Jurnal Rekayasa Sistem Informasi dan Teknologi
Volume 1, No 3 – Februari 2024
e-ISSN : 3025-888X

EVALUASI DAN PENGEMBANGAN LAYANAN SISTEM INFORMASI PPID DINAS KESEHATAN PROVINSI JAWA TIMUR DENGAN MENGGUNAKAN STANDAR DAN TEKNIS KEMANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE)

Benedictus Radyan Dwianggoro [1*], Luvia Friska Narulita[2]
[12]Universitas 17 Agustus 1945 Surabaya, Indonesia
benedictusradyan@gmail.com[1*]
Luvia@untag-sby.ac.id [2]

Received: 20-01- 2024	Revised: 25-01-2024	Approved: 01-02-2024

ABSTRAK

Komitmen pemerintah Indonesia yang teguh untuk meningkatkan efisiensi dan transparansi terlihat jelas dalam Perpres RI Nomor 95 tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE). Sejalan dengan komitmen ini, penelitian ini berfokus pada evaluasi dan peningkatan Layanan Sistem Informasi dari Layanan Informasi PPID di Dinkes Jatim, mengadopsi standar keamanan SPBE. Tujuan utamanya adalah menggunakan metode Prototyping dan mengikuti panduan yang disediakan oleh Standar Teknis dan Prosedur Keamanan SPBE, diimplementasikan melalui kerangka kerja Laravel.Proses penelitian dimulai dengan analisis masalah menggunakan teknik observasi dan wawancara. Kajian literatur memberikan wawasan penting untuk pengembangan sistem informasi PPID. Evaluasi layanan dilakukan untuk menghasilkan rekomendasi perbaikan. Fase implementasi menggabungkan metode Prototyping dengan indikator yang berasal dari standar teknis dan prosedur keamanan SPBE. Pengujian sistem, termasuk penerapan metode Penetration Testing, mengidentifikasi 9 kerentanan dalam situs web, dengan 2 pada level resiko sedang dan 7 pada level resiko rendah. Meskipun kemajuan dalam mematuhi standar keamanan memuaskan, rekomendasi pengembangan lanjutan dari OWASP ZAP sangat penting. Tujuan utamanya adalah memberikan kontribusi positif terhadap efektivitas, integrasi, keberlanjutan, efisiensi, akuntabilitas, interoperabilitas, dan keamanan Layanan Sistem Informasi PPID di Dinkes Jatim. Upaya ini sejalan dengan prinsip transparansi dan efisiensi dalam tata pemerintahan.

Kata kunci: Sistem Informasi, Pengembangan, Standar Keamanan Apalikasi Berbasis Website, Metode Prototyping, Metode Penetration Testing.

PENDAHULUAN

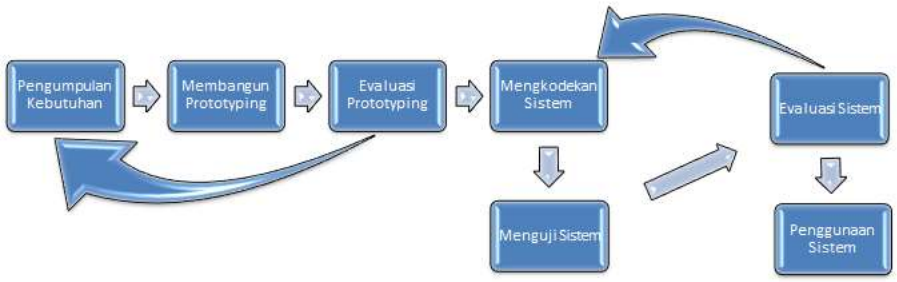
Dalam kaitannya dengan Perpres RI Nomor 95 Tahun 2018 mengenai SPBE, fokus utama penelitian ini adalah pada prinsip keamanan, sebagaimana dijelaskan pada Pasal 2 Bab 1 [1]. Salah satu instansi pemerintah yang belum menerapkan SPBE adalah PPID Dinas Kesehatan Provinsi Jawa Timur, bertanggung jawab dalam memberikan layanan informasi dan menjadi wadah pengajuan permohonan dari masyarakat. Sebagai layanan sistem informasi pemerintahan, PPID Dinas Kesehatan Provinsi Jawa Timur diharapkan dapat memberikan akses informasi yang cepat, akurat, dan transparan kepada masyarakat. Dengan menyadari hal tersebut, peneliti berinisiatif untuk mengevaluasi dan mengembangkan layanan Sistem Informasi PPID Dinas Kesehatan Provinsi Jawa Timur dengan menggunakan standar keamanan SPBE guna meningkatkan keamanan data masyarakat. Dalam tahap evaluasi, identifikasi atau analisis kelemahan sistem terutama dari aspek keamanan layanan sistem informasi PPID Dinas Kesehatan Provinsi Jawa Timur akan dilakukan. Sementara itu, untuk tahap pengembangan pada layanan sistem informasi PPID Dinas Kesehatan Provinsi Jawa Timur, metode Prototyping akan digunakan, dengan menerapkan standar keamanan aplikasi

berbasis website sesuai dengan pedoman Standar Teknis dan Prosedur Keamanan yang sudah diatur kedalam Peraturan BSSN Nomor 4 Tahun 2021 [2]. Metodologi penelitian akan mencakup analisis masalah, pengumpulan data melalui wawancara dan observasi dengan pihak terkait, studi literatur mengenai SPBE, standar keamanan, serta analisis SPBE. Implementasi pengembangan sistem baru yang memenuhi standar teknis dan prosedur keamanan SPBE juga akan dilakukan. Harapannya, penelitian ini dapat meningkatkan keamanan sistem informasi PPID Dinas Kesehatan Provinsi Jawa Timur dengan menggunakan Standar Teknis dan Prosedur Keamanan SPBE. Dengan demikian, Layanan Sistem Informasi PPID Dinas Kesehatan Provinsi Jawa Timur dapat memberikan layanan yang baik, cepat, dan transparan kepada khalayak umum dalam hal pengajuan permohonan [3].

METODE PENELITIAN

A. Metode *Prototyping*

Dalam fase pengembangan penelitian ini, metode yang akan digunakan adalah *Prototyping*. *Prototyping* merupakan suatu pendekatan dalam pengembangan perangkat lunak yang memungkinkan perancangan sistem [4]. Melalui pendekatan ini, pengembang dan klien dapat berpartisipasi dalam seluruh proses pembuatan prototipe sistem. Terkadang, klien hanya memberikan definisi umum mengenai keinginan mereka tanpa menyebutkan secara rinci mengenai input dan output yang diharapkan dari sistem yang akan dikembangkan [5]. Untuk mengatasi ketidakselarasan ini, kerjasama yang efektif antara pengembang dan klien menjadi krusial agar pengembang dapat memahami dengan jelas kebutuhan klien. Dengan demikian, hasilnya akan berupa desain sistem yang interaktif sesuai dengan kebutuhan. Informasi lebih lanjut mengenai tahapan metode *prototyping* dapat ditemukan pada Gambar 1.



Gambar 1 Tahapan Metode *Prototyping*

Dalam tahapan pengembangan model *Prototyping*, terdapat langkah-langkah yang harus diikuti, antara lain :

1) analisa Keperluan sistem
   Pada fase ini, pengembang melakukan analisis terhadap perangkat lunak dan seluruh kebutuhan sistem yang harus dikembangkan.
2) Pembuatan Prototipe
   Langkah ini melibatkan pembuatan desain sementara yang difokuskan pada presentasi kepada pihak pengguna.
3) Penilaian Prototipe

Evaluasi dilakukan untuk mengevaluasi sejauh mana prototipe memenuhi harapan pihak pengguna.

4) Pengkodean Sistem
   Prototipe yang telah mendapat persetujuan akan diimplementasikan ke dalam bahasa pemrograman.
5) Evaluasi Sistem
   Pada tahapan ini, dilakukan evaluasi terhadap perangkat lunak yang telah dibuat.
6) Penilaian Sistem
   Perangkat lunak yang telah selesai dikembangkan dievaluasi oleh pihak pengguna untuk memastikan kesesuaian dengan harapan.
7) Implementasi Sistem
   sistem yang telah diuji dan disetujui oleh pihak pengguna siap digunakan [6].

B. Metode Uji *Penetration Testing*

Penggunaan model uji penetrasi akan menjadi bagian dari pengujian keamanan sistem. Proses pengujian menggunakan metode uji penetrasi pada sebuah situs web merupakan suatu proses yang rumit dan harus dilakukan secara cermat guna mengidentifikasi serta mengatasi potensi kerentanan keamanan [7]. Setelah tahapan pengembangan selesai. langkah selanjutnya adalah melakukan pengujian kerentanan website dengan menggunakan tools bantuan dari OWASP zap. Yang nantinya hasil dari pengujian kerentanan tersebut akan berupa tabel hasil pengujian yang berisikan alert atau notifikasi kerentanan dan tingkatan kerentanan tersebut, tidak hanya itu di dalam tools owasp zap ini juga sudah memberikan rekomendasi dari setiap tingkat kerentanan yang terdeteksi. Untuk tahapan dari metode uji Penetration Testing adalah sebagai berikut :

1) Identifikasi Kerentanan
   Penetration testing membantu mengidentifikasi kerentanan keamanan yang ada dalam sistem. Dengan menguji sistem secara aktif, pengetes penetrasi dapat menemukan kerentanan keamanan data yang dapat dimanfaatkan oleh pihak yang tidak sah [8].
2) Evaluasi Keefektifan Kontrol Keamanan
   Metode ini memungkinkan evaluasi terhadap efektivitas kontrol keamanan yang telah diimplementasikan. Dengan melakukan serangan simulasi, pengujian penetrasi dapat membantu menentukan apakah kontrol keamanan yang ada sudah cukup kuat atau membutuhkan perbaikan [9].
3) Peningkatan Keamanan
   Penetration testing membantu meningkatkan tingkat keamanan sistem dengan mengidentifikasi kerentanan yang ada dan memberikan rekomendasi tindakan perbaikan. Ini memungkinkan organisasi untuk mengambil langkah-langkah yang diperlukan dalam memperbaiki kelemahan dan memperkuat sistem keamanan mereka.
4) Proses uji penetrasi harus dilakukan dengan izin dan persetujuan dari pemilik sistem yang diuji, dan harus dilaksanakan oleh profesional keamanan yang memiliki pengetahuan dan keterampilan yang memadai di bidang ini. Tujuannya adalah untuk meningkatkan keamanan sistem dengan memperbaiki kerentanan yang ditemukan dan mencegah potensi serangan dari pihak yang bermaksud jahat [10].

HASIL DAN PEMBAHASAN

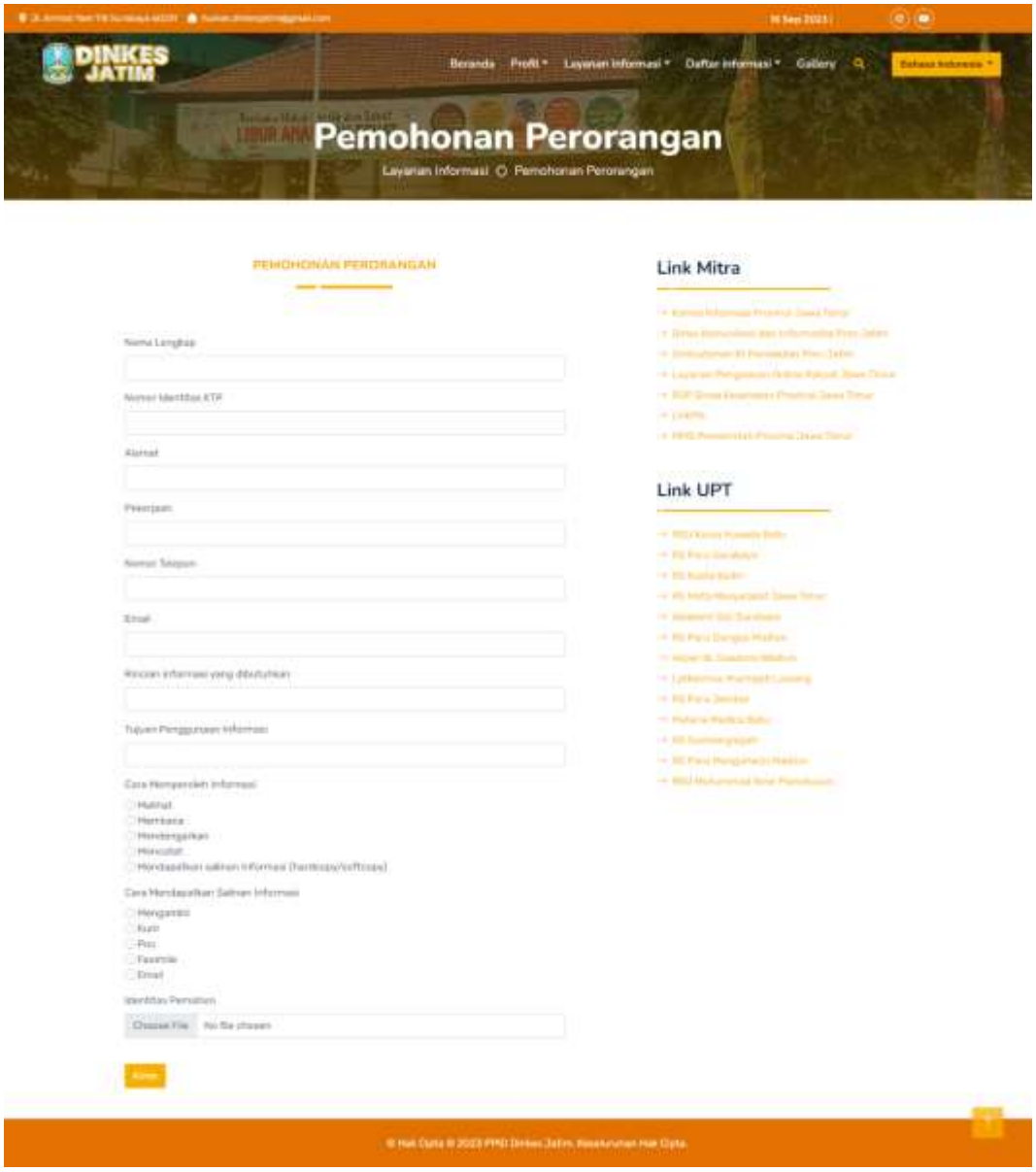
A. Implementasi Pengembangan Sistem

Untuk tampilan muka layanan sistem informasi PPID Dinas Kesehatan Provinsi Jawa Timur pada sisi pengungjung ini berisikan navigation bar untuk

melakukan pengajuan permohonan informasi perorangan, pengaduan, dan melihat profil dari PPID Dinas Kesehatan Provinsi Jawa Timur. Untuk tampilan muka pada sisi pengunjung Bisa Dilihat Pada Gambar 2.

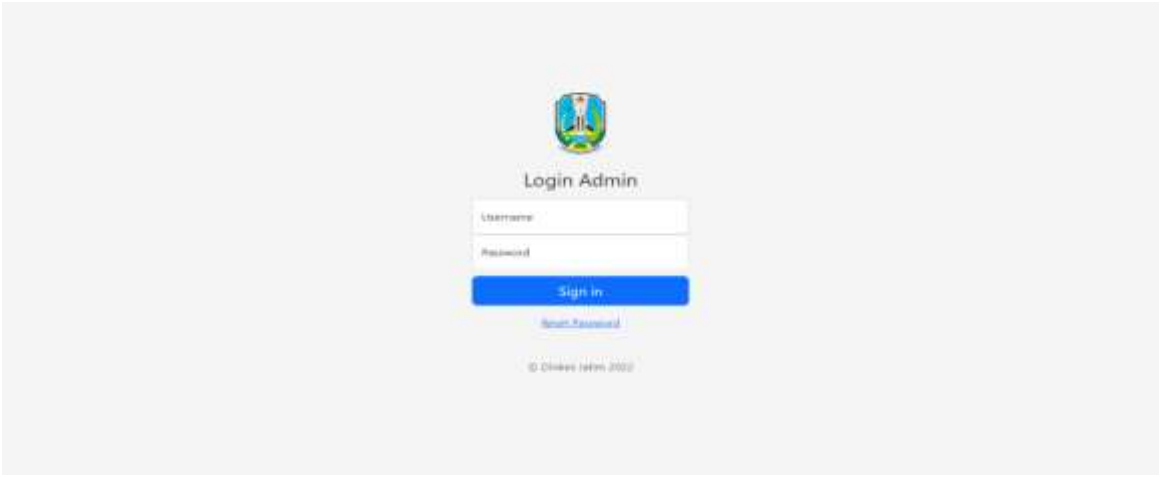
Gambar 2 Tampilan halaman beranda pengunjung

Ada pula tampilan untuk pengajuan permohonan informasi pada sisi pengunjung yang berisikan inputan data untuk melakukan pengajuan permohonan informasi. Untuk tampilan pengajuan permohonan informasi bias dilihat pada Gambar 3.



Gambar 3 Tampilan halaman pengajuan permohonan informasi pada sisi pengunjung

Kemudian untuk tampilan halaman login yang akan digunakan untuk masuk kedalam halaman admin ini terdapat inputan seperti username dan password dan tombol login, kemudian ada tombol untuk melakukan reset password. Untuk tampilan muka halaman login pada sisi admin bisa dilihat pada Gambar 4.

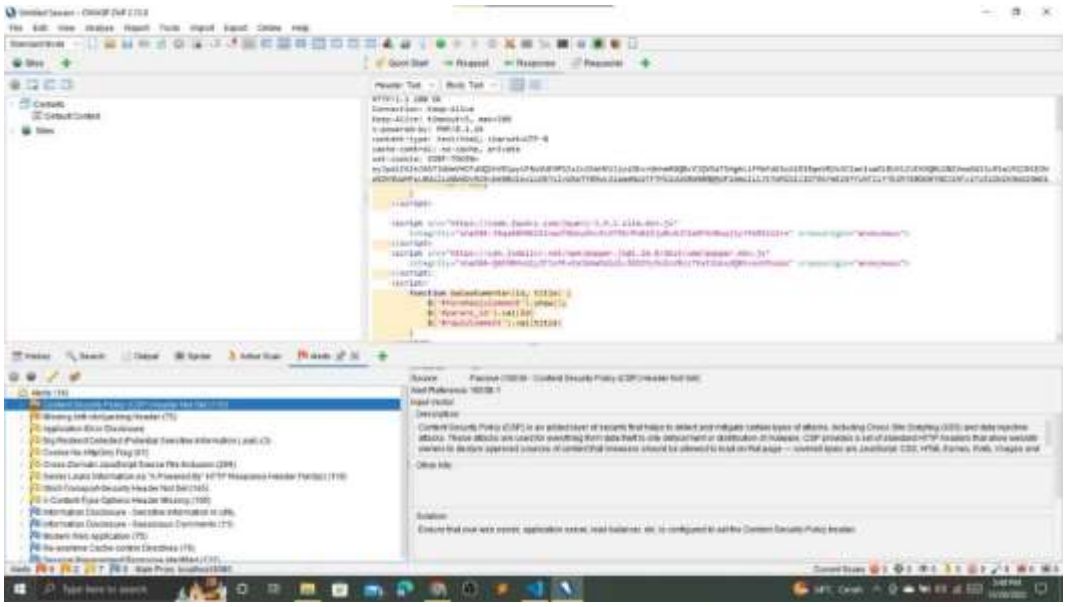


Gambar 4 Tampilan halaman login admin

B. Hasil Pengujian Sistem

Pada pengujian sistem ini menggunakan Penetration testing serta tools bantuan dari OWASP ZAP Yang nantinya hasil dari pengujian kerentanan website tersebut akan berupa tabel hasil pengujian yang berisikan alert atau notifikasi kerentanan dan tingkatan kerentanan tersebut , tidak hanya itu di dalam tools owasp zap ini juga sudah memberikan rekomendasi dari setiap tingkat kerentanan yang terdeteksi dan bisa menjadi bahan untuk dilakukan peroses pemeliharan dan pengembangan dikemudian hari. Untuk tampilan muka hasil pengujian kerentanan website yang telah dilakukan bisa dilihat pada Gambar 5.

Gambar 5 Tampilan hasil pengujian website menggunakan tools bantuan OWASP



ZAP

Berdasarkan hasil pengujian menggunakan alat (OWASP), ditemukan sejumlah celah keamanan pada layanan sistem informasi PPPID Dinas Kesehatan Provinsi Jawa Timur. Celah keamanan tersebut mencakup beberapa identifikasi,

antara lain: Ketidaksetelan Header Content Security Policy (CSP), Ketidakadaan Header Anti-clickjacking, Pengungkapan Kesalahan Aplikasi, Deteksi Redirect Besar (Potensial Bocornya Informasi Sensitif), Ketidakadaan Flag HttpOnly pada Cookie, Inklusi Berkas Sumber JavaScript Lintas Domain, Pengungkapan Informasi Server melalui Header Respons HTTP "X-Powered-By", Header Strict-Transport-Security yang Tidak Diatur, dan Ketidaksetelan Header X-Content-Type-Options. Kemudian untuk hasil scanning yang didapatkan adalah 9 alert dan dua level resiko, diantaranya adalah 2 medium dan 7 low. untuk penjelasan nya bisa dilihat pada Tabel 1.

Tabel 1.Hasil Pengujian Kerentanan Website

Alert	Resiko	Keterangan
Content Security Policy (CSP)	Medium	CSP berfungsi sebagai keamanan tambahan yang bertujuan untuk mengidentifikasi dan mengatasi jenis serangan tertentu, seperti (XSS) dan serangan penyisipan data.
Missing Anti-clickjacking Header	Medium	Respon tersebut tidak menyertakan baik Content-Security-Policy dengan direktif 'frame-ancestors' maupun X-Frame-Options untuk melindungi dari serangan 'ClickJacking'.
Application Error Disclosure	Low	Halaman ini mengandung pesan kesalahan/peringatan yang dapat mengungkapkan informasi sensitif, seperti lokasi file yang menyebabkan pengecualian yang tidak ditangani.
Big Redirect Detected (Potential Sensitive Information Leak)	Low	Server merespons dengan pengalihan yang memberikan tanggapan besar.
Cookie No HttpOnly Flag	Low	Cookie telah diatur tanpa flag HttpOnly, yang berarti bahwa cookie tersebut dapat diakses oleh JavaScript.
Cross-Domain JavaScript Source File Inclusion	Low	File pada halaman ini mencakup satu atau lebih file skrip dari domain pihak ketiga.
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	Server web sedang bocor informasi melalui satu atau lebih header tanggapan HTTP "X-Powered-By."
Strict-Transport-Security Header Not Set	Low	HTTP Strict Transport Security (HSTS) adalah mekanisme kebijakan keamanan web di mana server web menyatakan bahwa pengguna yang mematuhi (seperti

Alert	Resiko	Keterangan
		browser web) harus berinteraksi dengannya hanya melalui koneksi HTTPS yang aman (yaitu HTTP yang dilapisi dengan TLS/SSL).
X-Content-Type-Options Header Missing	Low	Header Anti-MIME-Sniffing X-Content-Type-Options tidak diatur menjadi 'nosniff.'

Kemudian adapun hasil saran rekomendasi perbaikan yang diberikan oleh tools OWASP ZAP untuk keperluan pengembangan sistem dikemudian hari. untuk rekomendasi perbaikan dari tools OWASP ZAP bias dilihat pada Tabel 2.

Tabel 2.Hasil Saran Rekomendasi Perbaikan Dari Tools Bantuan OWASP ZAP

Alert	Resiko	Rekomendasi Perbaikan
Content Security Policy (CSP)	Medium	Memastikan bahwa server web, server aplikasi, penyeimbang beban, dan sebagainya telah mengonfigurasi header Content-Security-Policy.
Missing Anti-clickjacking Header	Medium	Pastikan penggunaan HTTP CSP dan X-Frame-Options pada semua halaman web yang dihasilkan oleh situs atau aplikasi Anda, mengingat bahwa web browser modern mendukung keduanya.
Application Error Disclosure	Low	Lakukan pemeriksaan pada kode sumber halaman ini dan terapkan halaman kesalahan kustom.
Big Redirect Detected (Potential Sensitive Information Leak)	Low	Memastikan tidak ada informasi sensitif yang dapat bocor melalui respons pengalihan.
Cookie No HttpOnly Flag	Low	Pastikan bahwa flag HttpOnly diatur untuk semua cookie.
Cross-Domain JavaScript Source File Inclusion	Low	Pastikan file sumber JavaScript hanya dimuat dari sumber yang dapat dipercaya, dan sumber tersebut tidak dapat dikendalikan oleh pengguna akhir aplikasi.
Server Leaks Information via "X-Powered-By" HTTP Response Header	Low	Pastikan server web, server aplikasi, penyeimbang beban, dan lainnya sudah dikonfigurasi untuk menekan header "X-Powered-By".

Alert	Resiko	Rekomendasi Perbaikan
Field(s)		
Strict-Transport-Security Header Not Set	Low	Pastikan server web, server aplikasi, penyeimbang beban, dan lainnya sudah dikonfigurasi untuk menerapkan Strict-Transport-Security.
X-Content-Type-Options Header Missing	Low	Pastikan aplikasi/server web sudah mengatur header Content-Type dengan benar dan mengonfigurasi header X-Content-Type-Options sebagai 'nosniff' untuk semua halaman web.

KESIMPULAN

Berdasarkan hasil penelitian evaluasi dan pengembangan layanan sistem informasi PPID Dinas Kesehatan Provinsi Jawa Timur dengan menggunakan standar teknis dan keamanan, ditemukan sejumlah hasil terkait keamanan pada layanan sistem informasi PPPID Dinas Kesahatan Provinsi Jawa Timur. Hasil penelitian ini mencakup beberapa aspek, seperti kertidaksesuaian (CSP) Header, ketiadaan Anti-clickjacking Header, pengungkapan kesalahan aplikasi, deteksi pengalihan besar (potensial bocornya informasi sensitif), ketidakadaan flag HttpOnly pada Cookie, inklusi berkas sumber JavaScript lintas domain, ketidaksesuaian Strict-Transport-Security Header, dan ketidakadaan header X-Content-Type-Options. Hasil pemindaian menunjukkan 9 peringatan dengan dua tingkat risiko, terdiri dari 2 tingkat risiko medium dan 7 tingkat risiko rendah. Dari kesimpulan tadi maka dapat dikatakan bahwa penelitian terkait evaluasi dan pengembangan layanan sistem informasi PPID Dinas Kesehatan Provinsi Jawa Timur dengan menggunakan standar teknis dan keamanan ini bisa dikatakan sudah cukup berjalan dengan baik dikarenakan tidak ada celah kemanan yang menyentuh resiko tingkat high.

DAFTAR PUSTAKA

[1] Peraturan Presiden RI, “Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik,” *Menteri Huk. Dan Hak Asasi Mns. Republik Indones.*, p. 110, 2018.

[2] PERATURAN PERUNDANG-UNDANGAN KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA REPUBLIK INDONESIA, “Peraturan BSSN Nomor 4,” *Pedoman Manaj. Keamanan Inf. Sist. Pemerintah. Berbas. Elektron. Dan Standar Tek. Dan Prosedur Keamanan Sist. Pemerintah. Berbas. Elektron.*, 2021.

[3] A. Kurniawan, M. Chabibi, and R. S. Dewi, “Pengembangan Sistem Informasi Pelayanan Desa Berbasis Web Dengan Metode Prototyping Pada Desa Leran,” *JURIKOM (Jurnal Ris. Komputer)*, vol. 7, no. 1, p. 114, 2020, doi: 10.30865/jurikom.v7i1.1863.

[4] E. Kaban, K. Candra Brata, and A. Hendra Brata, “Evaluasi Usability Menggunakan Metode System Usability Scale (SUS) Dan Discovery

Prototyping Pada Aplikasi PLN Mobile (Studi Kasus PT. PLN)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 4, no. 10, pp. 3281–3290, 2020, [Online]. Available: http://j-ptiik.ub.ac.id

[5] Y. A. Prasetyo and N. Ambarsari, "Pengembangan Web E-Commerce Bojana Sari Menggunakan Metode Prototype," *e-Proceeding Eng.*, vol. 2, no. 1, pp. 1042–1056, 2015.

[6] M. Agustine Bacsafra and D. Mustika Kusumawardani, "Pengembangan Sistem Informasi Badan Pusat Statistik Kabupaten Kuningan Berbasis Android Dengan Metode Prototype," *J. Sains Komput. Inform. (J-SAKTI*, vol. 6, no. 1, pp. 379–390, 2022.

[7] S. Hidayatulloh and D. Saptadiaji, "Penetration Testing pada Website Universitas ARS Menggunakan Open Web Application Security Project (OWASP)," *J. Algoritm.*, vol. 18, no. 1, pp. 77–86, 2021, doi: 10.33364/algoritma/v.18-1.827.

[8] M. D. Al Vriano, "Pengujian Keamanan Web Juice Shop Dengan Metode Pentesting Berbasis Owasp Top 10," *J. Multidisiplin Saintek*, vol. 1, no. 06, pp. 81–90, 2023.

[9] Reza. Aditama; Edi. Negara, "Pemindai Kerentanan Terhadap Website Jago Masak Dengan Metode Pengujian Penetrasi OWASP ZAP," *J. Mantik*, vol. 6, no. 3, pp. 3406–3412, 2022.

[10] Y. A. Pohan, "Meningkatkan Keamanan Webserver Aplikasi Pelaporan Pajak Daerah Menggunakan Metode Penetration Testing Execution Standar," *J. Sistim Inf. dan Teknol.*, vol. 3, pp. 1–6, 2021, doi: 10.37034/jsisfotek.v3i1.36.