

PEMERINTAH KOTA PROBOLINGGO

**DOKUMEN PENDUKUNG**

**SISTEM MANAJEMEN KEAMANAN INFORMASI**

FORMULIR KERJA

IDENTIFIKASI STANDAR TEKNIS KEAMANAN

APLIKASI BERBASIS WEB

DINAS KOMUNIKASI DAN INFORMATIKA KOTA PROBOLINGGO

TAHUN 2024

**DOKUMEN PENDUKUNG**

**SISTEM MANAJEMEN KEAMANAN INFORMASI**

**DINAS KOMUNIKASI DAN INFORMATIKA KOTA PROBOLINGGO**

**Jenis** : Formulir Kerja

**Judul** : Identifikasi Standar Teknis Keamanan Aplikasi Berbasis Web

**No. Dokumen** : ${nomor\_naskah}

**No. Reg.** : FRK.SMKI.DISKOMINFO.0019

**Versi** : 01.00

**Tanggal Terbit :** ${tanggal\_naskah}

**Kendali** :

|  |  |  |
| --- | --- | --- |
| **Uraian** | **Nama** | **Jabatan** |
| Disiapkan oleh | DOYS FEBY ANGGA DEWA, S. Kom. | Kepala Seksi Keamanan Informasi dan Persandian |
| Diperiksa oleh | AKHMAD RIDOWI, S. Kom., MM. | Kepala Bidang Teknologi Informasi dan Komunikasi |
| Diverifikasi oleh | ANDRE NIRWANA KUSUMA, ST., MT. | Sekretaris Dinas |
| Disetujui oleh | Dr. AMAN SURYAMAN, AP., MM. | Kepala Dinas Komunikasi dan Informatika |

**Riwayat Vesi :**

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Versi** | **Tanggal** | **Keterangan** |
| 01. | 01.00 | ${tanggal\_naskah} | Rilis Perdana |

**Pengesahan** :KEPALA DINAS KOMUNIKASI

DAN INFORMATIKA KOTA PROBOLINGGO

${ttd\_pengirim}

**Dr. AMAN SURYAMAN, AP., MM.**

Pembina Utama Muda

NIP. 19751206 199412 1 001

**Ket. Registrasi :**

Nomor : FRK.SMKI.DISKOMINFO/0019/………………../20…..

Tanggal : ……………………………………………

**FORMULIR**

**IDENTIFIKASI FUNGSI STANDAR TEKNIS KEAMANAN APLIKASI BERBASIS WEB**

Kami yang bertanda tangan di bawah ini :

Nama :

NIP. :

Pangkat :

Jabatan :

Unit Kerja : Dinas Komunikasi dan Informatika

Instansi : Pemerintah Kota Probolinggo

*E Mail* Dinas :

No. Telp./WA. :

Berdasarkan :

1. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
2. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik.
3. Peraturan Wali Kota Probolinggo Nomor 15 Tahun 2022 tentang Kedudukan, Susunan Organisasi, Uraian Tugas dan Fungsi serta Tata Kerja Dinas Komunikasi Dan Informatika Kota Probolinggo.
4. Keputusan Kepala Dinas Komunikasi dan Informatika Kota Probolinggo Nomor : 188/1753/KEP/425.113/2022 tentang Buku Panduan Pembangunan/Pengembangan/Pemeliharaan Aplikasi Pemerintah Kota Probolinggo
5. Surat Kepala Dinas Komunikasi dan Informatika Kota Probolinggo Nomor ….. Tanggal ….. perihal Undangan Rapat Identifikasi Standar Teknis Keamanan Aplikasi Berbasis Web …..

telah melaksanakan kegiatan Identifikasi Standar Teknis Keamanan Aplikasi Berbasis Web, sebagai berikut :

1. **IDENTITAS APLIKASI**
2. **Nama Aplikasi :**
3. **Nomor Reg. :**
4. **URL :**
5. **Teknologi :**
6. **Penyelenggara :**
7. **DAFTAR FUNGSI DAN PROSEDUR KEAMANAN**

| ***No.*** | ***Fungsi*** | ***Prosedur*** | ***Check List*** | ***Dok.*** | ***Keterangan*** |
| --- | --- | --- | --- | --- | --- |
| **1.** | **Autentikasi** | 1. **Menggunakan Manajemen Kata Sandi untuk Proses Autentikasi.** |  | **Pranala** |  |
| 1. Menggunakan *Email* Aktif yang Terverifikasi untuk Pendaftaran Akun (jika Pengguna Aplikasi Lebih dari Satu Perangkat Daerah dan atau Publik). |  | Pranala |  |
| 1. Terdapat Menu Ubah Kata Sandi yang Mewajibkan Memasukkan Kata Sandi Pengguna saat ini pada Proses Perubahan Kata Sandi. |  | Pranala |  |
| 1. Menyediakan Fitur Lihat Sementara Kata Sandi Pengguna untuk Membantu Pengguna dalam Memasukan Kata Sandi. |  | Pranala |  |
| 1. Pengguna Wajib Merubah Kata Sandi saat Pertama Kali Masuk ke dalam Aplikasi, jika Akun Penguna Dibuat oleh Pengembang/Admin Aplikasi |  | Pranala |  |
| 1. Penggunaan Kata Sandi Bertingkat Diwajibkan bagi Aplikasi yang Menurut Hasil Penilaian Tim *Asesment* merupakan Aplikasi yang Mengelola Data Penting dan Sangat Rahasia. |  | Pranala |  |
| 1. Menyediakan *Captcha* atau Operasi Hitung pada Halaman *Login* dan Pendaftaran. |  | Pranala |  |
| 1. Menyediakan *Checklist Box* Pernyataan atas Kebenaran Data yang Diberikan pada Halaman Pendaftaran. |  | Pranala |  |
| 1. **Menerapkan Verifikasi Kata Sandi pada Sisi *Server.*** |  | **Pranala** |  |
| 1. Penerapan Kata Sandi sesuai Syarat juga termasuk untuk Kata Sandi pada *Server*. |  | Pranala |  |
| 1. Akun *Default* pada Server Dirubah (Contoh : *root*). |  | Pranala |  |
| 1. **Mengatur Jumlah Karakter, Kombinasi Jenis Karakter dan Masa Berlaku dari Kata Sandi.** |  | **Pranala** |  |
| 1. Panjang Minimal 8 Karakter. |  | Pranala |  |
| 1. Kombinasi antara Huruf Kecil, Huruf Besar, Angka dan Karakter Spesial (Simbol). |  | Pranala |  |
| 1. Dilakukan Validasi dari Sistem, jika Format Tidak Sesuai, maka Tidak Bisa Diproses. |  | Pranala |  |
| 1. Ditambahkan Keterangan Persyaratan Kata Sandi pada Kolom Input Kata Sandi. |  | Pranala |  |
| 1. Masa Berlaku Kata Sandi selama 1 Tahun. |  | Pranala |  |
| 1. Berlaku untuk Pembuatan maupun Perubahan Kata Sandi. |  | Pranala |  |
| 1. **Mengatur Jumlah Maksimum Kesalahan dalam Pemasukan Kata Sandi.** |  | **Pranala** |  |
| 1. Batas Maksimal 5 Kali. |  | Pranala |  |
| 1. Setelah Batas Maksimal, Pengguna Tertahan dan Bisa Input Kembali setelah 3 Menit. |  | Pranala |  |
| 1. **Mengatur Mekanisme Pemulihan Kata Sandi.** |  | **Pranala** |  |
| 1. Pemulihan atau *Reset* Kata Sandi Wajib Dilakukan Mandiri oleh Pengguna. |  | Pranala |  |
| 1. **Menjaga Kerahasiaan Kata Sandi yang Disimpan melalui Mekanisme Kriptografi.** |  | **Pranala** |  |
| 1. Menjaga Kerahasiaan Kata Sandi yang Disimpan pada *Database* melalui Mekanisme Kriptografi Satu Arah. |  | Pranala |  |
| 1. **Menggunakan Jalur Komunikasi yang Diamankan untuk Proses Autentikasi.** |  | **Pranala** |  |
| 1. Menggunakan Jalur Komunikasi yang Diamankan untuk Proses Autentikasi pada *Server.* |  | Pranala |  |
| **2.** | **Manajemen Sesi** | 1. **Menggunakan Pengendali Sesi untuk Proses Manajemen Sesi.** |  | **Pranala** |  |
| 1. **Menggunakan Pengendali Sesi yang Disediakan oleh Kerangka Kerja Aplikasi.** |  | **Pranala** |  |
| 1. **Mengatur Pembuatan dan Keacakan Token Sesi yang Dihasilkan oleh Pengendali Sesi.** |  | **Pranala** |  |
| 1. **Mengatur Kondisi dan Jangka Waktu Habis Sesi.** |  | **Pranala** |  |
| 1. Waktu Habis Sesi (Auto *Logout*) Minimal 10 Menit dan Maksimal 15 Menit. |  | Pranala |  |
| 1. *Logout* dan Kadaluwarsa Membatalkan Token Sesi, sehingga Tombol Kembali pada *Browser* tidak Melanjutkan Sesi Sebelumya. |  | Pranala |  |
| 1. Autentikasi Ulang Dilakukan secara Berkala dalam Waktu 12 Jam (Jika Aplikasi Mengijinkan Pengguna untuk Tetap Masuk) |  | Pranala |  |
| 1. **Validasi dan Pencantuman Session ID.** |  | **Pranala** |  |
| 1. **Pelindungan terhadap Lokasi dan Pengiriman *Token* untuk Sesi Terautentikasi.** |  | **Pranala** |  |
| 1. Aplikasi Tidak Mengungkapkan *Token* Sesi dalam Parameter URL. |  | Pranala |  |
| 1. **Pelindungan terhadap Duplikasi dan Mekanisme Persetujuan Pengguna.** |  | **Pranala** |  |
| 1. Satu Akun Pengguna Tidak Diperbolehkan Digunakan secara Bersamaan di Beda Perangkat. |  | Pranala |  |
| 1. Jika Pemilik Aplikasi Menghendaki Satu Akun Pengguna dapat Digunakan di Beda Perangkat, maka seluruh Risiko menjadi Tanggung Jawab Pemilik Aplikasi. |  | Pranala |  |
| **3.** | **Persyaratan Kontrol Akses** | 1. **Menetapkan Otorisasi Pengguna untuk Membatasi Kontrol Akses.** |  | **Pranala** |  |
| 1. *User Level Manajement* Minimal terdiri dari Tiga Level, yaitu : Superadmin/Admin, Operator dan *Executive*. |  | Pranala |  |
| 1. Semua Atribut Pengguna dan Data serta Informasi yang Digunakan Kontrol Akses Tidak Dapat Dimanipulasi oleh Pengguna. |  | Pranala |  |
| 1. Penjelajahan Direktori Dinonaktifkan. |  | Pranala |  |
| 1. Aplikasi tidak Mengizinkan Pengungkapan Metadata atau Direktori. |  | Pranala |  |
| 1. **Mengatur Peringatan terhadap Bahaya Serangan Otomatis apabila terjadi Akses yang Bersamaan atau Akses yang Terus Menerus pada Fungsi.** |  | **Pranala** |  |
| 1. **Mengatur Antarmuka pada Sisi Administrator.** |  | **Pranala** |  |
| 1. Antarmuka pada Sisi Administrator untuk Pengelolaan Konten sesuai Hak Akses Pengguna. |  |  |  |
| 1. **Mengatur Verifikasi Kebenaran *Token* ketika Mengakses Data dan Informasi yang Dikecualikan.** |  | **Pranala** |  |
| 1. Data dan Informasi agar hanya Bisa Diakses oleh yang Berhak. |  | Pranala |  |
| 1. Aplikasi atau *Framework* Memberlakukan Mekanisme Anti CSRF (*Cross-Site Request Forgery*) yang Kuat. |  | Pranala |  |
| **4.** | **Validasi Input** | 1. **Menerapkan Fungsi Validasi Input pada Sisi *Server*.** |  | **Pranala** |  |
| 1. Data Terstruktur Divalidasi dengan Kuat Menggunakan Penentuan Jenis Karakter, Panjang Karakter dan Pola yang Sesuai. |  | Pranala |  |
| 1. **Menerapkan Mekanisme Penolakan Input jika Terjadi Kesalahan Validasi.** |  | **Pranala** |  |
| 1. Data Tidak Tersimpan jika terjadi Kesalahan pada Proses Validasi. |  |  |  |
| 1. **Memastikan *Runtime Environment* Aplikasi Tidak Rentan terhadap Serangan Validasi Input.** |  | **Pranala** |  |
| 1. **Melakukan Validasi Positif pada Seluruh Input.** |  | **Pranala** |  |
| 1. **Melakukan Filter terhadap Data yang Tidak Dipercaya.** |  | **Pranala** |  |
| 1. Setiap Form atau *Field* Input Pengguna Dilakukan Sanitasi terhadap Jumlah dan Jenis Karakter yang Diizinkan (Tidak Menerima Karakter *Script*). |  | Pranala |  |
| 1. Melakukan *Setting* Anti *XSS* (*Cross Site Scripting*). |  | Pranala |  |
| 1. Melakukan Pelindungan terhadap Serangan LFI (*Local File Inclusion*) atau RFI (*Remote File Inclusion*). |  | Pranala |  |
| 1. **Menggunakan Fitur Kode Dinamis.** |  | **Pranala** |  |
| 1. **Melakukan Pelindungan terhadap Akses yang Mengandung Konten Skrip.** |  | **Pranala** |  |
| 1. Melakukan Pelindungan terhadap Serangan *Xpath Injection* atau *XML Injection Attacks*. |  | Pranala |  |
| 1. **Melakukan Pelindungan dari Serangan Injeksi Basis Data.** |  | **Pranala** |  |
| 1. *Query Sql* Menggunakan *Storage Procedure*. |  | Pranala |  |
| 1. Menerapkan *Function Procedure*. |  | Pranala |  |
| 1. Melakukan *Setting Environment* menjadi *Production*. |  | Pranala |  |
| 1. Aplikasi Tidak Menampilkan *Error System*. |  | Pranala |  |
| **5.** | **Kriptografi** | 1. **Menggunakan Algoritma Kriptografi, Modul Kriptografi, Protokol Kriptografi dan Kunci Kriptografi sesuai dengan Ketentuan Peraturan Perundang-undangan.** |  | **Pranala** |  |
| * Data Pribadi, Penting dan Rahasia Dienkripsi Menggunakan Mekanisme Enkripsi Satu Arah. |  | Pranala |  |
| * Enkripsi tidak Menggunakan Metode atau Algoritma yang tidak Aman. |  | Pranala |  |
| 1. **Melakukan Autentikasi Data yang Dienkripsi.** |  | **Pranala** |  |
| 1. **Menerapkan Manajemen Kunci Kriptografi.** |  | **Pranala** |  |
| 1. **Membuat Angka Acak yang Menggunakan Generator Angka Acak Kriptografi.** |  | **Pranala** |  |
| **6.** | **Penanganan *Error* dan Pencatatan *Log*** | 1. **Mengatur Konten Pesan yang Ditampilkan ketika Terjadi Kesalahan.** |  | **Pranala** |  |
| * Mengatur Tampilan Pesan saat Terjadi Kesalahan atau *Error*. |  | Pranala |  |
| 1. **Menggunakan Metode Penanganan *Error* untuk Mencegah Kesalahan Terprediksi dan tidak Terduga serta Menangani seluruh Pengecualian yang tidak Ditangani.** |  | **Pranala** |  |
| 1. **Tidak Mencantumkan Informasi yang Dikecualikan dalam Pencatatan *Log*.** |  | **Pranala** |  |
| * *Log* tidak Mencatat Informasi Sensitif atau Dikecualikan. |  |  |  |
| 1. **Mengatur Cakupan *Log* yang Dicatat untuk Mendukung Upaya Penyelidikan ketika Terjadi Insiden.** |  | **Pranala** |  |
| * *Log* Mencatat Aktivitas *User*. |  | Pranala |  |
| * *Log* Mencatat Proses Berhasil atau Gagal *Login*. |  | Pranala |  |
| * *Log* Mencatat Kesalahan Validasi Input. |  | Pranala |  |
| * *Log* Mencatat Kesalahan Kontrol Akses. |  | Pranala |  |
| * *Log* Mencatat Informasi tentang Garis Waktu Hari dan Jam Terperinci (DD/MM/YYYY dan HH:MM:SS). |  | Pranala |  |
| 1. **Mengatur Pelindungan *Log* Aplikasi dari Akses dan Modifikasi yang tidak Sah.** |  | **Pranala** |  |
| * *Log* Terlindungi dari Akses Illegal dan Modifikasi. |  |  |  |
| 1. **Melakukan Enkripsi pada Data yang Disimpan untuk Mencegah Injeksi *Log*.** |  | **Pranala** |  |
| 1. **Melakukan Sinkronisasi Sumber Waktu sesuai dengan Zona Waktu dan Waktu yang Benar.** |  | **Pranala** |  |
| * Zona Waktu *Server* Sesuai dan Benar. |  | Pranala |  |
| * Mengatur Rentang Waktu Penyimpanan *Log* sesuai Kebutuhan Aplikasi. |  | Pranala |  |
| **7.** | **Proteksi Data** | 1. **Melakukan Identifikasi dan Penyimpanan Salinan Informasi yang Dikecualikan.** |  | **Pranala** |  |
| 1. **Melakukan Pelindungan dari Akses yang tidak Sah terhadap Informasi yang Dikecualikan yang Disimpan Sementara dalam Aplikasi.** |  | **Pranala** |  |
| 1. **Melakukan Pertukaran, Penghapusan dan Audit Informasi yang Dikecualikan.** |  | **Pranala** |  |
| 1. **Melakukan Penentuan Jumlah Parameter.** |  | **Pranala** |  |
| 1. **Memastikan Data Disimpan dengan Aman.** |  | **Pranala** |  |
| * Menyediakan Prosedur *Backup* Data secara Otomatis Sistem. |  | Pranala |  |
| * Menyediakan Prosedur *Backup* Data secara Manual melalui Superadmin/Admin. |  | Pranala |  |
| * Data yang Di-*Backup* termasuk *File Upload*. |  | Pranala |  |
| * Data *Backup* tersimpan dengan Aman. |  | Pranala |  |
| 1. **Menentukan Metode untuk Menghapus dan Mengekspor Data sesuai Permintaan Pengguna.** |  | **Pranala** |  |
| * Jika Aplikasi Memiliki Fungsi *Export* Data dalam Bentuk *File* (pdf, xls, doc, ppt, dsb.) yang di dalamnya Mengandung Informasi Sensitif, Data Pribadi dan atau Data Rahasia, *File* *Output* Wajib Menggunakan *Password*, Diatur dalam SOP Terpisah. |  | Pranala |  |
| 1. **Membersihkan Memori setelah tidak Diperlukan.** |  | **Pranala** |  |
| **8.** | **Keamanan Komunikasi** | 1. **Menggunakan Komunikasi Terenkripsi.** |  | **Pranala** |  |
| * Aplikasi Menerapkan *Protocol* HTTPS atau SSL. |  | Pranala |  |
| * Komunikasi dengan *Server* Menggunakan Jaringan Internal Pemerintah Kota Probolinggo. |  | Pranala |  |
| 1. **Mengatur Koneksi Masuk dan Keluar yang Aman dan Terenkripsi dari Sisi Pengguna.** |  | **Pranala** |  |
| 1. **Mengatur Jenis Algoritma yang Digunakan dan Alat Pengujiannya.** |  | **Pranala** |  |
| 1. **Mengatur Aktivasi dan Konfigurasi Sertifikat Elektronik yang Diterbitkan oleh Penyelenggara Sertifikasi Elektronik.** |  | **Pranala** |  |
| **9.** | **Pengendalian Kode Berbahaya** | 1. **Menggunakan Analisis Kode dalam Kontrol Kode Berbahaya.** |  | **Pranala** |  |
| 1. **Memastikan Kode Sumber Aplikasi dan Pustaka tidak Mengandung Kode Berbahaya dan Fungsionalitas Lain yang tidak Diinginkan.** |  | **Pranala** |  |
| * Kode Sumber Aplikasi dan *Library* tidak Mengandung *Backdoor* dan Kode Berbahaya Lainnya. |  | Pranala |  |
| 1. **Mengatur Izin terkait Fitur atau Sensor terkait Privasi.** |  | **Pranala** |  |
| * Aplikasi Meminta Izin ke Pengguna sebelum Memanfaatkan Fitur dan Sensor dari Pengguna. |  | Pranala |  |
| * Pastikan Aplikasi hanya Meminta Izin yang Diperlukan. |  | Pranala |  |
| 1. **Mengatur Pelindungan Integritas.** |  | **Pranala** |  |
| * Melakukan Pengaturan CSP (*Content Security Policy*) dan CORS (*Cross Origin Resource Sharing*). |  | Pranala |  |
| 1. **Mengatur Mekanisme Fitur Pembaruan.** |  | **Pranala** |  |
| **10.** | **Logika Bisnis** | 1. **Memproses Alur Logika Bisnis dalam Urutan Langkah dan Waktu yang Realistis.** |  | **Pranala** |  |
| * Alur Bisnis sesuai dengan Alur Bisnis yang Ada dan tidak Melewatkan Langkah Alur Bisnis. |  | Pranala |  |
| * Alur Logika Bisnis dengan semua Langkah Lainnya Diproses dalam Waktu yang Realistis. |  | Pranala |  |
| 1. **Memastikan Logika Bisnis Memiliki Batasan dan Validasi.** |  | **Pranala** |  |
| 1. **Memonitor Aktivitas yang tidak Biasa.** |  | **Pranala** |  |
| 1. **Membantu dalam Kontrol Antiotomatisasi.** |  | **Pranala** |  |
| * Aplikasi Memiliki Kontrol Anti Otomatisasi. |  | Pranala |  |
| 1. **Memberikan Peringatan ketika Terjadi Serangan Otomatis atau Aktivitas yang Tidak Biasa.** |  | **Pranala** |  |
| **11.** | ***File*** | 1. **Mengatur Jumlah *File* untuk Setiap Pengguna dan Kuota Ukuran *File* yang Diunggah.** |  | **Pranala** |  |
| * Aplikasi tidak Menerima *File* dengan Ukuran Besar yang akan Membebani Penyimpanan. |  | Pranala |  |
| 1. **Melakukan Validasi *File* Sesuai dengan Tipe Konten yang Diharapkan.** |  | **Pranala** |  |
| * Aplikasi Melakukan Validasi terhadap *Type*, Ukuran dan Jumlah *File* yang Di-*upload* oleh Pengguna. |  | Pranala |  |
| * Permintaan Langsung ke *File* yang Di-*upload* tidak akan Dijalankan sebagai Konten HTML/*Javascript*. |  | Pranala |  |
| 1. **Melakukan Pelindungan terhadap Metadata Input dan Metadata *File*.** |  | **Pranala** |  |
| * Aplikasi Menerapkan Pengacakan Nama *File* yang Di-*upload* dan Tersimpan di *Server*. |  | Pranala |  |
| * Aplikasi Menyimpan *File* *Upload* di luar *Root Web*. |  | Pranala |  |
| 1. **Melakukan Pemindaian *File* yang Diperoleh dari Sumber yang tidak Dipercaya.** |  | **Pranala** |  |
| 1. **Melakukan Konfigurasi *Server* untuk Mengunduh *File* sesuai Ekstensi yang Ditentukan.** |  | **Pranala** |  |
| **12.** | **Keamanan *Application Programming Interface* dan *Web Service*** | 1. **Melakukan Konfigurasi Layanan Web.** |  | **Pranala** |  |
| * API Dibuat Menggunakan Aplikasi SPLP (Sistem Penghubung Layanan Pemerintah). Proses Integrasi dan Interoperabilitas Data yang Diselenggarakan melalui SPLP Kota Probolinggo Dilaksanakan oleh Unit Khusus di luar Ketentuan. |  | Pranala |  |
| 1. **Memverifikasi *Uniform Resource Identifier* API tidak Menampilkan Informasi yang Berpotensi sebagai Celah Keamanan.** |  | **Pranala** |  |
| * URL API tidak Mengekspose Informasi Sensitif, seperti Kunci API dan *Token* Sesi |  | Pranala |  |
| 1. **Membuat Keputusan Otorisasi.** |  | **Pranala** |  |
| * API yang Dibuat harus Menggunakan *Token*. |  | Pranala |  |
| * API Satuan Data yang harus Dijaga Kerahasiaannya Menggunakan *Token* atau Sistem Enkripsi dan Dekripsi dalam Proses Transaksi Data. |  | Pranala |  |
| 1. **Menampilkan Metode *Restful Hypertext Transfer Protocol* apabila Input Pengguna Dinyatakan Valid.** |  | **Pranala** |  |
| 1. **Menggunakan Validasi Skema dan Verifikasi sebelum Menerima Input.** |  | **Pranala** |  |
| 1. **Menggunakan Metode Pelindungan Layanan Berbasis Web.** |  | **Pranala** |  |
| 1. **Menerapkan Kontrol Antiotomatisasi.** |  | **Pranala** |  |
| **13.** | **Keamanan Konfigurasi** | 1. **Mengonfigurasi *Server* sesuai Rekomendasi *Server* Aplikasi dan Kerangka Kerja Aplikasi yang Digunakan.** |  | **Pranala** |  |
| * Konfigurasi *Server* Disesuaikan dengan Hasil Analisa Kebutuhan Server Aplikasi. |  | Pranala |  |
| 1. **Mendokumentasi, Menyalin Konfigurasi dan Semua Dependensi.** |  | **Pranala** |  |
| 1. **Menghapus Fitur, Dokumentasi, Sampel dan Konfigurasi yang tidak Diperlukan.** |  | **Pranala** |  |
| * Semua Data *Dummy*, Uji Coba dan tidak Diperlukan Dihapus (termasuk *User*, *Role*, *Table*, Kolom *Table*, dll.). |  | Pranala |  |
| 1. **Memvalidasi Integritas Aset jika Aset Aplikasi Diakses secara Eksternal.** |  | **Pranala** |  |
| 1. **Menggunakan Respons Aplikasi dan Konten yang Aman.** |  | **Pranala** |  |
| * Proses Pembuatan dan Pengembangan Aplikasi Dilakukan dengan Cara yang Aman. |  | Pranala |  |
| * *Setting* CSP (*Content Security Policy*) Dilakukan untuk Mengurangi Dampak Serangan XSS (*Cross Site Scripting*). |  | Pranala |  |
| * *Header* Origin yang Disediakan tidak Digunakan untuk Keputusan Autentikasi atau Kontrol Akses, karena *Header* Origin dapat dengan Mudah Diubah oleh Penyerang. |  | Pranala |  |
| * *Setting* CORS (*Cross Origin Resource Sharing*) Menggunakan Daftar *Domain* yang Terpercaya tidak Menggunakan “Null” Atau “\*”. |  | Pranala |  |

1. **KESIMPULAN**

1. **DOKUMENTASI**
2. Surat Undangan
3. Daftar Hadir
4. Foto

Demikian yang dapat kami sampaikan dan atas persetujuannya kami sampaikan terima kasih.

Probolinggo, ………………..

|  |  |  |
| --- | --- | --- |
| *Personal In Charge* Aplikasi,  **(……………………………………………………)** |  | Pelaksana Identifikasi,  **(……………………………………………………)** |