Standar Teknis Keamanan Aplikasi Berbasis Web

Badan Siber dan Sandi Negara (BSSN) telah menerbitkan standar teknis keamanan aplikasi berbasis web yang tertuang dalam Peraturan BSSN Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamananan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik.

- a. Autentikasi
- b. Manajemen Sesi
- c. Persyaratan Kontrol Akses
- d. Validasi Input
- e. Kriptografi pada Verifikasi Statis
- f. Penanganan Eror dan Pencatatan Log
- g. Proteksi Data
- h. Keamanan Komunikasi
- i. Pengendalian Kode Berbahaya
- j. Logika Bisnis
- k. Keamanan File
- l. Keamanan API dan Web Service
- m. Keamanan Konfigurasi

a. Autentikasi

Autentikasi dilakukan dengan:

1. menggunakan manajemen kata sandi untuk proses autentikasi;
2. menerapkan verifikasi kata sandi pada sisi server;
3. mengatur jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi;
   - jumlah karakter minimal 12 karakter;
   - kombinasi jenis karakter minimal terdiri dari huruf besar, huruf kecil, simbol dan angka, tidak ada perulangan karakter;
   - masa berlaku dari kata sandi minimal 6 bulan, dan tidak ada perulangan kata sandi
4. mengatur jumlah maksimum kesalahan dalam pemasukan kata sandi;
5. mengatur mekanisme pemulihan kata sandi;
6. menjaga kerahasiaan kata sandi yang disimpan melalui mekanisme kriptografi; dan
7. menggunakan jalur komunikasi yang diamankan untuk proses autentikasi.

b. Manajemen Sesi

Manajemen sesi dilakukan dengan:

1. menggunakan pengendali sesi untuk proses manajemen sesi;
2. menggunakan pengendali sesi yang disediakan oleh kerangka kerja aplikasi;
3. mengatur pembuatan dan keacakan token sesi yang dihasilkan oleh pengendali sesi;
4. mengatur kondisi dan jangka waktu habis sesi;
5. validasi dan pencantuman session id;
6. pelindungan terhadap lokasi dan pengiriman token untuk sesi terautentikasi; dan
7. pelindungan terhadap duplikasi dan mekanisme persetujuan pengguna.

c. Persyaratan Kontrol Akses

Persyaratan kontrol akses dilakukan dengan prosedur:

1. menetapkan otorisasi pengguna untuk membatasi kontrol akses;
2. mengatur peringatan terhadap bahaya serangan otomatis apabila terjadi akses yang bersamaan atau akses yang terus-menerus pada fungsi;
3. mengatur antarmuka pada sisi administrator; dan
4. mengatur verifikasi kebenaran token ketika mengakses data dan informasi yang dikecualikan

d. Validasi Input

Validasi input dilakukan dengan prosedur:

1. menerapkan fungsi validasi input pada sisi server;
2. menerapkan mekanisme penolakan input jika terjadi kesalahan validasi;
3. memastikan runtime environment aplikasi tidak rentan terhadap serangan validasi input;
4. melakukan validasi positif pada seluruh input;
5. melakukan filter terhadap data yang tidak dipercaya;
6. menggunakan fitur kode dinamis;
7. melakukan pelindungan terhadap akses yang mengandung konten skrip; dan
8. melakukan pelindungan dari serangan injeksi basis data.

e. Kriptografi pada Verifikasi Statis

Kriptografi pada verifikasi statis sebagaimana dilakukan dengan prosedur:

1. menggunakan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan ketentuan peraturan perundang-undangan;
2. melakukan autentikasi data yang dienkripsi;
3. menerapkan manajemen kunci kriptografi; dan
4. membuat angka acak yang menggunakan generator angka acak kriptografi.

f. Penanganan Eror dan Pencatatan Log

Penanganan eror dan pencatatan log dilakukan dengan prosedur:

1. mengatur konten pesan yang ditampilkan ketika terjadi kesalahan;
2. menggunakan metode penanganan eror untuk mencegah kesalahan terprediksi dan tidak terduga serta menangani seluruh pengecualian yang tidak ditangani;
3. mengatur cakupan log yang dicatat untuk mendukung upaya penyelidikan ketika terjadi insiden;
4. mengatur pelindungan log aplikasi dari akses dan modifikasi yang tidak sah;
5. melakukan enkripsi pada data yang disimpan untuk mencegah injeksi log; dan
6. melakukan sinkronisasi sumber waktu sesuai dengan zona waktu dan waktu yang benar.c. tidak mencantumkan informasi yang dikecualikan dalam pencatatan log;
7. mengatur cakupan log yang dicatat untuk mendukung upaya penyelidikan ketika terjadi insiden;
8. mengatur pelindungan log aplikasi dari akses dan modifikasi yang tidak sah;
9. melakukan enkripsi pada data yang disimpan untuk mencegah injeksi log; dan
10. melakukan sinkronisasi sumber waktu sesuai dengan zona waktu dan waktu yang benar.

g. Proteksi Data

Proteksi data dilakukan dengan prosedur:

1. melakukan identifikasi dan penyimpanan salinan informasi yang dikecualikan;
2. melakukan pelindungan dari akses yang tidak sah terhadap informasi yang dikecualikan yang disimpan sementara dalam aplikasi;
3. melakukan pertukaran, penghapusan, dan audit informasi yang dikecualikan;
4. melakukan penentuan jumlah parameter dengan meminimalkan parameter yang di butuhkan untuk request kepada server
5. memastikan data disimpan dengan aman;
6. menentukan metode untuk menghapus dan mengekspor data sesuai permintaan pengguna; dan
7. membersihkan memori setelah tidak diperlukan.

h. Keamanan Komunikasi

Keamanan komunikasi dilakukan dengan prosedur:

1. menggunakan komunikasi terenkripsi;
2. mengatur koneksi masuk dan keluar yang aman dan terenkripsi dari sisi pengguna;
3. mengatur jenis algoritma yang digunakan dan alat pengujiannya; dan
4. mengatur aktivasi dan konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik.

i. Pengendalian Kode Berbahaya

Pengendalian kode berbahaya dilakukan dengan prosedur:

1. menggunakan analisis kode dalam kontrol kode berbahaya;
2. memastikan kode sumber aplikasi dan pustaka tidak mengandung kode berbahaya dan fungsionalitas lain yang tidak diinginkan;
3. mengatur izin terkait fitur atau sensor terkait privasi;
4. mengatur pelindungan integritas; dan
5. mengatur mekanisme fitur pembaruan.

j. Logika Bisnis

Logika bisnis dilakukan dengan prosedur:

1. memproses alur logika bisnis dalam urutan langkah dan waktu yang realistis;
2. memastikan logika bisnis memiliki batasan dan validasi;
3. memonitor aktivitas yang tidak biasa;
4. membantu dalam kontrol antiotomatisasi; dan
5. memberikan peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa.

k. Keamanan File

Keamanan file dilakukan dengan prosedur:

1. mengatur jumlah file untuk setiap pengguna dan kuota ukuran file yang diunggah;
2. melakukan validasi file sesuai dengan tipe konten yang diharapkan;
3. melakukan pelindungan terhadap metadata input dan metadata file;
4. melakukan pemindaian file yang diperoleh dari sumber yang tidak dipercaya; dan
5. melakukan konfigurasi server untuk mengunduh file sesuai ekstensi yang ditentukan.

I. Keamanan API dan Web Service

Keamanan API dan *web service* dilakukan dengan prosedur:

1. melakukan konfigurasi layanan web;
2. memverifikasi uniform resource identifier API tidak menampilkan informasi yang berpotensi sebagai celah keamanan;
3. membuat keputusan otorisasi;
4. menampilkan metode RESTful hypertext transfer protocol apabila input pengguna dinyatakan valid;
5. menggunakan validasi skema dan verifikasi sebelum menerima input;
6. menggunakan metode pelindungan layanan berbasis web; dan
7. menerapkan kontrol antiotomatisasi.

m. Keamanan Konfigurasi

Keamanan konfigurasi dilakukan dengan prosedur:

1. mengonfigurasi server sesuai rekomendasi server aplikasi dan kerangka kerja aplikasi yang digunakan;
2. mendokumentasi, menyalin konfigurasi, dan semua dependensi;
3. menghapus fitur, dokumentasi, sampel, dan konfigurasi yang tidak diperlukan;
4. memvalidasi integritas aset jika aset aplikasi diakses secara eksternal; dan
5. menggunakan respons aplikasi dan konten yang aman.