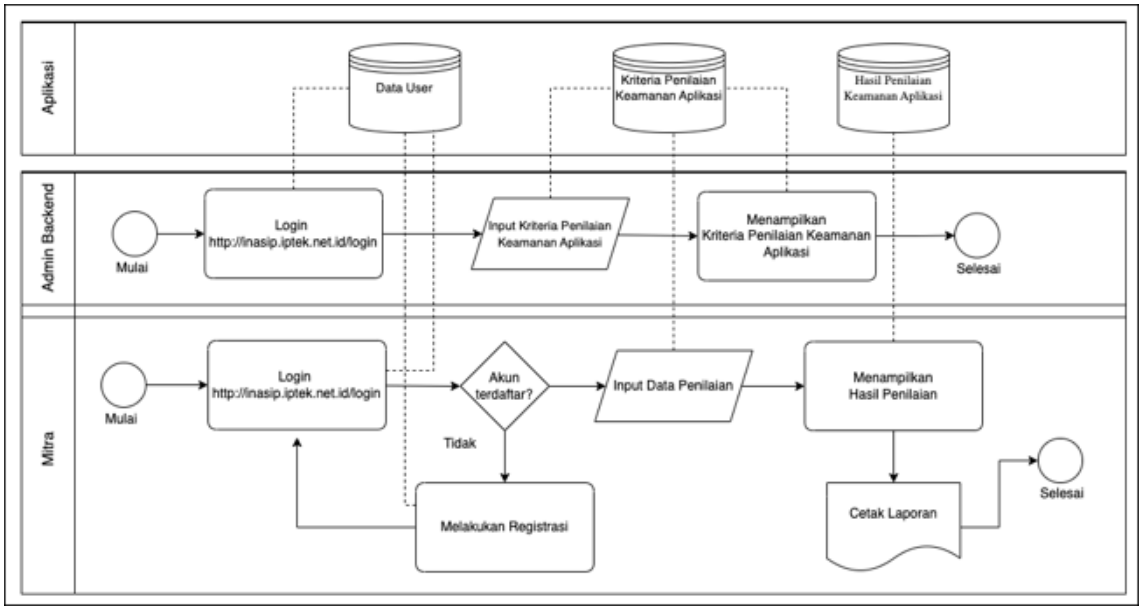
Terdapat dua peran pengguna pada sistem informasi penilaian keamanan aplikasi, yaitu administrator dan mitra. Administrator adalah peran yang memiliki kendali terhadap semua fitur aplikasi, seperti pengelolaan pengguna, pengelolaan persyaratan keamanan aplikasi, dan pengelolaan projek. Sedangkan mitra 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 3.1.



Gambar 3.1 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 3.2.



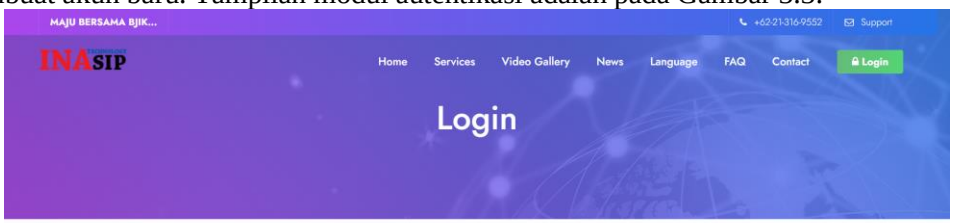
Gambar 3.2 Diagram Aktivitas Sistem Informasi Penilaian Keamanan Aplikasi

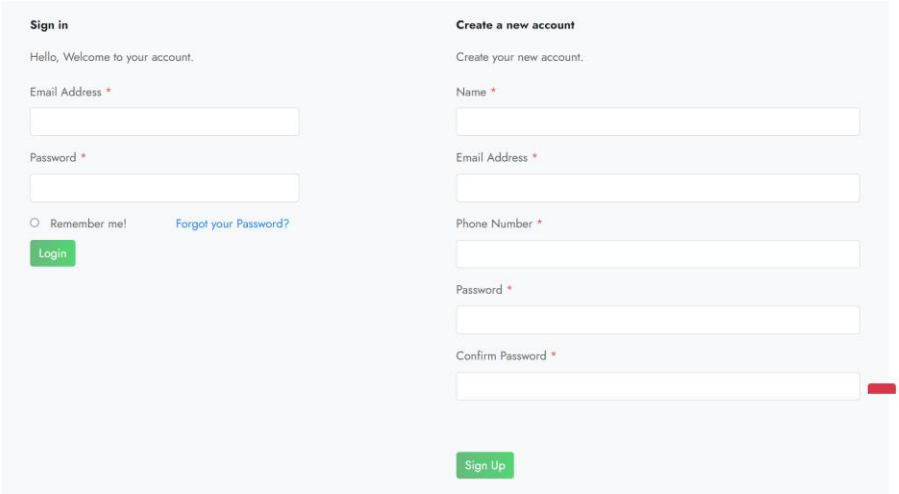
B. Implementasi

Modul-modul yang telah dilakukan implementasi adalah sebagai berikut.

1) Modul Autentikasi

Modul Autentikasi berfungsi untuk melakukan verifikasi pengguna bahwa pengguna adalah sah untuk melakukan akses terhadap sistem informasi. Autentikasi yang digunakan berupa kombinasi antara alamat *e-mail* dengan *password*. Jika pengguna pertama kali menggunakan sistem informasi, maka harus membuat akun baru. Tampilan modul autentikasi adalah pada Gambar 3.3.

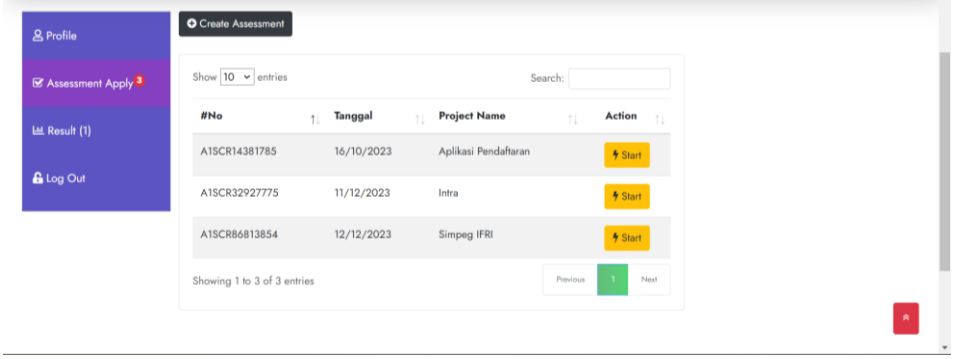




Gambar 3.3 Modul Autentikasi

2) Modul Projek

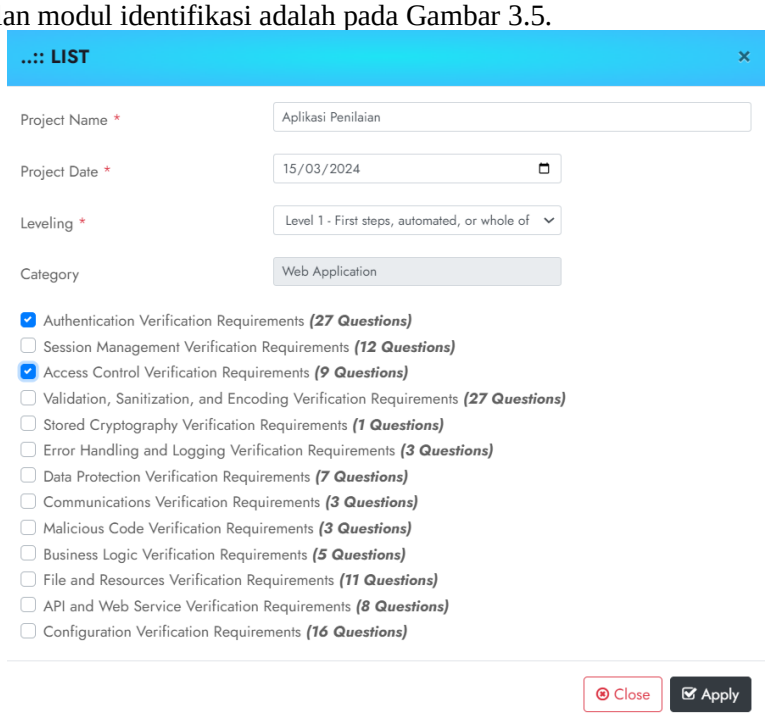
Modul Projek berfungsi untuk menampilkan riwayat penilaian aplikasi yang telah dibuat, baik yang telah selesai dilakukan penilaian ataupun yang belum selesai dilakukan penilaian. Tampilan modul projek adalah pada Gambar 3.4.



Gambar 3.4 Modul *Projek*

3) Modul Identifikasi

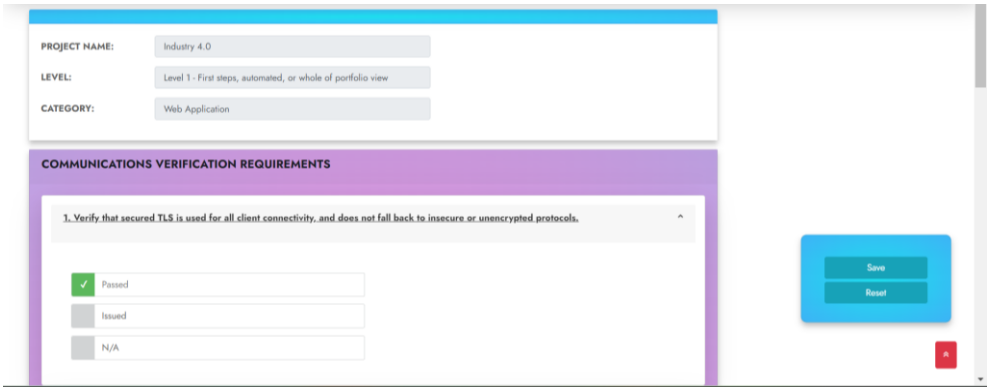
Modul Identifikasi berfungsi untuk melakukan identifikasi aplikasi yang akan dilakukan penilaian, seperti nama aplikasi, tanggal pembuatan, tingkat keamanan, jenis aplikasi, dan domain persyaratan yang digunakan. Modul ini tampil ketika pengguna membuat penilaian aplikasi pertama kali dengan tampilan modul identifikasi adalah pada Gambar 3.5.



Gambar 3.5 Modul Identifikasi

4) Modul Penilaian

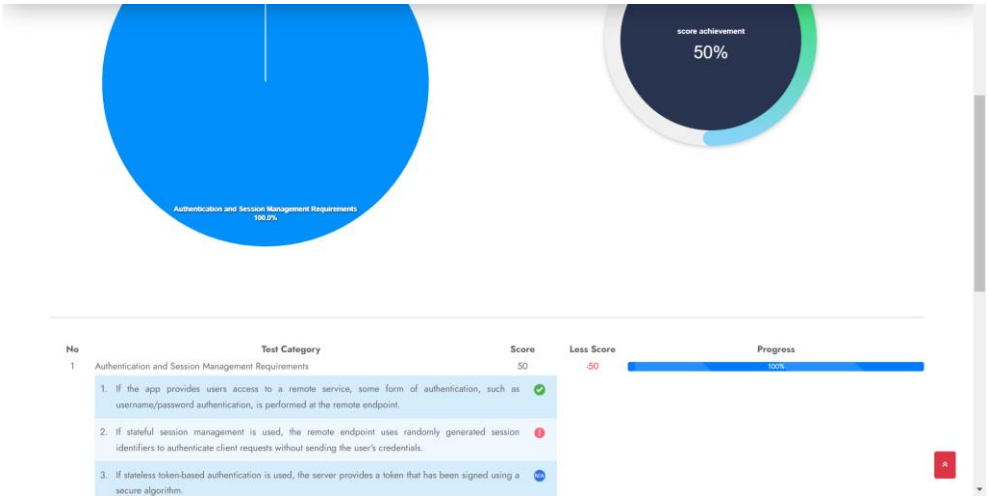
Modul Penilaian berfungsi untuk melakukan penilaian kesesuaian terhadap persyaratan yang dibutuhkan. Penilaian terdiri dari 3 nilai, yaitu *passed* jika sesuai, *issued* jika tidak sesuai, dan *N/A* jika tidak dapat dilakukan penilaian. Tampilan modul penilaian adalah pada Gambar 3.6



Gambar 3.6 Modul Penilaian

5) Modul Pelaporan

Modul Pelaporan berfungsi untuk menampilkan nilai hasil penilaian keamanan aplikasi secara keseluruhan. Tampilan modul pelaporan adalah pada Gambar 3.7



Gambar 3.7 Modul Pelaporan

C. Pengujian Fungsional

Tahap ini berfokus pada pengujian fungsional yang bertujuan untuk memverifikasi apakah hasil yang diperoleh dari sistem sesuai dengan apa yang diharapkan. Pengujian ini merupakan pengujian yang dilakukan di sisi pengguna dengan metode *black box*, yaitu penguji tidak perlu mengetahui kode program sistem informasi [17]. Hasil pengujian fungsional pada masing-masing modul yang telah dibangun adalah seperti pada Tabel 3.1

Tabel 3.1 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 3.1, semua modul aplikasi telah dilakukan pengujian fungsional dengan metode *black box* dan hasilnya adalah 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.

IV. KESIMPULAN

Pengembangan sistem informasi penilaian keamanan aplikasi telah dilakukan dengan menggunakan metode SDLC yang terdiri dari tahap analisis kebutuhan, desain, konstruksi, implementasi, pengujian, dan pemeliharaan. Persyaratan-persyaratan yang terdapat pada sistem informasi ini mengacu pada ASVS yang sesuai untuk aplikasi web dan mobile. Desain pengembangan sistem informasi ini berupa diagram use-case dan diagram aktivitas yang membangun 5 modul aplikasi, yaitu modul autentikasi, modul projek, modul identifikasi, modul penilaian, dan modul pelaporan. Selanjutnya, sistem informasi dilakukan pengujian fungsional di sisi pengguna dengan menggunakan metode *black box*. Berdasarkan hasil pengujian fungsional dari masing-masing modul dapat diketahui bahwa sistem informasi penilaian

keamanan aplikasi yang telah dikembangkan adalah telah sesuai dengan kebutuhan dan persyaratan, baik pengguna maupun regulasi. Oleh karena itu, sistem informasi dapat digunakan oleh pemilik atau pengembang aplikasi untuk meningkatkan keamanan aplikasi secara mandiri.

DAFTAR PUSTAKA

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

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

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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] "OWASP Application Security Verification Standard". Accessed: 3 May 2024. [Online]. Available: https://owasp.org/www-project-application-security-verification-standard/.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] Hermawan, Adam. "Sistem informasi manajemen dan tracking berkas (studi kasus: Ptsp kecamatan kebon jeruk)". JUSIBI (Jurnal Sistem Informasi dan Bisnis) 1.2 (2019).

[17] 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.

[18] PHP: Hypertext Preprocessor. Available: https://www.php.net/.

[19] MySQL. Available: https://www.mysql.com/.

[20] Laravel. Available: https://laravel.com/.