ANALISIS IT SECURITY ASSESMENT PADA APLIKASI DATABALIKAN

Noor Vika Hizviani

Universitas Gunadarma, noorvika@staff.gunadarma.ac.id

ABSTRAK

Analisis IT Security Assessment pada Aplikasi DataBalikan merupakan sebuah penelitian yang bertujuan untuk mengevaluasi keamanan sistem pada aplikasi DataBalikan. Dalam era digital yang terus berkembang, perlindungan data dan sistem informasi menjadi semakin penting, terutama dengan meningkatnya ancaman keamanan cyber. Penelitian ini bertujuan untuk memahami tingkat keamanan aplikasi DataBalikan serta mengidentifikasi potensi kerentanan yang mungkin ada dalam sistemnya. Metode analisis IT Security Assessment digunakan untuk mengevaluasi kekuatan dan kelemahan sistem, termasuk dalam hal keamanan data, akses pengguna, dan perlindungan terhadap serangan cyber. Hasil penelitian ini memberikan pemahaman yang lebih baik tentang keamanan aplikasi DataBalikan serta rekomendasi perbaikan yang dapat dilakukan untuk meningkatkan tingkat keamanan dan mengurangi risiko keamanan cyber. Penelitian ini diharapkan dapat memberikan kontribusi bagi pengembangan sistem informasi yang lebih aman dan dapat dipercaya di masa depan.

Kata kunci: *IT Security Assessment, keamanan sistem, aplikasi DataBalikan, kerentanan sistem, perlindungan data.*

PENDAHULUAN

Penerapan TIK pada lembaga pemerintahan untuk mendukung layanan publik, memudahkan dan mengakses ke dalam big data yang dimiliki oleh pemerintah. Hak akses ke sumber data pemerintah, menyebabkan akses ke sistem atau aplikasi tersebut sangat rentan dengan gangguan dalam dunia cyber. Keamanan informasi sangat vital dalam penggunaan sistem atau aplikasi harus segera ditingkatkan, agar kebocoran data dan informasi oleh pihak yang belum berhak untuk menggunakannya dapat dicegah.

Penerapan dari *e-goverment* salah satunya adalah dengan adanya KTP el. Pada standar pelayanan dalam sebuah unit pelayanan harus berdasarkan UU nomor 25 tahun 2009 tentang pelayanan publik. Dimana pelayanan merupakan rangkaian aktifitas yang dapat dirasakan melalui hubungan antara penerima dan pemberi layanan dengan menggunakan organisasi sebagai peralatan atau wadah dalam memberi layanan. Dengan memanfaatkan Teknologi Informasi sebagai alat bantu untuk mengembangkan konsep e-goverment yang berkualitas untuk Kementrian Dalam Negeri. (Oman Somantri1, Indra Dwi Hasta, 2017). Penyelenggaraan administrasi kependudukan melalui optimalisasi layanan kependudukan kepada masyarakat merupakan salah satu hal strategis berdasarkan Peraturan Menteri Dalam Negeri Nomor 67 Tahun 2020 tentang Rencana Strategis (Renstra) Kementrian Dalam Negeri Tahun 2020-2024. Aplikasi databalikan dikembangkan pertama kali pada tahun 2017, yang bertujuan membangun ”Big data” dari lembaga pengguna yang memanfaatkan elemen data dari KTP el yang dimiliki oleh Ditjen dukcapil, sebagai *feedback* lembaga pengguna harus memberikan informasi yang dimiliki berdasarkan elemen data yang ada. Aplikasi databalikan akan menerima data unik dari lembaga pengguna seperti nomor selluler, nomor rekening nasabah pada bank, nomor kepesertaan, nomor kepemilikan dan sebagainya. Untuk mendapatkan

feedback Direktorat Jendral Kependudukan dan Pencatatan Sipil sebagai hak untuk mendapatkan data balikan dari lembaga pengguna yang sudah tertuang dalam perjanjian kerjasama yang sudah tertuang pada petunjuk teknis dengan lembaga pengguna.

Sistem informasi milik pemerintah yang memberikan layanan kepada publik sangat rentan akan menyusupan atau virus dari manapun, apapun jenis aplikasinya yang terhubung dengan internet, memiliki kerantangan terhadap kejahatan informasi lebih tinggi. Dibutuhkan keamanan yang berlapis untuk melindungi aplikasi dan sistem informasi yang merupakan aset bagi lembaga pemerintahan. Tanpa perlindungan dan pengawasan keamanan sistem yang baik maka bisa terjadi asset informasi yang berharga akan hilang dan mudah disusupi orang yang tidak bertanggung jawab. Menjaga keamanan informasi sangat diperlukan usaha dengan memperhatikan factor-faktor keamanan dari seluruh piranti pendukung, jaringan dan fasilitas lain yang terkait langsung maupun tidak langsung dengan proses pengolahan informasi. Untuk menjamin keamaan data balikan tersebut maka Ditjen Dukcapil mengembangkan sistem pengamanan data yang baik, untuk dapat menampung dan mengolah data balikan dalam jumlah besar untuk diintegrasikan dalam database kependudukan nasional. Aplikasi data balikan saat ini dihadapkan dengan semakin banyaknya data dan informasi yang diterima oleh Lembaga pengguna sebagai akibat dari penggunaan elemen data dari KTP el yang ada pada SIAK yang dimanfaatkan oleh lembaga pengguna. Perlunya penguatan keamanan sistem informasi diperlukan dan ditingkatkan oleh Ditjen Dukcapil dalam pemeliharaan aplikasi.

Menurut Tata Sutabri (2012) informasi merupakan sekumpulan data yang dikelompokan dan diinterpretasi untuk digunakan dalam pengambilan keputusan. Oleh karena itu informasi merupakan aset yang harus dilindungi guna mencegah penyalahgunaan dari sebuah informasi tersebut. Keamanan informasi hal penting yang harus diperhatikan dan dimulai sejak aplikasi mulai go live. Hal ini harus menjadi perhatian lebih dari penyelenggara pemerintahan dalam mengelola aplikasi yang terhubung dengan internet. Fungsi-fungsi yang ada pada aplikasi harus tetap utuh dalam melakukan fungsi pelayanan publik. Meningkatnya kejahatan dalam menggunakan teknologi informasi mulai tahun 2003, seperti carding (credit card fraud), ATM/EDC skimming, hacking, phising (internet banking fraud), maupun virus-virus yang masuk ke sistem melalui jaringan internet (ID-SIRTII/CC, 2017).

Gambar 1. Jumlah pengguan internet di Indonesia tahun 2023
(sumber : https://dataindonesia.id/internet/detail/pengguna-internet-di-indonesia-sentuh-212-juta-pada-2023)

Sebagai lembaga pemerintah yang memberikan layanan publik, Kementrian Dalam Negeri, khususnya Ditjen Dukcapil, harus mengamankan berbagai macam teknologi informasi yang digunakan, hal ini mewajibkan setiap sistem informasi atau aplikasi yang memberi layanan publik, dilakukan proses IT *Security Asessment* (ITSA), yang berguna menilai apakah semua penggunaan teknologi informasi yang digunakan sudah layak digunakan untuk layanan publik, sesuai dengan hak akses dan tidak ada kebocoran data. Penilaian di negara saat ini dilakukan oleh suatu lembaga independen, yaitu oleh Badan Siber dan Sandi Negara (BSSN). Dari lembaga ini yang akan menilai kelayakan dari penggunaan teknologi informasi milik pemerintah. Tahun 2022, pada Ditjen Dukcapil dibantu oleh BSSN melakukan audit khusus untuk IT *Security Assessment* (ITSA) pada aplikasi databalikan.

Proses assesment dari keamanan teknologi informasi merupakan transformasi hubungan pemerintahan dengan kontiniunya karena pemerintah yang berbasis eletronik (Ijeoma & Nwaodu, 2013). Penilaian itu akan membuat kepercayaan rakyat Indonesia, dimana data dan informasi tiap rakyat akan tersimpan pada aplikasi tersebut, yang berkaitan dengan penggunaan KTP el.

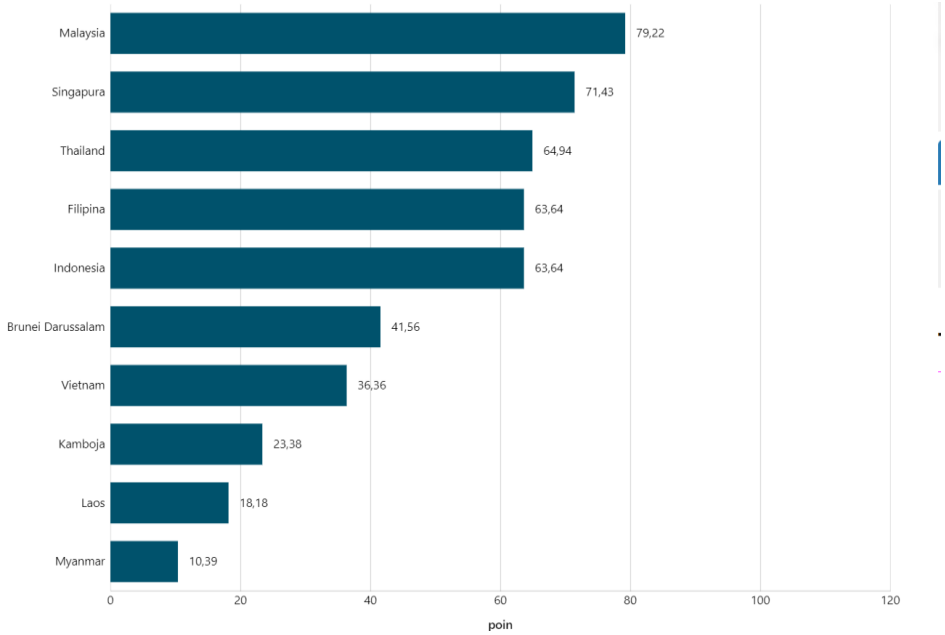
METODE PENELITIAN

Penelitian ini bertujuan untuk mengkaji hasil analisa pelaksanaan ITSA di Kementrian Dalam Negeri yang dilakukan oleh BSSN. Metode kualitatif melalui pendekatan deskriptif eksploratif dan *Case study*. Menggunakan data primer untuk penelitian ini untuk memahami kebijakan dalam lembaga pemerintahan diimplementasikan dan efektivitasnya dalam menjaga keamanan sistem informasi (aplikasi) yang ada pada Ditjen Dukcapil. BSSN melakukan eksplorasi secara mendalam terhadap program, kejadian, proses, aktivitas dalam mengumpulkan data secara mendetail yang berkaitan dengan aplikasi data balikan dan penggunanya. Dalam pengumpulan data dilakukan dengan cara observasi, terhadap aplikasi data balikan dan wawancara terhadap pengguna internal dari aplikasi data balikan, untuk menghasikan data primer yang dibutuhkan dalam proses analisa ITSA.

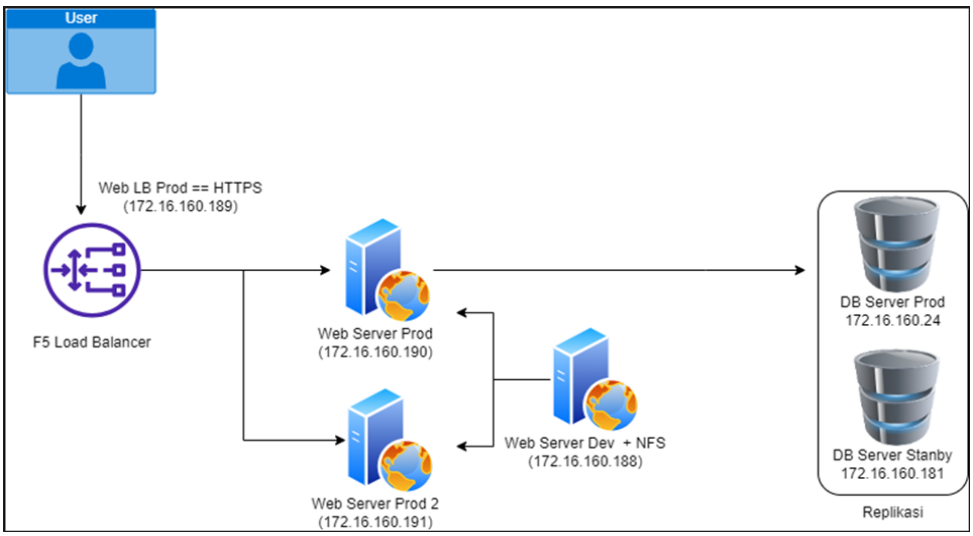
HASIL DAN PEMBAHASAN

A. Keamanan Sistem Informasi

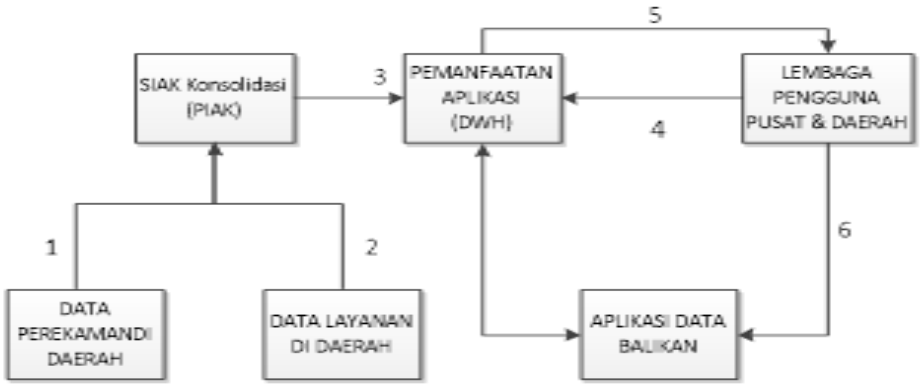
Keamanan informasi merupakan upaya melindungi informasi serta sistem informasi dari akses, penggunaan, pengungkapan, pengoperasian, modifikasi atau penghancuran oleh pengguna yang tidak berwenang agar memastikan kerahasian, integritas serta kemudahan pengguna. Memperhatikan aspek keamanan informasi merupakan salah satu kekuatan dari organisasi atau perusahaan, karena terjadi pemrosesan data dan hasilnya akan tersimpan dan dapat dibagikan. Untuk itu diperlukan evaluasi dari keamanan sistem informasi dengan langkah langkah dasar seperti akses kontrol sistem, pemakaian jaringan dan telekomunikasi, pengembangan sistem, penerapan *criptography*, mencegah resiko, dan penerapan regulasi yang bersifat adil yaitu peraturan berlaku terdiri dari hukum, investigasi dan kode etik. Berikut adalah grafik dari daftar negara dengan Skor Indeks Keamanan Siber Tertinggi di Asia Tenggara versi NCSI pada tahun 2023 :



Gambar 2. Daftar Negara dengan Skor Indeks Keamanan Siber di Asia Tenggara Tahun 2023



Gambar 3. Tampilan Infrastruktur Aplikasi Data Balikan



Gambar 4. Alur proses Informasi Aplikasi Data Balikan

B. Aplikasi Data Balikan

Aplikasi Data Balikan melayani Aplikasi Data Balikan saat ini didukung oleh infrastruktur untuk melakukan fungsinya dalam melayani lembaga pengguna. Berikut infrastruktur dari Aplikasi Data Balikan :

Proses alur data untuk penggunaan data dalam aplikasi data balikan memanfaatkan aplikasi *Data warehouse* untuk menerima data balikan dari lembaga pengguna untuk dapat mengakses KTP el. Berikut alur data dengan pemanfaatan dari Aplikasi data balikan :

C. ITSA (*Information Technology Security Assessment*)

Information Technology Security Assesment (ITSA) merupakan layanan untuk menunjang keamanan dan membantu kelancaran penyelenggaraan berbagai layanan erusa berbasis sistem informasi melalui pengujian kerentanan, pemberian saran dan rekomendasi pengamanan untuk meminimalisir celah kerawanan yang terdapat dalam suatu sistem informasi. Penerima (*stakeholders*) layanan ITSA adalah instansi pemerintah pusat, pemerintah daerah, BUMN, dan lain sebagainya sedangkan penyelenggara layanan ITSA adalah Kelompok/Fungsi Operasi Identifikasi dan Proteksi, Direktorat Operasi Keamanan Siber BSSN. Tujuan dari *Assesment* ini antara lain :

1. Mengidentifikasi celah keamanan pada sistem elektronik untuk menanggulangi adanya potensi kerentanan yang dapat dimanfaatkan oleh pihak eksternal maupun internal untuk melanggar kebijakan keamanan atau perusakan sistem elektronik;
2. Melakukan uji coba penetrasi, eksploitasi, dan validasi terhadap kerentanan yang ditemukan;
3. Melakukan penilaian tingkat risiko kerentanan yang ditemukan;
4. Mengetahui efektivitas sistem deteksi dini, pencegah serangan, dan penanganan insiden yang digunakan;
5. Menjamin kerahasiaan, integritas, dan ketersediaan data maupun layanan sistem elektronik;
6. Membantu proses penguatan dan proteksi sistem elektronik;

Beberapa framework yang bisa digunakan untuk sistem keamanan, tata erusa, keamanan informasi dalam mengatasi serangan siber dalam erusahaan atau organisasi seperti Programming and Budgeting Cyber Security Framework. Untuk melalukan persiapan dan respon dalam menangani kemungkinan dan aktivitas membutuhkan biaya dalam menangani keamanan dunia maya.

D. OWASP (Open Web Applikcation Security Project)

Penggunaan framework OWASP pada Analisa ITSA untuk aplikasi databalikan pada Ditjen Dukcapil. Open Web Application Security Project (OWASP) adalah komunitas terbuka yang didedikasikan untuk memungkinkan organisasi mengembangkan, membeli, dan memelihara aplikasi yang dapat dipercaya *(https://owasp.org/Top10/id/A00-about-owasp/).* Target dari analisa aplikasi databalikan milik Ditjen Dukcapil, Kementrian Dalam Negeri, yang mana aplikasi dabalikan merupakan salah satu aplikasi yang memberikan layanan publik. Strategi pengujian kerentanan terhadap aplikasi databalikan menggunakan metode OWASP TOP 10 2021 dengan penjelasan sebagai berikut:

1) Kategori A01:2021-*Broken Access Control* . Kesalahan atau kekurangan konfigurasi kontrol akses pada sistem elektronik yang menyebabkan pengungkapan informasi sensitif secara yang tidak sah, modifikasi data, atau penghancuran semua data, dan atau melakukan fungsi di luar

batas kewenangan hak akses pengguna.

2) Kategori A02:2021-*Cryptographic Failures*. Kesalahan atau kekurangan konfigurasi keamanan kriptografi pada sistem elektronik sehingga data atau informasi sensitif seperti kata sandi, catatan kesehatan, informasi pribadi dan rahasia bisnis yang ditransmisikan dan atau tersimpan di sistem secara tidak aman.
3) Kategori A03:2021- *Injection*. Kesalahan atau kekurangan konfigurasi pada sistem elektronik sehingga pengguna dapat melakukan injeksi kode yang mengakibatkan kerusakan, kebocoran data sensitif, modifikasi data, dan atau ambil alih sistem. Kerentanan ini diakibatkan karena tidak adanya validasi, filter, dan sanitasi input pengguna pada sistem
4) Kategori A04:2021 – *Insecure Design*. Kesalahan desain yang diterapkan dalam pembangunan sistem sehingga menyebabkan sistem tidak aman dan terdapat kebocoran informasi yang dapat dieksploitasi.
5) Kategori A05:2021 – *Security Misconfiguration*. Kesalahan atau kekurangan konfigurasi keamanan pada sistem elektronik yang dapat dieksploitasi.
6) Kategori A06:2021 – *Vulnerable And Outdated Component*. Penggunaan versi sistem yang usang dan rentan sehingga dapat dieksploitasi.
7) Kategori A07:2021 – *Identification and Authentication Failures*. Kesalahan konfigurasi autentikasi pada sistem elektronik sehingga menyebabkan kegagalan proses autentikasi dan otorisasi dalam sistem.
8) Kategori A08:2021 – *Software and Data Integruty Failures*. Kesalahan dan kekurangan konfigurasi pada sistem elektronik yang menyebabkan kerusakan integritas data yang ditransmisikan dan tahu disimpan dalam sistem.
9) Kategori A09:2021. *Security Logging and Monitoring Failures*. Kesalahan atau kekurangan konfigurasi pada sistem elektronik yang menyebabkan sistem tidak memiliki kemampuan pencatatan untuk audit dan monitoring aktivitas keamanan.
10) Kategori A10:2021. *Server side Request Forgery*. Kesalahan dalam pengembangan sistem elektronik sehingga memungkinkan pengambilan sumber daya secara remote yang tidak divalidasi.

Pada skema indentifikasi dalam ITSA sistem eletronik berbasis web, seperti pada gambar dibawah ini :

Skema dari aplikasi databalikan yang dilakukan akan menggunakan skema elektronik untuk jaringan publik atau eksternal yang digunakan oleh Lembaga pengguna, dimana penguji (*tester*) menggunakan internet yang dimana melewati *firewall* untuk menembus *server*, dari sini dilakukan proses analisa *security assessment* pada aplikasi data balikan untuk melihat celah-celah kemungkinan terjadinya kebocoran data dan informasi pada aplikasi.

Selain pada jaringan publik atau eksternal, pengujian dilakukan pada jaringan internal. Skema dari aplikasi databalikan yang dilakukan akan menggunakan skema elektronik untuk jaringan publik atau eksternal, dimana penguji (*tester*), melewati *router* dengan menggunakan internet untuk terhubung ke *server*, dari sini dilakukan proses analisa *security assessment*, untuk mengalisa celah dari aplikasi dari *server*.

Proses penilaian resiko kerentanan, menggunakan OWASP *risk rating methodology* Dimana untuk nilai *risk* dengan menjumlahkan *likehood* (kemungkinan) dilakukan perkalian dengan *impact* (dampak). Untuk mencari nilai *likehood* (kemungkinan) adalah dengan menjumlahkan nilai dari

threat agent factors dengan *vulnerability factors* kemudian di bagi menjadi dua. Pada *threat agent factors* adalah dengan menjumlahkan *skill level, motive, opportunity, size* kemudian dibagi empat. Nilai *Vulnerability factors* dengan menjumlahkan *ease of discovery, ease of exploit, awareness,* dan *instrucsion detection* dibagi dengan empat. Untuk *Impact* didapat dari penjumlahan *technical impact factors* dan *business impact factor* kemudian dibagi dua. Dengan rumus *Technical impact factors* adalah dengan menjumlahkan dari *Loss of confidentiality, Loss of Integrity, Loss of Availability* kemudian di bagi empat. Untuk *Business Impact Factors* dengan menjumlahkan nilai dari *ide damage, Reputation Damage, non compliance, privacy violation* kemudian dibagi empat.

Dari setiap resiko kerentanan yang dianalisa dengan metode OWASP didapat rincian sebagai berikut :

1. *Critical* dengan cara memungkinkan eksekusi kode pada aplikasi atau perintah pada server; merusak aplikasi atau server; mengakses, mengambil dan modifikasi data sensitif, mengambil alih *server*, merusak citra pemilik sistem elektronik, ditandai dengan warna ungu.
2. *High* dengan cara memungkinkan eksekusi kode pada aplikasi atau perintah pada *server*; merusak aplikasi atau *server;* merusak citra pemilik sistem elektronik, ditandai dengan warna merah.
3. *Medium* terdapat kebocoran informasi, kesalahan atau kekurangan konfigurasi pada aplikasi atau *server* yang dapat dimanfaatkan untuk menemukan kerentanan lain atau eksploitasi, ditandi dengan warna orange
4. *Low* terdapat kebocoran informasi, kesalahan atau kekurangan konfigurasi pada aplikasi atau *server* yang dapat dimanfaatkan untuk menemukan kerentanan dengan rekayasa sosial untuk eksploitasi, ditandai dengan warna kuning.
5. *Info* terdapat kebocoran informasi yang kemungkinan kecil dapat dieksploitasi, ditandai dengan warna hijau.

Penilaian untuk hasil analisa ITSA (*Information Technology Security Assessment*) menghasilkan beberapa nama kerentanan berdasarkan metode OWASP, sebagai berikut

1. PII *Dislosure.* Dengan merekomendasikan untuk menerapkan JSON *web token* (JWT) untuk pembatasan akses pada masing-masing grup *user* (*role*). Kondisi statusnya berwarna ungu pada saat proses Analisa ITSA.
2. *Weak Password Policy*. Dengan menerapkan kebijakan pengguna *password* pada aplikasi yaitu setiap *username* memiliki *password* yang berbeda; menerapkan kebijakan pengguna *password* yang baik sebagaimana mengacu pada NIST 800-63 dan/atau PCI DSS Standards *requirement* 8; menerapkan kebijakan perubahan *password* dalam tentang waktu tertentu. Kondisi statusnya berwarna merah pada saat proses Analisa ITSA.
3. *Insecure Direct Object Reference.* Dengan menghindari penggunaan parameter ID pada *form request* pada *website* atau melakukan *indirect object reference* menggunakan enkripsi atau *hash* terhadap ID tersebut; akses kontrol terhadap pengguna harus disesuaikan dengan haknya; akses kontrol harus diterapkan untuk mendisiplinkan pengguna dalam mengakses aplikasi sesaui dengan haknya; membatasi *user* yang terautentikasi dengan penggunaan *session* agar informasi perihal data pribadi *user* lain. Kondisi statusnya berwarna merah pada saat proses Analisa ITSA.

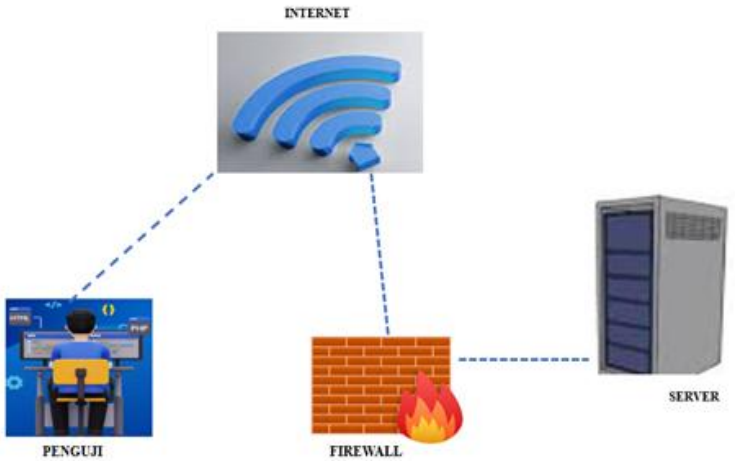
4. *Vertical Privilege Escalation.* Dengan menerapkan JSON *web token* (JWT) untuk melakukan pembatasan akses pada masing-masing grup *user* (*role*); tidak menampilkan informasi sensitif seseorang pada *response* website; melakukan proteksi terhadap informasi sensitif dengan menggunakan enkripsi atau *has.* Kondisi statusnya berwarna merah pada saat proses Analisa ITSA.
5. *Session Fixation*. Dengan mengatur aplikasi agar menetapkan *cookie* baru saat pengguna berhasil *login.* Kondisi statusnya berwarna ungu pada saat proses Analisa ITSA.
6. *Old Session Does Expire After Password Change.* Dengan melakukan manajemen penggunaan *cookie* sesi yang baik.

Setelah kerentanan pada aplikasi data balikan diindetifikasi, kemudian di lakukan teknik pengujian sistem menggunakan *black box testing. Back box testing* adalah pengujian yang dilakukan untuk mengamati hasil *input* dan *output* dari perangkat lunak tanpa mengetahui struktur kode dari perangkat lunak. Dimana pengujian di lakukan pada akhir pembuatan perangkat lunak (*software*) untuk mengetahui *software* berjalan dengan baik. Pada tes ini yang berperan sebagai pihak eksternal, peretas atau *hacker*, dan tidak membutuhkan informasi apapun. Pada pengujian dengan *grey box testing* adalah sebuah metodologi kombinasi dari *black box* dan *white box testing*, menguji *software* berdasarkan spesifikasi tetapi menggunakan cara kerja dari dalam. Pada metode ini membantu pada pengembang untuk mengevaluasi seberapa bagus perangkat lunak yang telah dirancang.

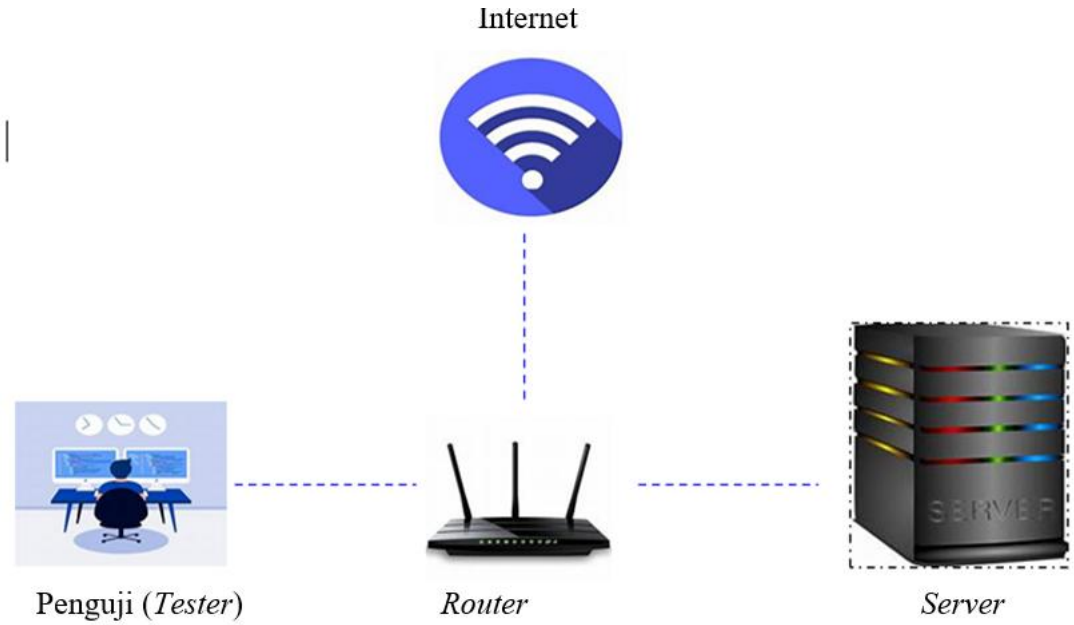
Dari proses analisa ITSA, didapat *assessment* yang sudah dikategorikan dengan warna. Berikut dampak dari hasil penilaian dari keamanan sistem aplikasi ini, beberapa kegiatan akan terhambat, seperti :

1. Terjadi *error*
2. Terjadi gangguan layanan publik
3. Terjadi *Denial of service (DOS)*
4. Terjadi injeksi kode/perintah berbahaya pada sistem
5. Terjadi perubahan data pada database
6. Peningkatan *traffic* data ke *server*
7. Peningkatan proses pada *server*

Gambar 3. *Security Assessment* Category Level (sumber : *Critical Ethical Hacking 2012*)



Gambar 4. Skema Penggunaan Sistem elektronik untuk Jaringan publik atau eksternal



Gambar 5. Skema Penggunaan Sistem elektronik untuk Jaringan publik atau eksternal

KESIMPULAN DAN SARAN

Dalam proses ITSA (*Information Technology Security Assessment*) merupakan hal penting dalam penggunaan sistem elektronik, terutama pada lembaga pemerintahan. Aplikasi layanan publik penting untuk dilakukan proses *assessment security* sistem informasi secara berkala, untuk menjaga integritas datanya dari kebocoran data. Proses assessment yang dilakukan pada aplikasi databalikan, menemukan beberapa 6 (enam) kerentanan pada aplikasi tersebut. Hal ini mengharuskan proses perbaikan pada beberapa sub modul yang ada pada aplikasi databalikan yang memiliki nilai keretanan yang direkomendasikan oleh tim assessment. Tingkat penilaian dikategorikan dengan *Low, Medium, Critical, High* dan *Note*. Hasil *assessment* direkomendasikan untuk dilakukan perbaikan dari 6 kerentanan yang ditemukan dalam proses *assessemnt*. ITSA akan menjadi rangkaian kegiatan yang akan dilakukan dalam Kemendagri Ditjen Dukcapil guna menjaga integritas informasi dari

aplikasi data balikan yang berisi data dan informasi penduduk.

DAFTAR PUSTAKA

Aditya Wibisono Kuncoro, Fayruz Rahma, S.T, M.ENG, (2022). "Analisis Metode Open Web Application Security Project (OWASP) pada Pengujian Keamanan Website: Literature Review" https://journal.uii.ac.id/AUTOMATA/article/view/21893, Januari, 2022

Bita Parga Zen, Rudy A.G Gultom, Agus H.S Reksoprodjo, (2018). "Analisis Security Assessment Menggunakan Metode Penetration Testing Dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara",. https://www.researchgate.net/publication/344493542. Juni, 2020.

Moh Yunus, (2019) "Analisis Kerentanan Aplikasi Berbasis Web Menggunakan Kombinasi Security Tools Project Berdasarkan Framework Owasp Versi 4", https://ejournal.gunadarma.ac.id/index.php/infokom/article/view/1988.

Noor Vika Hizviani, 2021. "Rancangan Aplikasi Data Balikan pada Kementrian Dalam Negeri", https://ibn.e-journal.id/index.php/KOMPUTASI/article/view/297 , Mei, 2021.

Rusydi Umar, Imam Riadi, Eko Handoyo, 2019. "Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI)," http://ejournal.undip.ac.id/index.php/jsinbis, 2019.

Reynaldo Adi Putra Pratama Gala 1), Rizal Sengkey 2), Charles Punusingon, 2020. "Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI". https://ejournal.unsrat.ac.id/index.php/informatika, Juli-september, 2020.

Online Tentang OWASP https://owasp.org/Top10/id/A00-about-owasp/ ITSA (*IT security assessment*) https://bssn.go.id/information-technology-security-assessment/