Kertas Kerja Audit Aplikasi: smp.spmbpekanbaru.id

Kategori:  
Boundary Controls

Index:  
BC-01

Kriteria:  
Akses hanya boleh dilakukan oleh user yang terautentikasi. (COBIT 2019 DSS05.04)

Tujuan Pemeriksaan:  
Memastikan sistem memiliki autentikasi pengguna dan batasan akses.

Bukti Audit:  
Uji akses dashboard tanpa login diarahkan ke halaman login.

Kondisi Saat Ini:  
Login form tersedia, pengguna tidak bisa akses halaman pribadi tanpa login.

Temuan:  
Tidak ada CAPTCHA saat login.

Dampak:  
Berpotensi rawan brute-force attack.

Tingkat Kesesuaian:  
Sebagian Sesuai

Rekomendasi:  
Tambahkan CAPTCHA dan batas percobaan login.

Tanggapan:  
-

Target Penyelesaian:  
-

Status:  
-

Kategori:  
Input Controls

Index:  
IC-01

Kriteria:  
Validasi input harus dilakukan untuk mencegah data tidak valid.

Tujuan Pemeriksaan:  
Memastikan validasi input form saat pendaftaran siswa.

Bukti Audit:  
Uji form: isi nama dengan angka, isi email salah format.

Kondisi Saat Ini:  
Validasi dasar tersedia, tapi beberapa field tidak validasi panjang atau karakter spesial.

Temuan:  
Field seperti 'Nama Ibu' menerima angka.

Dampak:  
Risiko data tidak valid tersimpan di database.

Tingkat Kesesuaian:  
Sebagian Sesuai

Rekomendasi:  
Tambahkan validasi karakter & panjang di sisi server dan client.

Tanggapan:  
-

Target Penyelesaian:  
-

Status:  
-

Kategori:  
Communication Controls

Index:  
CC-01

Kriteria:  
Data harus dikirim via saluran aman. (ISO/IEC 27001 A.10.1)

Tujuan Pemeriksaan:  
Memastikan komunikasi antar sistem aman (SSL/TLS).

Bukti Audit:  
URL menggunakan HTTPS.

Kondisi Saat Ini:  
Sertifikat SSL aktif dan valid.

Temuan:  
-

Dampak:  
-

Tingkat Kesesuaian:  
Sesuai

Rekomendasi:  
-

Tanggapan:  
-

Target Penyelesaian:  
-

Status:  
Close

Kategori:  
Processing Controls

Index:  
PC-01

Kriteria:  
Proses data harus akurat dan bisa ditelusuri.

Tujuan Pemeriksaan:  
Memastikan proses pendaftaran berjalan benar dan menangani kesalahan.

Bukti Audit:  
Uji daftar dengan data duplikat dan isi tidak lengkap.

Kondisi Saat Ini:  
Proses pendaftaran berhasil namun tidak jelas apakah ada error log atau audit trail.

Temuan:  
Tidak ditemukan pesan error spesifik saat input salah.

Dampak:  
Sulit melakukan pelacakan kesalahan data.

Tingkat Kesesuaian:  
Sebagian Sesuai

Rekomendasi:  
Tambahkan audit trail dan error handler yang informatif.

Tanggapan:  
-

Target Penyelesaian:  
-

Status:  
-

Kategori:  
Database Controls

Index:  
DC-01

Kriteria:  
Data harus disimpan secara aman dan tidak mudah diakses tanpa izin.

Tujuan Pemeriksaan:  
Memastikan integritas dan kerahasiaan data siswa.

Bukti Audit:  
Tidak dapat dilihat langsung, tapi form tidak menunjukkan sanitasi input.

Kondisi Saat Ini:  
Tidak dapat diverifikasi apakah data disanitasi atau dienkripsi.

Temuan:  
Tidak ada mekanisme input sanitizer terdeteksi di form.

Dampak:  
Rentan SQL Injection atau data korup.

Tingkat Kesesuaian:  
Tidak Sesuai

Rekomendasi:  
Gunakan sanitasi input (prepared statements) dan enkripsi untuk data sensitif.

Tanggapan:  
-

Target Penyelesaian:  
-

Status:  
-

Kategori:  
Output Controls

Index:  
OC-01

Kriteria:  
Output harus akurat dan hanya bisa diakses oleh pihak yang berwenang.

Tujuan Pemeriksaan:  
Memastikan cetak kartu dan hasil seleksi tidak bocor atau salah orang.

Bukti Audit:  
Tampilan cetak kartu hanya bisa diakses setelah login.

Kondisi Saat Ini:  
Kartu dan hasil hanya muncul setelah login, namun belum ada watermark atau proteksi PDF.

Temuan:  
Tidak ada mekanisme otentikasi tambahan sebelum cetak.

Dampak:  
Potensi kartu dipalsukan atau disalahgunakan.

Tingkat Kesesuaian:  
Sebagian Sesuai

Rekomendasi:  
Tambahkan proteksi output (captcha, watermark, atau tanda digital).

Tanggapan:  
-

Target Penyelesaian:  
-

Status:  
-