Catatan Rilis — CMS Sekolahku v3.2.0

> Tanggal rilis: 13 Oktober 2026 · Versi sebelumnya: v3.1.2 Dokumen ini menjelaskan semua perubahan dalam bahasa sehari-hari untuk pengguna non-IT.

1. Tampilan Website Baru

Seluruh tampilan website depan diganti dengan sistem multi-theme: tiga tema bawaan — **Nusantara** (navy-merah, aktif bawaan), **Cakrawala** (biru-kuning), dan **Lentera** (hijau) — lengkap dengan menu jelajah 13 halaman dan footer baru. **Halaman admin tidak berubah sama sekali** — cara kerja admin seperti biasa.

Multi-theme: website mendukung lebih dari satu tema tampilan. Tema aktif bernama `nusantara` dan bisa diganti lewat **Admin → Settings → Tema Tampilan** (menggantikan pengaturan "Warna Tema" yang lama). Menambah tema baru cukup dengan membuat folder baru — bila ada file yang kurang, otomatis memakai file tema `nusantara` sehingga halaman tetap tampil.

Menu dinamis: halaman statis baru (dan menu kustom) dari **Admin → Menus** ikut tampil di panel jelajah, disusul setelah 13 halaman bawaan dengan nomor lanjutan. Halaman yang masih draft otomatis tidak ditampilkan; terbitkan halaman agar tautannya muncul.

2. Satu Halaman Panjang → Banyak Halaman

Keluhan utama versi lama: semua konten menumpuk di beranda sehingga scroll sangat panjang. Sekarang tiap bagian punya halaman sendiri:

Dulu (1 halaman)	Sekarang (halaman sendiri)
Beranda (semua)	Beranda — hanya ringkasan + tautan "Lihat semua"
Profil	`/profile`
Program	`/program`
Pengajar	`/teachers`
Prestasi	`/achievements`
Ekstrakurikuler	`/extracurriculars`
Testimoni	`/testimonials`
Galeri	`/gallery`
Agenda	`/agenda`
FAQ	`/faq`
Berita, Download, Kontak	Tetap `/news`, `/downloads`, `/contact`

3. Istilah PPDB → SPMB

Mengikuti istilah resmi pemerintah, semua tulisan dan link PPDB menjadi **SPMB** (Seleksi Penerimaan Murid Baru), termasuk bagian penerimaan di beranda (`#spmb`).

Bagian penerimaan di beranda kini menampilkan **"10 Langkah Mudah Mendaftar"** — dari Identitas Diri sampai Finalisasi & Cetak PDF — lengkap dengan progress bar yang memandu calon siswa tahap demi tahap.

Beda jenjang, beda tahapan: isi tiap langkah bisa diubah lewat **Admin → Settings → Tahapan SPMB** (tambah, hapus, atau susun ulang). Untuk sekolah SD/SMP/SMA yang tahapannya berbeda (misalnya Nilai Rapor tematik vs per mata pelajaran), tersedia tombol **Preset SD/SMP/SMA** untuk menyesuaikan cepat.

4. Alamat Halaman Berbahasa Inggris

Alamat halaman kini Inggris (`/profile`, `/teachers`, ...). **Penting:** alamat lama (`/profil`, `/pengajar`, ...) tidak aktif lagi — perbarui bookmark, dan tautan dari media sosial/brosur bila ada. Alamat `/kontak` dihapus, gunakan `/contact`.

5. Halaman Berita Lebih Lengkap

- **Daftar berita** (`/news`): ada foto pengganti otomatis bila berita belum punya gambar, ada tombol Cari + Reset, saringan kategori langsung aktif saat diklik.
- **Detail berita**: ada kolom kanan berisi Pencarian, Kategori, Berita Terbaru, Arsip, Tags, dan Ikuti Kami (pada tema Nusantara; tema Cakrawala/Lentera tampil satu kolom tanpa sidebar). Komentar pengunjung tetap masuk ke admin untuk disetujui.

6. Perbaikan Lain

- Tulisan copyright footer yang dobel ("© 2026 ... © 2026 ...") sudah benar.
- Upload foto kepala sekolah yang dulu error sudah bisa (perlu izin folder, lihat panduan upgrade bila error).
- Tombol "Jelajahi Sekolah" yang sempat salah alamat sudah benar ke `/profile`.
- Teks berjalan di beranda kini otomatis terisi dari pengumuman, berita, agenda, dan prestasi terbaru — tidak perlu diketik manual.
- Foto kepala sekolah hanya tampil di bagian sambutan (tidak dobel di mana-mana).
- **Tingkat prestasi tersimpan** — dulu pilihan tingkat (Nasional, Provinsi, ...) di admin gagal tersimpan; sekarang bisa.
- **Status agenda otomatis** — status acara (Akan Datang/Berlangsung/Selesai) kini mengikuti tanggal dengan sendirinya; pilihan status manual di form admin dihapus.
- **Form kontak/komentar** — kirim ulang tanpa reload halaman tidak lagi error 403.
- **Form tambah/edit halaman & berita di admin** — penyunting teks (Quill) tidak menangkap isinya karena salah menempel ke form logout; konten selalu dianggap kosong. Sekarang sudah benar.
- **Komponen internal (dependency) diperbarui** — CodeIgniter 4.7.4 → 4.7.5 dan 4 komponen pendukung (deep-copy, php-parser, phpunit, recursion-context). Hanya versi kecil (bugfix), tidak mengubah cara pakai.

- **Status menu kini jelas** — menu bawaan (System) selalu tampil dan kini ditandai **"Bawaan"** (sebelumnya menampilkan tombol Aktif/Nonaktif yang menyesatkan). Status **Aktif/Nonaktif** benar-benar berlaku untuk menu **Custom** dan **Halaman** (menu halaman mengikuti terbit/draft halamannya).
- **Keterangan cache menu diperbaiki** — sebelumnya tertulis perubahan menu baru tampil setelah 5 menit dan ada tombol ?nocache; nyatanya perubahan menu langsung tampil begitu disimpan.
- **Arti kolom "Urutan" menu diperjelas** — kolom Urutan (dan seret baris) hanya mengatur urutan menu **Custom & Halaman** di panel jelajah, dan urutan daftar di halaman admin. Urutan 13 halaman bawaan tema tetap mengikuti tema, jadi menggeser baris System tidak mengubah header. Menu anak (dropdown) juga hanya mengubah struktur daftar — tema belum menampilkan dropdown, sehingga anak menu tidak muncul di navigasi depan.
- **Tombol Hapus tidak lagi error 403 setelah aksi cepat** — dulu, setelah memakai **Quick Edit** (berita) atau **menyeret baris** (galeri, guru, program, ekskul, prestasi, testimoni, FAQ, download, menu), semua tombol **Hapus** di halaman itu (termasuk tombol Logout) gagal dengan pesan error, karena kode keamanan (CSRF) sudah berganti tetapi form masih memakai yang lama. Kini kode keamanan diperbarui otomatis di seluruh halaman setiap aksi cepat berhasil — tanpa perlu reload.
- **Sakelar "Tampil di website" kini benar-benar berfungsi** — pada **Guru, Program, Ekstrakurikuler, Testimoni, dan Prestasi**, mematikan sakelar "Tampil di website" dulu tidak berefek: item tetap muncul di halaman depan. Sekarang item yang disembunyikan tidak lagi tampil di halaman publik (dan beranda), dan daftar admin menampilkan kolom **Status** (**Tampil**/**Tersembunyi**) agar terlihat jelas item mana yang disembunyikan.
- **Kolom "URL" pada Program kini berfungsi** — dulu mengisi **Link URL** di Program tidak berefek: kartu program selalu mengarah ke tombol SPMB. Sekarang kartu program di halaman **Program** dan cuplikan **Beranda** mengarah ke URL yang diisi (bila kosong, tetap ke tombol SPMB bawaan). Catatan: isian **Ikon** (Font Awesome) memang belum ditampilkan tema, dan form admin kini memberi keterangan agar tidak menyesatkan.
- **Ikon & warna Ekstrakurikuler kini tampil di website** — dulu mengisi **Ikon** dan **Warna Ikon** di Ekskul tidak berefek: halaman Ekstrakurikuler hanya menampilkan judul dan deskripsi. Sekarang ikon berwarna tampil pada label setiap kegiatan di ketiga tema (Font Awesome ikut dimuat di tema, sama seperti panel admin). Beberapa isian form admin Ekskul (judul, deskripsi, ikon, warna) juga diamankan agar tidak bisa menyusupkan HTML.
- **Foto & urutan Prestasi kini berfungsi di website** — dulu mengisi **URL Foto** di Prestasi tidak berefek: halaman **Prestasi** tidak menampilkan foto. Sekarang foto siswa tampil bulat di samping nama pada ketiga tema. Selain itu, **seret baris** di daftar Prestasi dulu hanya berlaku antar-item bertahun sama (daftar diurutkan per tahun lebih dulu), sehingga memindahkan item ke kelompok tahun lain seolah berhasil tetapi tidak berpengaruh setelah halaman dimuat ulang. Kini urutan sepenuhnya mengikuti kolom **Urutan** — apa yang Anda seret itulah yang tampil di website. **Tahun** juga kini wajib diisi (otomatis berisi tahun berjalan bila dikosongkan) sehingga tidak ada lagi prestasi bertahun kosong yang tampil sebagai bagian tahun "0000".
- **Agenda: urutan, status, dan tanggal diperbaiki** — (1) isian **Urutan** pada Agenda dulu tidak berpengaruh apa pun (daftar selalu urut tanggal); kini dipakai sebagai penentu urutan untuk acara di **tanggal yang sama**, dan kolom **Urutan** ditampilkan di daftar admin. (2) Agenda yang **sudah lewat** dulu

masih bisa muncul di halaman Agenda/beranda/dashboard sebagai "agenda mendatang" karena penyaringnya memakai kolom status yang tidak pernah diperbarui — kini penyaring memakai tanggal, jadi acara lewat tidak lagi tampil (badge status di admin sudah benar sejak awal). (3) Kolom **Tanggal** kini benar-benar wajib di server — sebelumnya agenda tanpa tanggal tetap bisa tersimpan sebagai `0000-00-00`.

- **Galeri: kategori, unggulan, dan keamanan diperbaiki** — (1) isian **Kategori** dulu tersimpan tetapi tidak tampil di mana pun; kini menjadi **tab penyaring** di halaman Galeri dan label kecil pada setiap foto. (2) Centang **Gambar unggulan** dulu tidak berefek; kini foto unggulan tampil **lebih dulu** dan diberi tanda ★ **Unggulan**. (3) **Gambar kini wajib** — sebelumnya item galeri tanpa gambar bisa tersimpan, padahal item seperti itu tidak pernah muncul di website. (4) Menghapus item galeri kini lebih aman (file foto dihapus setelah baris database benar-benar terhapus), pesan "tidak ditemukan" muncul saat mengubah/menghapus data yang sudah tiada, dan isian form Galeri diamankan agar tidak bisa menyusupkan HTML.

- **FAQ: urutan, tampilan, dan keamanan diperbaiki** — (1) Isian **Kategori** dulu membuat daftar di halaman FAQ dikelompokkan per kategori, sehingga kolom **Urutan** tidak lagi berpengaruh penuh (item kategori pertama selalu mendahului item kategori berikutnya walau nomor urutnya lebih besar). Kini urutan tampil sepenuhnya mengikuti kolom **Urutan**, dan judul kategori tetap muncul mengikuti urutan item. (2) Jawaban yang ditulis **beberapa baris** kini tampil berbaris (sebelumnya semua baris menyatu jadi satu paragraf panjang). (3) Isian form FAQ diamankan agar tidak bisa menyusupkan HTML, **Pertanyaan dibatasi 255 karakter** (sesuai kapasitas kolom — dulu kelebihan karakter dipotong diam-diam), dan pesan kesalahan kini berbahasa Indonesia. (4) Mengubah/menghapus FAQ yang sudah tiada tidak lagi melapor "berhasil". Daftar admin kini menampilkan kolom **Status** (**Tampil**/**Tersembunyi**), pilihan **Kategori** diambil dari kategori yang sudah pernah dipakai, dan tampilan tanggal dibuat seragam.

- **Halaman Statis: alamat (slug), menu, dan gambar diperbaiki** — (1) Mengubah **Judul** dulu otomatis mengubah **alamat halaman** (`/{slug}`), sehingga tautan lama (bookmark, tautan dari media sosial, hasil pencarian) mati; kini alamat halaman **tetap** dan tersedia kolom **Slug** untuk mengganti alamat bila memang dikehendaki. (2) Mematikan sakelar **Tambah ke menu navigasi** dulu hanya melepas keterkaitan dari halaman, tetapi tautannya **tetap tampil** di menu; kini tautan benar-benar dihapus. (3) Isian **URL Gambar** (gambar sampul halaman + pratinjau berbagi) dulu tidak tersedia di form padahal dipakai website; kini bisa diisi. (4) Isian form Halaman diamankan agar tidak bisa menyusupkan HTML, **Meta Title/Description dibatasi 255 karakter** (dulu kelebihan karakter dipotong diam-diam) dengan pesan berbahasa Indonesia, alamat yang bentrok dengan halaman bawaan (mis. `news`) otomatis diberi akhiran agar halaman tetap bisa dibuka, mengubah/menghapus halaman yang sudah tiada tidak lagi melapor "berhasil" atau memicu error, dan daftar admin menampilkan kolom **Menu**.

- **Pesan Masuk: keamanan dan tampilan diperbaiki** — (1) Tombol **Hapus** di halaman detail pesan dulu menampilkan **nama pengirim** di dalam dialog konfirmasi dengan cara yang membuat nama berisi tanda petik dapat **menyusupkan kode** yang berjalan di browser admin (siapa pun bisa mengirim nama semacam itu lewat form kontak). Kini konfirmasi memakai kotak dialog biasa dan nama hanya tampil sebagai teks. (2) Menghapus pesan yang sudah tidak ada tidak lagi melapor "berhasil" (kini "Pesan tidak ditemukan."). (3) Tiga label di Dashboard diperjelas agar sesuai isinya: "Pesan Masuk" → **Pesan Belum Dibaca**, "Komentar" → **Komentar Menunggu**, dan judul blok "Pesan Baru" → **Pesan Terbaru**. (4) Pesan kesalahan pada form kontak publik kini berbahasa Indonesia (sebelumnya berbahasa Inggris, mis. "The email field must contain a valid email address."). (5) Daftar pesan kini punya **penyaring**

status — Semua / **Belum dibaca** / **Sudah dibaca** (dengan jumlah masing-masing), tombol **Tandai sudah dibaca**/**Tandai belum dibaca** per pesan, dan **Hapus terpilih** (centang beberapa pesan sekaligus) — sebelumnya menandai pesan kembali "belum dibaca" dan menghapus banyak pesan sekaligus tidak mungkin dilakukan dari daftar. (6) Form kontak kini **dibatasi 5000 karakter** per pesan (dulu pesan panjang dipotong diam-diam tanpa peringatan) dan **dibatasi per alamat jaringan** (5 kiriman per 10 menit), sehingga batas 1 pesan/30 detik yang dulu bisa dilewati cukup dengan menghapus cookie tidak lagi mudah ditembus bot. (7) Urutan daftar pesan yang waktu kirimnya sama tidak lagi berpotensi tertukar antar halaman.

- **Komentar Berita: tombol Balas, moderasi, dan keamanan diperbaiki** — (1) Menekan tombol **Balas** pada komentar dulu **tidak melakukan apa pun** (tidak ada reaksi sama sekali); kini tombol itu mengisi kolom balasan dengan nama komentator yang dibalas dan menampilkan penanda **"Membalas … · Batal"** di atas form, sehingga balasan bisa ditujukan dengan benar pada ketiga tema. (2) Daftar **Komentar** kini punya **penyaring status** — Semua / **Menunggu** / **Disetujui** (dengan jumlah masing-masing) — plus **Setujui terpilih** dan **Hapus terpilih** (centang beberapa komentar sekaligus), dan tombol **Tolak** yang selama ini hanya ada di panduan kini benar-benar tersedia untuk komentar yang masih menunggu. (3) Kolom **Berita** pada daftar dulu hanya menampilkan **angka** id artikel — kini menampilkan **judul berita** yang bisa diklik ke artikelnya, dan **email** komentator ikut tampil di bawah namanya. (4) Menyetujui/menolak/menghapus komentar yang sudah tidak ada tidak lagi melapor "berhasil" (kini "Komentar tidak ditemukan."). (5) Pesan kesalahan form komentar kini berbahasa Indonesia (sebelumnya Inggris, mis. "The name field must be at least 3 characters in length."). (6) Komentar kini **dibatasi 2000 karakter** di server, dan penghitung karakter di form benar-benar berjalan (dulu label tertulis "0/500" sementara batas kolom 2000 dan server menerima pesan sepanjang apa pun lalu memotongnya diam-diam tanpa peringatan). (7) Selain batas 1 komentar/30 detik per sesi, komentar kini juga **dibatasi per alamat jaringan** (5 komentar per 10 menit), sehingga bot yang menghapus cookie tidak mudah menembusnya. (8) Komentar yang dikirim ke **berita yang masih draft** kini ditolak (dulu bisa tersimpan meski halamannya tidak bisa dibuka). (9) Kiriman komentar dengan **ID balasan palsu** dulu membuat halaman publik menampilkan **error 500**; kini diabaikan dengan aman (balasan hanya diterima untuk komentar yang benar-benar ada, sudah disetujui, dan berasal dari artikel yang sama). (10) Urutan daftar komentar yang waktu kirimnya sama tidak lagi berpotensi tertukar antar halaman. (11) Halaman detail berita tidak lagi di-cache 5 detik: dulu pesan kesalahan form bisa **hilang** (form terkirim dari halaman versi lama) dan isi form (nama/email) pengunjung sebelumnya bisa ikut tersimpan di cache lalu tampil ke pengunjung lain.

- **Menu Navigasi: keamanan, urutan, dan tampilan diperbaiki** — (1) **Seret baris** di daftar Menu dulu membuat kolom **Status** berubah menjadi angka dan kolom **Urutan** tidak ikut diperbarui; kini kolom yang benar yang diperbarui. (2) Bila urutan ditolak server (mis. memindahkan menu ke bawah anaknya sendiri), halaman dulu seolah berhasil — baris tetap bergeser padahal tidak tersimpan; kini muncul pemberitahuan berisi alasannya, lalu daftar dimuat ulang agar sesuai data tersimpan. (3) Ada celah yang membuat susunan menu bisa **berputar** (A di bawah B, B di bawah C, C di bawah A): menu tersebut lalu **hilang dari daftar** dan membuka edit/urutan berikutnya membuat halaman error berat. Kini susunan berputar **ditolak saat disimpan**, dan bila data lama sudah terlanjur berputar, daftar tetap bisa dibuka serta menampilkan peringatan berisi jumlah item yang tidak tampil. (4) Isian **Target** dan **Kunci Section** kini diperiksa di server (sebelumnya nilai apa pun dari luar form bisa tersimpan), dan **URL** tidak boleh sama dengan item menu/halaman lain (dulu bisa muncul dua tautan kembar). (5) URL menu yang menunjuk pengaturan berisi skema berbahaya (`javascript:`) tidak lagi ditampilkan di navigasi depan. (6) Menu **Halaman** kini bisa dibuka lewat tombol edit untuk mengatur induk &

urutannya (sebelumnya ikut terkunci seperti menu bawaan) — tombol hapus tetap hanya untuk menu **Custom** — dan kolom **URL** tidak lagi menampilkan garis miring ganda untuk tautan luar. (7) Anak menu kini benar-benar menjorok di daftar admin.

- **Pengguna: keamanan dan tampilan diperbaiki** — (1) Form **Tambah/Edit Pengguna** kini meminta **Konfirmasi Kata Sandi**, sehingga salah ketik sandi tidak lagi membuat akun baru tidak bisa dipakai. (2) Isian form tidak lagi hilang saat ada kesalahan pengisian (dulu semua kolom kembali kosong). (3) Nama Lengkap tidak lagi bisa dipakai menyisipkan kode berbahaya: dulu seorang **Editor** dapat menulis kode di nama lengkapnya sendiri, dan kode itu **berjalan di browser Superadmin** saat Superadmin membuka halaman edit pengguna tersebut. (4) Menu **Pengguna** di sidebar kini **hanya tampil untuk Superadmin** (dulu Admin/Editor juga melihatnya, lalu ditolak dengan "Akses ditolak"). (5) Kolom **Terakhir Login** kini benar-benar terisi setiap kali pengguna login (dulu selalu "-"). (6) Menghapus pengguna yang sudah tidak ada tidak lagi melapor "berhasil" (kini "Pengguna tidak ditemukan."). (7) Perubahan **peran** atau **menonaktifkan akun** kini langsung berlaku — pengguna yang sedang login langsung kehilangan akses tanpa harus logout dulu (dulu peran lama tetap dipakai sampai logout), dan pesan kesalahan pengisian pengguna kini berbahasa Indonesia.

- **Pengaturan Situs: keamanan, unggahan, dan tampilan diperbaiki** — (1) Isian **Banner Halaman**, **tautan Program & Layanan di footer**, **logo teks**, dan **judul bagian Hero** kini tidak lagi bisa dipakai menyisipkan kode yang berjalan di browser pengunjung (dulu isi kolom Pengaturan tercetak mentah ke halaman depan); HTML pada judul Hero kini tampil sebagai teks biasa. (2) **Banner halaman**, **tautan Program & Layanan di footer**, dan **logo teks** kini benar-benar tampil di ketiga tema — sebelumnya isian itu tersimpan tetapi tidak pernah dipakai tema (footer selalu menampilkan daftar bawaan). Bila dibiarkan kosong, teks bawaan tema yang dipakai, jadi tampilan lama tidak hilang. (3) Tautan (media sosial, tombol Hero, URL SPMB, dan daftar tautan footer) kini diperiksa di server: skema berbahaya seperti `javascript:` ditolak dan nilai lama dipertahankan (tautan footer otomatis menjadi `#`), bukan disimpan lalu dipasang sebagai tautan. (4) **Email kontak** kini diperiksa di server (dulu nilai apa pun tersimpan). (5) Unggahan gambar **Tentang Kami** & **Kepala Sekolah** kini divalidasi: berkas yang bukan gambar, ukuran melebihi batas server/5 MB, atau dimensi melebihi ±25 MP ditolak dengan pesan yang jelas dan **gambar lama dipertahankan** (dulu berkas apa pun diproses dan dapat memicu error). (6) Menyimpan Pengaturan tidak lagi **menghapus** data yang tidak ada di form — mis. sisa data versi lama seperti `role_title`/`sambutan` pada Kepala Sekolah — dan satu baris **Keunggulan** berisi "0" tidak lagi ikut terbuang. (7) Menyimpan setelan kini memakai satu perintah atomik per kunci, sehingga dua penyimpanan yang bersamaan tidak lagi dapat membuat baris setelan ganda (yang membuat nilai yang tampil bisa acak). (8) Setting **warna tema** (`theme_color`) dihapus karena sudah tidak dipakai sejak adanya **Tema Tampilan**.

- **Testimoni: keamanan, foto, dan urutan diperbaiki** — (1) Isian form **Testimoni** (nama, peran, kutipan, URL foto) dulu dicetak mentah: nama atau foto berisi tanda petik dapat **menjebol form** sehingga kode berbahaya berjalan di browser admin yang membuka halaman **Edit** (siapa pun yang bisa masuk admin — termasuk Editor — dapat menanam kode yang berjalan di browser Superadmin). Kini semua isian ditampilkan sebagai teks biasa. (2) Isian **URL Foto** kini benar-benar berfungsi: dulu tersimpan tetapi tidak pernah dipakai website, sehingga foto testimoni tidak pernah muncul. Sekarang foto tampil **bulat** di halaman **Testimoni** dan pada kutipan di **Beranda** ketiga tema — bila foto dikosongkan, tampilan lama (tanda kutip/inisial) yang dipakai. (3) Menghapus testimoni yang sudah tidak ada tidak lagi melapor "berhasil" (kini "Testimoni tidak ditemukan."). (4) Isian form tidak lagi hilang saat ada kesalahan pengisian (dulu nama/peran/kutipan/foto/sakelar kembali kosong). (5) Pesan kesalahan

pengisian kini berbahasa Indonesia (dulu mis. *"The name field must be at least 3 characters in length."*), dan judul halaman admin "Testimonial" → **Testimoni**. (6) Kutipan panjang yang dipotong di daftar admin tidak lagi memotong di tengah huruf beraksen (dulu muncul karakter rusak "�"); perbaikan yang sama juga diterapkan pada daftar **Program** dan **Galeri**. (7) **Seret baris** pada daftar yang lebih dari satu halaman dulu menulis ulang nomor urut mulai dari 0, sehingga urutan **halaman ke-2 menimpa halaman pertama** dan item berpindah-pindah setelah dimuat ulang; kini nomor urut mengikuti halaman yang sedang dibuka. Perbaikan yang sama berlaku untuk **Guru, Program, Ekstrakurikuler, Prestasi, Download, FAQ, dan Galeri**. (8) Bila server menolak pengurutan, halaman tidak lagi seolah berhasil — muncul pemberitahuan berisi alasannya lalu daftar dimuat ulang (pola yang sudah dipakai di menu **Menu**).

- **Alamat sekolah di footer tidak lagi dobel** — sebelumnya alamat tampil dua kali: di kolom deskripsi (kiri) dan di kolom Kontak (kanan). Kini alamat hanya tampil sekali di kolom **Kontak** pada ketiga tema (Nusantara, Cakrawala, Lentera).

- **Teks Keunggulan di Beranda lebih mudah dibaca** — pada tema **Nusantara**, bagian **Keunggulan** (section 03) kini memakai huruf tanpa kait (sans-serif) yang lebih jelas untuk kalimat seperti "Terakreditasi A oleh BAN-S/M", dan setiap keunggulan hanya tampil **sekali** di kartunya (sebelumnya kalimat yang sama tampil dua kali). Perbaikan yang sama berlaku pada bagian **Budaya Sekolah** di halaman Profil.

- **Keamanan halaman Berita diperketat** — kata kunci pencarian serta parameter kategori/bulan kini hanya dibaca sebagai teks (bukan daftar), sehingga alamat seperti `/news?search[]=...` tidak lagi memicu halaman error. Endpoint pencarian AJAX kini mengirim `X-Content-Type-Options: nosniff`, dan data **SEO (JSON-LD)** artikel di-encode dengan aman sehingga judul/penulis berita yang mengandung `</script>` tidak lagi bisa menjalankan kode di browser pengunjung. Tautan kanonik/`og:url` di ketiga tema juga di-escape.

7. Yang Perlu Anda Lakukan Setelah Upgrade

1. **Lengkapi konten contoh** — sebagian teks masih "Lorem ipsum". Buka Admin → Settings → Tentang Kami, tulis profil, visi-misi, dan keunggulan sekolah yang sebenarnya.
2. **Upload foto asli** — foto sekolah (Tentang Kami), foto guru, foto berita, dan foto galeri. Tanpa foto, tampil huruf inisial pengganti.
3. **Isi link sosial media** — Admin → Settings → Sosial Media (Facebook, Instagram, YouTube, TikTok). Selama kosong, bagian "Ikuti Kami" menampilkan pemberitahuan.
4. **Sesuaikan tahapan SPMB dengan jenjang sekolah** — buka Admin → Settings → Tahapan SPMB, gunakan preset SD/SMP/SMA bila perlu, lalu ubah seperlunya.
5. **Ketahui hal ini:**
    - Menu **Admin → Menus kini hanya menambah tautan** di panel jelajah (navigasi utama 13 halaman tetap bawaan tema; halaman yang masih draft tidak tampil). Menu baru selalu tampil setelah 13 halaman bawaan — kolom Urutan hanya berlaku antar menu tambahan.
    - Pengaturan **warna tema (theme_color) diganti pemilih Tema Tampilan** — pilih theme di Admin → Settings → Tema Tampilan (baris setelan lamanya dihapus otomatis saat upgrade).
    - **Dark mode (mode gelap) dihapus** mengikuti tema baru.

8. Catatan Teknis (untuk Developer)

- Tema Nusantara: `.fas h3` (Keunggulan di beranda & Budaya Sekolah di profil) kini memakai `var(--sans)` (Archivo) 17px/700, bukan `var(--serif)` (Fraunces) 20px yang sulit dibaca pada kalimat panjang. `pages/home.php` dan `pages/profile.php` tidak lagi merender `<h3>` (dipotong 60 karakter) + `<p>` dari teks highlight yang sama — kini satu `<h3>` berisi teks penuh. `style.min.css` diregenerasi dengan `php minify.php`.
- Controller baru `App\Controllers\Site` + 9 view modul; `Routes` Inggris; `menu_helper` + `Sitemap` disesuaikan.
- Frontend multi-theme: view di `app/Views/themes/<nama>/`, aset di `public/themes/<nama>/`, loader `theme_view()`/`theme_asset()` + fallback ke `nusantara`, setting `active_theme`, pemilih theme di admin, cache per-theme. 9 file `*-theme.css` dihapus.
- `APP_VERSION` → `v3.2.0`; migrasi data di `UPGRADE.sql` (menu, tombol, copyright, `active_theme`, kolom `achievements.level` ENUM → VARCHAR, sinkron status events, isi `spmb_steps` bawaan bila kosong, indeks `idx_messages_created` dan `idx_comments_created` bila belum ada); template komentar pindah dari localStorage ke database; token CSRF form kontak disinkron ulang tiap kirim.
- Tahapan SPMB dinamis: setting `spmb_steps` (JSON, maks 12 langkah, tanpa migrasi — fallback ke 10 langkah bawaan bila kosong) + helper `default_spmb_steps()` / `spmb_step_presets()` (SD/SMP/SMA) / `resolve_spmb_steps()`; judul & progress bar mengikuti jumlah langkah otomatis.
- Rantai menu lama (`get_menu_tree`/`build_menu_tree`/`render_menu_items`/`get_section_settings_array` + cache `menu_tree_<theme>`) dihapus karena tidak dipakai view mana pun; `menu_helper` kini hanya `resolve_menu_url()` + `get_extra_nav_items()`. Setting `section_settings` tidak lagi dibaca (baris DB dibiarkan agar upgrade non-destruktif). `MenuItemModel::getActiveTree()` (sisa rantai lama, tanpa pemanggil) juga dihapus; `buildTree()` tetap dipakai `getFlatTree()`.
- Token CSRF (cookie, `Security::$regenerate = true`) kini disinkronkan ke seluruh form oleh helper `window.syncCsrf(hash)` di `app/Views/admin/layout.php` — memperbarui `<meta name="csrf-token">` **dan** semua `input[name="csrf_test_name"]`. Semua halaman admin yang memakai AJAX (`news` quick-update; reorder `gallery`/`teachers`/`programs`/`extracurriculars`/`achievements`/`testimonials`/`faq`/`downloads`/`menus`) memanggilnya dengan `csrfHash` dari respons, sehingga form yang di-render server (tombol Hapus per-baris, logout) tidak lagi 403 setelah token berputar.
- Kolom `show` (sakelar "Tampil di website") kini dihormati: `getOrdered()` di `TeacherModel`/`ProgramModel`/`ExtracurricularModel`/`TestimonialModel`/`AchievementModel` ditambah `->where('show', 1)` (sebelumnya hanya `EventModel`/`DownloadModel`/`GalleryModel`/`FaqModel` yang memfilter `show`). Kelima daftar admin menambahkan kolom **Status** (`Tampil`/`Tersembunyi`). Catatan: `show` adalah kata kunci MySQL — query builder CI4 meng-escape otomatis, jangan tulis query mentah tanpa backtick.
- Field `programs.link_url` kini dipakai tema lewat helper `program_link($program, $fallback)` (`app/Helpers/theme_helper.php`): URL absolut (`http(s)://`) dipakai apa adanya, selain itu lewat `base_url()`; fallback `#spmb` di halaman Program dan `program` di cuplikan beranda (3 tema + 3 header/home). `programs.icon` masih belum dirender tema.
- Ikon ekskul kini dirender di `app/Views/themes/<tema>/pages/extracurriculars.php` (di label `.cat`: `<i class="<?= esc($ex['icon']) ?>" style="color:<?= esc($ex['icon_color']) ?>">`), dan Font Awesome 6.5 (cdnjs — versi sama dengan panel admin) dimuat di `layouts/header.php` ketiga tema; sebelumnya tema hanya punya sprite SVG sendiri. Nilai `title`/`description`/`icon`/`icon_color` di `app/Views/admin/extracurriculars/index.php`

+ `form.php` kini lewat `esc()`. Catatan: `extracurriculars.icon_color` bertipe `varchar(7)` — format ARGB `#RRGGBBAA` (8 digit) tidak muat dan nilai lebih panjang akan terpotong diam-diam.

- Prestasi: `photo` kini dirender di `app/Views/themes/<tema>/pages/achievements.php` lewat `ach_photo($a)` (URL absolut / path diawali `/` dipakai apa adanya, selain itu `base_url('uploads/achievements/<file>')`; belum ada UI upload, jadi kolom ini berisi URL). `Achievements::index()` diurut `sort_order` saja (tidak lagi `year DESC` lebih dulu) dan view tema mengelompokkan tahun secara berurutan mengikuti item (bukan `krsort($byYear)`), sehingga seret-urut (reorder) = urutan publik. Kolom `year` kini wajib: form `achievements/form.php` memakai `required` + default tahun berjalan, dan `create()`/`update()` mengubah nilai kosong/`0` menjadi tahun berjalan (baris lama bertahun `0000` ditampilkan sebagai tahun berjalan oleh view). Nilai `student_name`/`class_name`/`achievement`/`photo` (termasuk pratinjau `<img>`) di form admin Prestasi kini lewat `esc()`.
- Agenda (`events`): `EventModel::getUpcoming()` tidak lagi memakai `orWhere('status', 'ongoing')` — kolom `status` hanya dihitung saat simpan dan tidak pernah disegarkan (tidak ada cron/command), sehingga acara lewat terus ikut tampil; kini cukup `event_date >= hari ini` (sudah mencakup hari ini) dan diurut `event_date ASC, sort_order ASC`. `Admin\Events::index()` diurut `event_date DESC, sort_order ASC` dan `admin/events/index.php` menambah kolom **Urutan** (colspan 7→8). Aturan validasi `event_date` diubah dari `permit_empty|max_length[20]` menjadi `required|valid_date` + pesan Indonesia. Catatan: `status = 'cancelled'` tetap didukung (dikecualikan dari `getUpcoming`), tetapi form tidak lagi mengirim `status`, jadi "Dibatalkan" belum dapat dipilih dari UI.
- Galeri (`galleries`): `GalleryModel::getVisible()` kini menerima filter kategori dan diurut `is_featured DESC, sort_order ASC, id ASC` (unggulan selalu di depan), sedangkan `getCategories($onlyVisible)` mengembalikan `[['name'=>…, 'count'=>…]]` — dipakai tab di `Site::gallery()` dan datalist form admin (sebelumnya `[['category'=>…]]`). `Site::gallery()` membaca `?category=` (nilai kategori dipakai apa adanya, tanpa slug) dan `pages/gallery.php` ketiga tema menambahkan `.tabs`/`.tab` + chip kategori + penanda `★ Unggulan` di `.g-cap .no` (nomor `G.xx` dihitung dari posisi hasil filter). `Admin\Gallery::create()` menolak simpan tanpa upload gambar valid (kolom `image` NOT NULL, tetapi koneksi DB non-strict dulu menyimpan string kosong sehingga item tak tampil; validasi tetap di controller, bukan di `GalleryModel`, agar `update()` — yang boleh tanpa gambar baru — tidak ikut gagal). `update()`/`delete()` kini memeriksa keberadaan baris lebih dulu (sebelumnya `update()` id tak ada tetap melapor "berhasil"), dan `delete()` menghapus baris DB sebelum file (sebelumnya file dulu, sehingga delete DB gagal meninggalkan baris menunjuk file hilang). `admin/gallery/index.php` menambah kolom **Unggulan** + **Status** (colspan 7→9; badge Urutan tetap di `td:nth-child(6)` sehingga JS reorder tak berubah) dan form-nya memakai `esc()` + menghapus hidden `old_image` yang tak pernah dibaca.
- FAQ (`faq`): `pages/faq.php` ketiga tema tidak lagi mengelompokkan item lewat `$cats[...][]` (yang menimpa urutan `sort_order`) — kini menelusuri `$faq` (sudah urut `sort_order` dari `FaqModel::getVisible()`) dan mencetak `.faq-cat` setiap kali kategori berubah (pola sama dengan Prestasi), serta memakai `nl2br(esc($f['answer']))`. Aturan `question` di `FaqModel` `max_length[500]` → `max_length[255]` (sesuai kolom `varchar(255)`), pesan `min_length`/`max_length` kini Indonesia. Tambah `FaqModel::getCategories()` (nama kategori unik dari data, `natcasesort`) + `$this->data['categories']` di `Admin\Faq::new()`/`edit()` untuk datalist form (menggantikan 5 kategori bawaan hardcoded). `Admin\Faq::update()`/`delete()` kini `find($id)` lebih dulu (pesan "FAQ tidak ditemukan."),

`admin/faq/index.php` menambah kolom **Status** (colspan 6→7; badge Urutan tetap di `td:nth-child(5)` sehingga JS reorder tak berubah), dan `admin/faq/form.php` memakai `esc()` pada question/answer/category + `maxlength` + placeholder Indonesia + format tanggal `d M Y H:i` yang seragam.

- Halaman Statis (`pages`): `Admin\Pages::update()` kini memeriksa keberadaan baris lebih dulu (sebelumnya id tak ada + `add_to_menu=1` menulis `menu_items` dengan `page_id` yatim → FK `menu_items_ibfk_2` → HTTP 500), dan slug **tidak lagi diturunkan ulang dari judul** setiap simpan — form mengirim slug saat ini sehingga URL lama tetap hidup; slug hanya berubah bila kolomnya diubah/dikosongkan (`slugFromInput()` + `makeUniqueSlug($slug, $id)`). `PageModel::$reservedSlugs` mencegah slug bentrok rute eksplisit (catch-all `/(:any)` selalu kalah); `makeUniqueSlug()` menambah akhiran angka bila slug masuk daftar itu. Mematikan `add_to_menu` kini menghapus baris menu (anak menu dinaikkan ke induknya) — dulu hanya diubah jadi `type=custom` + `page_id=NULL` sehingga tautan tetap tampil di nav. `image` kini masuk whitelist `create()`/`update()` (sebelumnya kolom dipakai view/`og_image` tetapi tidak pernah di-set dari admin) + validasi `permit_empty|max_length[255]`; form memakai `esc()` untuk title/slug/excerpt/image/meta, `maxlength`, placeholder Indonesia, pratinjau gambar, dan JS slug otomatis dari judul selama belum disentuh. `admin/pages/index.php` menambah kolom **Menu** (colspan 6→7) dari `menu_items.page_id` (`SELECT page_id ... WHERE page_id IS NOT NULL`). Catatan: `meta_title`/`meta_description` kini juga divalidasi maks 255 (sebelumnya terpotong diam-diam); slug halaman lama yang sudah terlanjur bentrok rute bawaan tidak diubah otomatis.
- Pesan Masuk (`contact_messages`): `admin/messages/show.php` tidak lagi menginterpolasi `$item['name']` ke handler JS inline (`onclick="return confirm('…"<?= esc($item['name']) ?>"…')"`). `esc()` HTML memang mengubah `'` menjadi `'`, tetapi browser meng-decode entitas di dalam atribut **sebelum** JS dieksekusi, sehingga nama seperti `X');alert(1)//` (dikirim anonim lewat `/contact/send`, hanya `strip_tags`) menjebol string JS → stored XSS di sesi admin sekaligus melewati konfirmasi. Kini memakai modal `data-coreui-toggle`/`data-coreui-target` seperti `admin/messages/index.php`, nama dirender sebagai teks HTML ter-escape, dan form hapus tetap POST + `csrf_field()`. `Admin\Messages::delete()` kini `find($id)` lebih dulu → "Pesan tidak ditemukan." (`BaseModel::delete()` → `doDelete()` → `$builder->delete()` selalu mengembalikan `true` walau 0 baris terhapus, sehingga dulu selalu "Pesan berhasil dihapus."). `admin/dashboard.php`: label tile "Pesan Masuk" → "Pesan Belum Dibaca" dan "Komentar" → "Komentar Menunggu" (keduanya memang bukan total, melainkan `getUnreadCount()`/`getPendingCount()`), serta judul blok "Pesan Baru" → "Pesan Terbaru" (`getRecent(5)` tidak memfilter `is_read`). `Contact::send()` kini mengirim `$validationMessages` Indonesia ke `$this->validate()` — `app/Config/App.php` `defaultLocale = 'en'` dan `app/Language/en/Validation.php` mengembalikan `[]`, sehingga tanpa itu pesan bawaan CI4 tampil berbahasa Inggris di toast pengunjung. Lanjutan perbaikan: `Admin\Messages::index()` membaca `?status=unread|read` (nilai lain = semua) dan menambahkan `orderBy('id','DESC')` sebagai tie-breaker — `created_at` berpresisi detik, dan tanpa tie-breaker urutan baris dengan waktu sama tidak dijamin stabil antar halaman (paginasi CI4 mempertahankan query string, jadi `?status=` ikut pada tautan pager); jumlah per status dihitung lewat `countAllResults()` pada instance model baru. Route POST baru: `read/(:num)` → `markRead()`, `unread/(:num)` → `markUnread()`, `bulk-delete` → `bulkDelete()` (semua lewat helper privat `setReadStatus()`/`listUrl()`, dengan `find($id)` dan pesan Indonesia; `bulkDelete()` menghitung `whereIn('id',$ids)->countAllResults()` lebih dulu karena

`delete()` tetap `true` walau 0 baris). `admin/messages/index.php` menambah kolom centang + kolom Aksi 170px, filter `btn-group`, dan **satu** form hapus massal di luar tabel (`#bulkDeleteForm`) — checkbox baris & tombol submit modal memakai atribut `form="bulkDeleteForm"` agar tidak ada `<form>` bersarang (form hapus per baris tetap sendiri); script in-section mengurus "pilih semua", penghitung, dan `disabled` tombol. `Contact::send()` kini juga memanggil `service('throttler')->check('contact-ip-'.$ip, 5, 600)` (pola sama `Admin\Auth`) — batas lama (`session('contact_last_sent')`, 1 pesan/30 detik) hilang begitu cookie dihapus, dan pemanggilan throttle sengaja diletakkan **setelah** validasi agar kiriman yang gagal validasi tidak menghabiskan jatah (hanya pesan yang benar-benar tersimpan yang dihitung); `$proxyIPs` di `app/Config/App.php` masih `[]`, jadi bila hosting memakai proxy/CDN semua pengunjung akan terlihat sebagai satu IP dan jatah ini berlaku kolektif — setel `$proxyIPs` (mis. `['*' => 'HTTP_X_FORWARDED_FOR']`) atau naikkan angkanya bila itu terjadi. Aturan `message` ditambah `max_length[5000]` + pesan Indonesia (sebelumnya kolom TEXT 65.535 menerima 70.000 karakter dengan balasan "berhasil" lalu memotongnya), dan `maxlength="5000"` ditambahkan pada textarea kontak ketiga tema. Indeks `idx_messages_created (created_at, id)` ditambahkan di `schema_database.sql` + blok bersyarat `information_schema`/`PREPARE` (yang pertama di `UPGRADE.sql`) — menghapus `Using filesort` yang muncul di `EXPLAIN` ketika tabel hanya punya `PRIMARY` + `idx_messages_read`.

- Komentar Berita (`news_comments`): `Admin\Comments::index()` kini `select('news_comments.*, news.title AS news_title, news.slug AS news_slug')->join('news', 'news.id = news_comments.news_id', 'left')` — view dulu membaca `news_title`/`commenter_name` yang tidak pernah ada di hasil query, sehingga kolom **Berita** selalu menampilkan angka `news_id`; kolom juga dikualifikasi (`news_comments.created_at`/`news_comments.id`) karena `news` punya kolom senama. Ditambah penyaring `?status=pending|approved` (nilai lain = semua) + `counts` dari instance model baru, tie-breaker `orderBy('id','DESC')`, dan aksi massal satu route `POST /admin/comments/bulk` (field `action=approve|delete`, `ids[]` disanitasi). `approve()`/`reject()`/`delete()` + `bulk()` kini `find($id)`/`whereIn(...)->countAllResults()` lebih dulu → "Komentar tidak ditemukan." (`update()`/`delete()` tetap `true` walau 0 baris). `admin/comments/index.php` mengikuti pola `admin/messages/index.php`: satu form `#bulkForm` di luar tabel + checkbox `form="bulkForm"` dan tombol submit modal yang membawa `name="action"` (form per baris tetap sendiri, jadi tidak ada `<form>` bersarang), kolom centang + kolom Aksi 150px, tombol **Tolak** untuk komentar menunggu, serta nama+email komentator dan judul berita bertaut.
- `News::comment()`: `getBySlugAnyStatus()` → `getBySlug()` (komentar ke berita draft kini 404, konsisten dengan `detail()`); `$validationMessages` Indonesia diteruskan ke `$this->validate()` (locale bawaan `en`); aturan `message` ditambah `max_length[2000]` dan `email max_length[100]` (dulu kolom TEXT 65.535 menerima 70.000 karakter dengan balasan "berhasil" lalu memotongnya). Tambah throttle per IP `service('throttler')->check('comment-ip-'.$ip, 5, 600)` **setelah** validasi (batas per sesi `comment_last_sent` tetap ada), pola sama `Contact::send()`. `parent_id` kini diselesaikan lewat `NewsCommentModel->where('id',$pid)->where('news_id',$post['id'])->where('is_approved',1)->first()`; nilai yang tidak cocok jadi `NULL` — sebelumnya nilai mentah dari POST diteruskan ke kolom ber-FK `news_comments_parent_id_foreign`, sehingga `parent_id=999999` memicu `DatabaseException` → **HTTP 500**. `News::detail()` melepas `cachePage(5)`: `ResponseCache` mengunci cache hanya per method+URI (cookie/sesi/flashdata diabaikan), sehingga (a) pesan galat validasi hilang saat halaman tersaji dari cache dan (b) HTML berisi `old('name')/old('email')`

pengunjung sebelumnya ikut tersimpan di cache lalu tampil ke pengunjung lain (terbukti: pengunjung lain melihat nama+email penanda selama TTL 5 detik). Catatan: `Controller::cachePage()` menerima **detik**, jadi `cachePage(5)` = 5 detik (komentar lama di `Contact::index()` yang menyebut "5 minutes" tidak akurat).

- Komentar (tema): tombol `.c-reply` kini membawa `data-comment-id` (dulu JS tema nusantara menyasar `.spc-reply`/`.spc-item`/`data-comment-id` yang tidak ada di markup → fitur balas mati), ditambah elemen `#cReplyInfo`/`#cReplyCancel` di atas form dan JS pengisi `#comment_parent_id`. JS balas + penghitung karakter juga ditambahkan ke `single_post.php` tema cakrawala & lentera (sebelumnya hanya nusantara), dan label `#cLeft` "0/500" → "0/2000" mengikuti `maxlength` + aturan server (dulu counter tidak pernah diperbarui JS). `NewsCommentModel`: `avatar` dihapus dari `$allowedFields` (tidak pernah di-set/dirender — tema memakai inisial + `crc32`), dan `getByNews()`/`getPendingRecent()` ditambah tie-breaker `id`. Indeks `idx_comments_created (created_at, id)` ditambahkan di `schema_database.sql` + blok bersyarat `information_schema`/`PREPARE` (bagian 9 `UPGRADE.sql`) — `EXPLAIN` berubah dari `type: ALL / key: NULL / Using filesort` menjadi `key: idx_comments_created / Backward index scan` (diuji dengan 303 baris; pada tabel 3 baris optimizer tetap memilih scan+sort).
- `composer.lock`: codeigniter4/framework v4.7.4 → v4.7.5, myclabs/deep-copy 1.13.4 → 1.14.0, nikic/php-parser v5.8.0 → v5.9.0, phpunit/phpunit 10.5.64 → 10.5.66, sebastian/recursion-context 5.0.1 → 5.0.2 (`composer.json` tidak berubah; `vendor/` dibangun ulang via `composer install`).
- Pengguna (`users`): `Admin\Auth::attempt()` kini menulis `last_login` (`$userModel->skipValidation(true)->update($id, ['last_login' => date('Y-m-d H:i:s')])`) — kolom itu sebelumnya hanya dibaca view sehingga selalu `NULL`. `Admin\BaseController::initController()` memverifikasi ulang akun ke DB pada tiap request admin (`select('id, role, is_active')` lewat `session('userId')`): akun yang hilang/nonaktif langsung diusir (`session()->remove(['isLoggedIn','userId','username','fullName','role'])` + flash → `/login`), `$this->data['user']['role']` diambil dari DB (bukan sesi) dan `session('role')` disinkronkan bila berbeda — dulu peran lama tetap dipakai sampai logout. `admin/layout.php`: item sidebar **Pengguna** dibungkus `if (($user['role'] ?? '') === 'superadmin')` (dulu tampil untuk semua peran), dan flash `success`/`error` serta nama di header (`$user['fullName']`) kini lewat `esc()` — `Auth::attempt()` menggabungkan `full_name` ke flash "Selamat datang …" sedangkan `full_name` dapat diubah pemilik akun sendiri lewat Profil tanpa validasi karakter (self-XSS → tetap ditutup). `admin/users/form.php` memakai `old()` + `esc()` (dulu `value="<?= $item[...] ?>"` mentah: `full_name` berisi `"><i>…` menjebol atribut `value` → stored XSS di browser superadmin, terbukti lewat Profil editor), checkbox `is_active` memakai hidden `0` + checkbox `1` (agar `old()` benar saat tidak dicentang), dan kolom **Konfirmasi Kata Sandi** baru (`password_confirm`, dicek di `create()`/`update()` → "Konfirmasi sandi tidak cocok."). `UserModel`: `avatar` dihapus dari `$allowedFields` (tidak pernah diisi/dirender) dan pesan `max_length`/`min_length`/`is_active.in_list` Indonesia dilengkapi (sebelumnya pesan Inggris bawaan CI4). `Admin\Users`: `index()` mengikutkan baris ber-`role` NULL (`groupStart()->where('role !=','superadmin')->orWhere('role', null)->groupEnd()`) + `orderBy('id','ASC')` (stabilkan paginasi), `delete()` kini `find($id)` lebih dulu → "Pengguna tidak ditemukan." (dulu `delete()` mengembalikan `true` walau 0 baris), dan `create()`/`update()` menangkap `DatabaseException` (balapan unique index) → pesan Indonesia alih-alih HTTP 500; kolom `role` di `schema_database.sql` kini `NOT NULL DEFAULT 'editor'` + bagian 10

`UPGRADE.sql` (`UPDATE users SET role='editor' WHERE role IS NULL` lalu `ALTER TABLE users MODIFY role ENUM(...) NOT NULL DEFAULT 'editor'`) — baris ber-`role` NULL dulu tidak terhitung oleh `role != 'superadmin'` sehingga hilang dari daftar.

- Menu Navigasi (`menu_items`): `MenuItemModel::getDescendantIds()` dulu rekursif tanpa penjaga — data berputar membuat proses berjalan tanpa henti sampai memori server habis (`memory_limit=-1`, terbukti: `PHP Fatal error: Allowed memory size ... exhausted` di `MenuItemModel.php(96)`); kini penelusuran berulang (queue + daftar `visited`), ditambah `MenuItemModel::hasCycle(array $parentMap)`. `Admin\Menus::reorder()` dulu memvalidasi cycle lewat `getDescendantIds()` **yang membaca keadaan di database**, sehingga payload beberapa item sekaligus (A→B, B→C, C→A) lolos (terbukti: `{"success":true}` dengan `1.parent_id=2, 2.parent_id=3, 3.parent_id=1`; id 1–3 hilang dari daftar) — kini disusun dulu peta parent **usulan** (seluruh baris + timpaan payload, `new MenuItemModel()` agar tidak terpengaruh state builder) lalu diuji `hasCycle()` sebelum menulis; respons gagal 422 berisi pesan, dan kegagalan tulis kini 500 + pesan (dulu `{"success":false}` tanpa status/pesan). `Admin\Menus::index()` menambah `orphanCount` (total baris – jumlah `getFlatTree()`) dan `admin/menus/index.php` menampilkan peringatan bila ada item tak terjangkau. JS `saveOrder()` memperbaiki `td:nth-child(7)` → `td:nth-child(8)` (kolom **Urutan**; dulu badge **Status** yang tertimpa angka — dibuktikan dengan Chrome headless memakai markup + potongan JS asli: Status `Bawaan` tetap, Urutan `7` → `14`) dan menangani jalur gagal (`alert` berisi pesan server + `location.reload()`, diverifikasi lewat `sessionStorage`), sebelumnya respons non-sukses diabaikan tanpa pesan sehingga UI tetap bergeser padahal DB tidak berubah. Skema berbahaya kini satu sumber aturan: `is_dangerous_url()` di `app/Helpers/menu_helper.php` dipakai `Admin\BaseController::isDangerousUrl()` (dulu salinan regex) **dan** `get_extra_nav_items()` — URL hasil substitusi placeholder `{kunci}` (mis. `spmb_url` = `javascript:…`) dulu lolos validasi simpan lalu tercetak `href="javascript:…"` di header tema; kini item seperti itu dilewati saat render (item bernilai sah tetap tampil, diuji). `Admin\Menus::SECTION_KEYS` menjadi sumber tunggal daftar kunci bagian untuk form + whitelist simpan (`sanitizeSectionKey()`; nilai di luar daftar jadi `NULL` — dulu string bebas ≤100 karakter tersimpan dan salah satunya di-echo mentah di cabang menu terkunci `form.php:121`, kini `esc()`); `MenuItemModel` `target`: `permit_empty|in_list[_self,_blank]` → `required|in_list[_self,_blank]` + pesan Indonesia (dulu `target=` kosong tersimpan sebagai string kosong di luar definisi `ENUM`, karena koneksi CI4 `strictOn=false` membuat session `sql_mode` tanpa `STRICT_TRANS_TABLES`); `Admin\Menus::hasDuplicateUrl()` menolak URL kembar antar item non-`system` (normalisasi huruf kecil + strip `/`, jadi `x` = `x/`, dan mencakup item bertipe `page`). Daftar admin: item bertipe **Halaman** kini punya tombol edit (`$isSystem` = `type === 'system'`; hapus tetap `$canDelete` = `type === 'custom'`) sehingga induk & urutannya bisa diatur dari form (`update()` hanya mengirim `parent_id`+`sort_order` untuk item terkunci), kolom URL tidak lagi dipaksa berawalan `/` (dulu `https://…` tampil `/https://…`), `esc()` pada `sort_order` kedua view, kode mati `<?= $locked ? '' : '' ?>` dihapus, dan CSS `.table-row-child`/`.child-indent` (dulu kelas tanpa aturan) kini menjorokkan kolom Judul. Catatan: `menu_items.updated_at` sudah `ON UPDATE CURRENT_TIMESTAMP` sehingga reorder lewat query builder mentah tetap memperbarui waktu ubah — tidak perlu di-set manual. Tanpa perubahan skema, jadi `UPGRADE.sql`/`schema_database.sql` tidak berubah. Otorisasi: `Admin\Menus`, `Admin\Pages`, dan `Admin\Settings` **tidak** memeriksa peran (hanya `Admin\Users` yang membatasi Superadmin) — perilaku ini dipertahankan sesuai keputusan, dan klaim "Hanya untuk Superadmin" pada `PANDUAN_PENGGUNA.md` (B.15/B.16 + matriks Role) dihapus agar dokumen sesuai kenyataan (terbukti

dengan akun `role=editor` sementara: `/admin/menus`, `/admin/pages`, `/admin/settings` → HTTP 200 dan `POST /admin/menus/reorder` tersimpan, sedangkan `/admin/users` → 302).

- Pengaturan (`settings`): `SettingModel::setSetting()` kini memakai `upsert()` (`INSERT … ON DUPLICATE KEY UPDATE`, aman karena `settings.key` ber-UNIQUE; `upsert()` CI4 4.7 memakai `batchExecute` → identifier ter-backtick) — dulu `where('key',…)->first()` lalu `insert()`, sehingga dua request bersamaan sama-sama tidak menemukan baris dan dua-duanya INSERT (terbukti: dua baris `key` sama → nilai acak). `Admin\Settings` ditulis ulang: konstanta `PLAIN_KEYS`/`JSON_DATA_KEYS`/`JSON_LINK_KEYS`/`EXTRA_KEYS`/`URL_KEYS` menjadi satu sumber daftar kunci untuk `index()` dan `save()`, validasi URL lewat `is_safe_link_url()` (helper baru di `app/Helpers/menu_helper.php`, satu aturan dengan header tema), email lewat `filter_var(FILTER_VALIDATE_EMAIL)`, dan unggahan lewat `validateImageUpload()` + `uploadImage()` (satu jalur untuk Tentang Kami & Kepala Sekolah): `MAX_UPLOAD_BYTES` 5 MB, `MAX_UPLOAD_PIXELS` 25 MP, `effectiveUploadBytes()` = minimum batas aplikasi / `upload_max_filesize` / `post_max_size`, `getimagesize()` + whitelist JPEG/PNG/WebP. Galat dikumpulkan lalu dilaporkan lewat flash `error` sambil mempertahankan nilai lama (dulu `die()`-style langsung `return` tanpa pesan/penyimpanan sebagian). `array_filter` highlights diberi callback `$l !== ''` (dulu ikut membuang baris "0"), `mergeJson()` menjaga kunci lama `about`/`principal` saat form tidak merender kuncinya, `encodeJson()` jatuh ke `[]`/`{}` sesuai tipe bila `json_encode` gagal (dulu selalu `'[]'` — kunci asosiatif bisa terhapus). `app/Views/admin/settings.php`: 54 titik cetak nilai (36 `value=`, 2 `src=`, 1 `href=`, 9 `<textarea>`, 6 pratinjau) kini lewat `esc()` — sebelumnya `value="<?= $settings[...] ?>"` mentah, dan setelan berisi `"` dapat menjebol atribut (mis. `hero_title`). Tema: helper `theme_banner()`, `theme_setting_links()`, `theme_brand_text()` (ber-`static` cache), dan `theme_nav_url()` di `app/Helpers/theme_helper.php` membaca setelan langsung dari DB (variabel view tiap controller berbeda bentuk: `page_banners` JSON string, `footer_*` JSON string di News/Contact/Downloads tetapi array di `Home.php`), lalu dirender di `pages/{news,contact,downloads,page,single_post}.php` + `layouts/{header,footer}.php` ketiga tema dengan fallback ke markup lama bila kosong; kolom ke-2 footer jadi **Program** (`footer_services`) dan **Layanan** (`footer_links`). `.hero-badge` ditambahkan ke 3 `public/themes/*/css/style.css` lalu `php minify.php`. `theme_color` dihapus dari `Home`/`News`/`Contact`/`Downloads`/`Pages` (4 kemunculan di `News`) + `SettingSeeder`, dengan `DELETE` barisnya di bagian 11 `UPGRADE.sql`.
- Testimoni (`testimonials`): `app/Views/admin/testimonials/form.php` kini `esc()` + `old()` untuk `name`/`role`/`quote`/`photo`/`sort_order`/`show` (dulu `value="<?= $item[...] ?>"` mentah — `name` berisi `" onmouseover="…` menjebol atribut, `photo` `" onerror="…` ikut menjebol `<img src>`, dan `quote` berisi `</textarea><script>` keluar dari textarea → stored XSS di panel admin, terbukti lewat uji POST+GET halaman Edit; `withInput()` sudah dipanggil controller tetapi form membaca `$item` sehingga isian hilang saat validasi gagal). `TestimonialModel::$validationMessages` dilengkapi `min_length`/`max_length` Indonesia, dan `Admin\Testimonials::delete()` kini `find($id)` lebih dulu → "Testimoni tidak ditemukan." (`BaseModel::delete()` selalu `true` walau 0 baris). Kolom `photo` yang selama ini tidak dipakai kini dirender sebagai avatar bulat: `pages/testimonials.php` ketiga tema memakai `<span class="t-ava"><img …>` bila `photo` terisi (tema lain: `<span class="q">“</span>`), `pages/home.php` menambah `.quote-ava` di dalam `<cite>` (nusantara/cakrawala) atau `<img>` di dalam `.g-mini-av` (lentera), dengan `.t-ava`/`.quote-ava`/`.g-mini-av img` di 3 `public/themes/*/css/style.css` lalu `php minify.php`.

- Reorder + paginasi (8 modul): `reorder(array $ids)` kehilangan konteks halaman — daftar admin `paginate(10)`, jadi halaman ke-2 menulis `sort_order` 0..9 dan bertabrakan dengan halaman pertama (item berpindah setelah reload). Kini `reorder(array $ids, int $offset = 0)` menulis `$offset + $i` di `TeacherModel`/`ProgramModel`/`AchievementModel`/`DownloadModel`/`ExtracurricularModel`/`FaqModel`/`GalleryModel`/`TestimonialModel`; `reorder()` tiap controller membaca `$offset = max(0, (int) ($input['offset'] ?? 0))` (sebelum `reorderIdsExist()` sudah menyaring `ids`), dan JS `admin/*/index.php` mengirim `const offset = <?= (int) (($pager->getCurrentPage() - 1) * 10) ?>` pada payload, memakainya untuk badge Nomor/Urutan, menangani respons gagal (`!data.success` → `alert` pesan server + `location.reload()`) dan `fetch` gagal (`.catch`), pola yang sama dengan `admin/menus/index.php`. `substr`/`strlen` (80 byte kutipan, 60 caption, 80 deskripsi) diganti `mb_substr`/`mb_strlen` di `admin/{testimonials,programs,gallery}/index.php`.
- Keamanan `News`: helper privat baru `News::queryParam()` menormalkan `search`/`category`/`month`/`q` menjadi `string` yang di-trim atau `null` bila kosong (nilai array dibuang, bukan di-cast menjadi `"Array"` yang memicu `TypeError` di `NewsModel::search()`/`getFiltered()`/`searchByQuery()`), dan `News::search()` menambah header `X-Content-Type-Options: nosniff`. JSON-LD di `News::detail()` (satu-satunya produsen `$ldjson`) kini memakai `JSON_HEX_TAG|JSON_HEX_AMP|JSON_HEX_APOS|JSON_HEX_QUOT`: sebelumnya `JSON_UNESCAPED_SLASHES` mempertahankan `</script>` pada `headline`/`description`/`author`/`publisher` sehingga judul berita dapat menutup tag `<script type="application/ld+json">` lebih awal (stored XSS oleh admin; `json_encode` lama terbukti menghasilkan `</script>` mentah). Ketiga `layouts/header.php`: `current_url()` pada `rel=canonical` dan `og:url` kini lewat `esc()` (defense-in-depth). Refleksi `?search=` sendiri sudah aman (`esc()` pada teks "Hasil pencarian" dan `value` input) dan diuji ulang via curl + Chrome headless.