STANDAR KEAMANAN APLIKASI BERBASIS WEB

Nomor Dokumen	: 067/90.10/Diskominfo.04
Revisi	: 0.0
Tanggal Terbit	: 10 Januari 2022

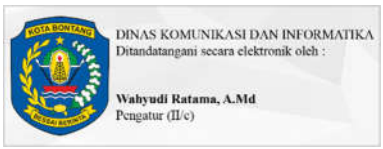
DINAS KOMUNIKASI DAN INFORMATIKA KOTA BONTANG

HALAMAN PENGESAHAN

Disiapkan Oleh :

1. Hendy Safari, A.Md

2. Wahyudi Ratama, A.Md



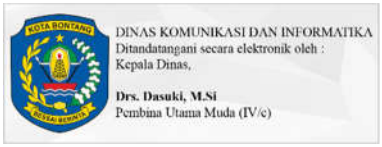
Diperiksa Oleh :

1. Kepala Bidang Statistik dan Persandian,
   Ilham Wahyudi, S.Si

2. Kepala Seksi Tata Kelola Keamanan dan Persandian,
   Nur Alam, S.E

Disetujui Oleh :

Kepala Dinas,
Drs. Dasuki, M.Si



Password : 123

RIWAYAT PERUBAHAN

Rev	Tanggal	Uraian	Penanggungjawab
0.0		Terbitan Awal	Kepala Dinas, Drs. Dasuki, M.Si

1. Tujuan

Mencegah/meminimalisir celah kerawanan suatu Aplikasi berbasis Web, melalui fitur-fitur, code pemograman dan celah kerawanan lainnya yang berasal dari proses awal pembangungan suatu Aplikasi berbasis Web.

2. Ruang Lingkup

Standar ini berlaku untuk :
Seluruh Aplikasi berbasis Web yang dibuat oleh seluruh Perangkat Daerah termasuk Dinas Komunikasi dan Informatika Kota Bontang, baik melalui Pihak Ketiga ataupun Tenaga Ahli lainnya. Dan akan dihosting pada server Website/Aplikasi Pemerintah Kota Bontang yang dikelola oleh Dinas Komunikasi dan Informatika Kota Bontang.

3. Istilah dan Definisi

a.	Framework	:	Sebuah kerangka kerja yang digunakan untuk mengembangkan Aplikasi berbasis Desktop atau Aplikasi berbasis Website.
b.	Native PHP	:	Membuat suatu aplikasi berbasis website dengan PHP yang dimulai dari Nol.
c.	Object Oriented Programming (OOP)	:	Pemrograman yang berorientasi pada objek yang merupakan model pemrograman komputer dengan pengaturan desain perangkat lunak di sekitar data atau objek.
d.	Captcha	:	Jenis/Fitur tindakan keamanan yang dikenal sebagai autentikasi tantangan-tanggapan untuk membedakan komputer dan manusia.
e.	Kriptografi	:	Disiplin ilmu yang mempelajari teknik enkripsi naskah asli (*plaintext*) yang tersusun acak, dengan memanfaatkan kunci enkripsi sehingga naskah tersebut berubah menjadi teks yang sulit terbaca (*ciphertext*) oleh user yang tidak memiliki kunci dekripsi.
f.	Application Programming Interface (API)	:	Sekumpulan definisi dan protokol untuk membangun dan mengintegrasikan perangkat lunak aplikasi.

Sesuai dengan ketentuan peraturan perundang-undangan yang berlaku, surat ini telah ditandatangani secara elektronik yang tersertifikasi oleh Balai Sertifikasi Elektronik (BSrE) sehingga tidak diperlukan tanda tangan dan stempel basah.

g. Web Service : Mekanisme komunikasi dua aplikasi/mesin terlepas dari arsitektur dan teknologi yang digarisbawahi.

h. Uniform Resource Identifier (URI) : Sebuah alamat yang menunjuk ke sebuah resource di internet. URI biasanya terdiri dari bagian yang disebut skema (scheme) yang diikuti sebuah alamat.

i. RESTful HTTP : Suatu arsitektur metode komunikasi yang menggunakan protokol HTTP untuk pertukaran data dan metode ini sering diterapkan dalam pengembangan aplikasi.

4. Referensi

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.

5. Standar

5.1. Code Pemrograman

a. Menggunakan *Framework* minimal :

No.	Framework	Versi
1	Yii	1.0 – terbaru
2	Codeigniter	3.1.11 – terbaru
3	Laravel	7.0 – terbaru

Diperbolehkan untuk tidak menggunakan *Framework* yang tersebut diatas, selama menggunakan *Framework* dengan stable version keluaran diatas tahun 2019.

b. Menggunakan Code Pemrograman *Native PHP* dengan menerapkan konsep *OOP* dan menggunakan bahasa pemograman minimal PHP 7.

c. Semua Resource/Library (seperti Library Font, Datatable pada Bootstrap) pemograman harus berada di dalam Folder Aplikasi.

5.2. Autentikasi

a. Menggunakan manajemen kata sandi untuk proses autentikasi.

b. Mengatur jumlah karakter (minimal 8 karakter) dan kombinasi jenis karakter (minimal menggunakan 3 dari 4 jenis karakter yaitu Huruf Kecil, Huruf Besar, Bilangan dan Karakter Khusus seperti @#$%^&*()[]{}) dari kata sandi.

c. Mengatur jumlah maksimum kesalahan dalam pemasukan kata sandi.

d. Mengatur mekanisme pemulihan kata sandi.

e. Menambahkan *Captcha* pada setiap halaman Login.

f. Menerapkan mekanisme *Kriptografi* minimal SHA256 untuk menjaga kerahasiaan kata sandi.

5.3. Manajemen Sesi

a. Menggunakan pengendali sesi untuk proses manajemen sesi.

b. Menggunakan pengendali sesi yang disediakan oleh *Framework* Aplikasi.

c. Mengatur kondisi dan jangka waktu habis sesi.

5.4. Kontrol Akses

a. Menetapkan otorisasi pengguna untuk membatasi kontrol akses.

b. Mengatur peringatan terhadap bahaya serangan otomatis apabila terjadi akses yang bersamaan atau akses yang terus-menerus pada fungsi.

5.5. Validasi Input

a. Menerapkan mekanisme penolakan input jika terjadi kesalahan validasi.

b. Melakukan filter terhadap data yang tidak dipercaya.

c. Melakukan perlindungan terhadap akses yang mengandung konten skrip dan serangan injeksi basis data.

5.6. Notifikasi Error dan Pencatatan Log Aplikasi

a. Mengatur konten pesan yang ditampilkan ketika terjadi kesalahan.

b. Mengatur cakupan log yang dicatat untuk mendukung upaya penyelidikan ketika terjadi insiden.

c. Mengatur perlindungan log aplikasi dari akses dan modifikasi yang tidak sah.

5.7. File

a. Mengatur jumlah file untuk setiap pengguna dan kuota ukuran file yang diunggah.

b. Melakukan validasi file sesuai dengan tipe konten yang diharapkan.

c. Melakukan perlindungan terhadap metadata input dan metadata file.

Sesuai dengan ketentuan peraturan perundang-undangan yang berlaku, surat ini telah ditandatangani secara elektronik yang tersertifikasi oleh Balai Sertifikasi Elektronik (BSrE) sehingga tidak diperlukan tanda tangan dan stempel basah.

5.8. Keamanan API dan *Web service*

a. Memverifikasi *URI* dari *API* tidak menampilkan informasi yang berpotensi sebagai celah keamanan.

b. Menampilkan metode *RESTful HTTP* apabila input pengguna dinyatakan valid.

c. Menerapkan kontrol antiotomatisasi.

6. Penutup

Hal-hal lain yang belum tertuang dalam ketentuan ini, karena adanya perubahan kebijakan eksternal ataupun internal maka akan diadakan penyesuaian lebih lanjut dan merupakan bagian yang tidak terpisahkan dengan ketentuan ini.

Sesuai dengan ketentuan peraturan perundang-undangan yang berlaku, surat ini telah ditandatangani secara elektronik yang tersertifikasi oleh Balai Sertifikasi Elektronik (BSrE) sehingga tidak diperlukan tanda tangan dan stempel basah.