Laporan Temuan Penilaian Keamanan ConnectSphere

Kayla Putri Maharani | 5026231158 PAI B

Klien: PT Digital Kreatif Nusantara (DKN)
Aplikasi: ConnectSphere.id, Platform Media Sosial Profesional
Tanggal Laporan: 26 September 2025
ID Proyek: ACD-DKN-0925
Versi Laporan: 1.0

Daftar Isi

Pernyataan Kerahasiaan dan Disclaimer

Pernyataan Kerahasiaan

Dokumen ini adalah milik eksklusif PT Digital Kreatif Nusantara (DKN) dan Aegis Cyber Defense (ACD). Dokumen ini mengandung informasi kepemilikan dan rahasia bisnis. Duplikasi, redistribusi, atau penggunaan, baik sebagian maupun keseluruhan, dalam bentuk apa pun, memerlukan persetujuan tertulis dari kedua belah pihak.

Disclaimer

Pengujian penetrasi ini dianggap sebagai *snapshot* keamanan yang dilakukan pada periode 15 September 2025 hingga 24 September 2025. Temuan dan rekomendasi yang disajikan mencerminkan informasi yang dikumpulkan selama penilaian dan tidak mencakup perubahan atau modifikasi yang mungkin telah dilakukan di luar periode tersebut.

Informasi Kontak

Nama	Jabatan	Organisasi	Informasi Kontak
Budi Hartono	Chief Technology Officer (CTO)	PT DKN	Office: (021) 555-1001, Email: budi.hartono@digitalkreatif.id
Citra Dewi	IT Manager	PT DKN	Office: (021) 555-1002, Email: citra.dewi@digitalkreatif.id
Kayla Putri Maharani	Kontak Firma ACD	(Detail Kontak Firma)	

Tinjauan Penilaian (Assessment Overview)

Penilaian ini dilakukan untuk mengevaluasi postur keamanan aplikasi dan infrastruktur ConnectSphere milik PT Digital Kreatif Nusantara.

Komponen Penilaian

Jenis pengujian yang dilakukan adalah External Penetration Test (Black-Box Test), dirancang untuk meniru peran penyerang tanpa pengetahuan atau sumber daya internal. Metodologi yang digunakan berpegangan pada panduan industri global, termasuk NIST SP 800-115 dan OWASP Testing Guide (v4).

Ruang Lingkup (Scope)

Ruang lingkup pengujian meliputi seluruh aset yang terkait dengan platform media sosial profesional ConnectSphere.id.

Penilaian	Detail
Jenis Pengujian	External Penetration Test (Black-Box)
Target Utama	Domain connectsphere.id dan seluruh subdomainnya
Target IP Publik	103.45.67.89
Periode Pengujian	15 September 2025 – 24 September 2025

Sesuai permintaan klien, pengujian ini secara ketat mengecualikan serangan Denial of Service (DoS) dan Social Engineering. Klien tidak memberikan informasi atau akses apapun (black-box test).

Peringkat Keparahan Temuan (Finding Severity Ratings)

Keparahan	Rentang Skor CVSS V3	Definisi
Critical	9.0 – 10.0	Eksploitasi relatif mudah dan biasanya menghasilkan kompromi tingkat sistem secara penuh. **Tindakan perbaikan segera diwajibkan.**
High	7.0 – 8.9	Eksploitasi lebih sulit tetapi dapat menyebabkan peningkatan hak akses dan potensi kehilangan data atau *downtime*.
Moderate	4.0 – 6.9	Kerentanan tidak mudah dieksploitasi atau memerlukan langkah tambahan, misalnya rekayasa sosial.
Low	0.1 – 3.9	Kerentanan tidak dapat dieksploitasi tetapi akan mengurangi permukaan serangan organisasi.
Informational	N/A	Tidak ada kerentanan. Informasi tambahan mengenai kontrol yang kuat atau dokumentasi.

Ringkasan Eksekutif

Ringkasan Umum (Non-Teknis)

Penilaian keamanan ConnectSphere mengungkapkan tingkat risiko operasional dan fidusia yang sangat tinggi. Empat jalur serangan Kritis berhasil dieksploitasi, masing-masing berujung pada kompromi total, baik terhadap infrastruktur internal (Domain Controller) maupun aset data pengguna yang paling sensitif (Database Produksi dan Arsip Data Pengguna).

Kegagalan ini bersifat sistemik, mencerminkan kelemahan mendasar dalam manajemen aset (aset terlupakan), disiplin SDLC (kredensial hardcoded), dan kontrol akses jaringan (sistem logging terbuka). PT DKN saat ini menghadapi risiko maksimum pelanggaran PII (Personally Identifiable Information) secara massal, yang dapat memicu konsekuensi kepatuhan regulasi yang parah dan kerusakan reputasi yang sulit dipulihkan.

Ringkasan Dampak Bisnis

Temuan Kritis	Fokus Akar Masalah	Dampak Bisnis Utama (Risiko Fidusia)
Temuan 1: Forgotten Blog	Tata Kelola Aset Lalai	Kredensial service account terekspos dalam plain text, memberikan akses tidak sah ke data pengembangan fitur baru (server staging).
Temuan 2: Developer's Mistake	SDLC & Kebersihan Kredensial	Kompromi total atas seluruh data pengguna dan pesan pribadi karena kredensial database produksi bocor dalam riwayat Git.
Temuan 3: Internal Pivot	Manajemen *Patch* & Akses Internal	Kendali penuh atas seluruh infrastruktur DKN, termasuk Domain Controller, karena eksploitasi sistem internal yang usang dan pencurian kredensial Domain Admin.
Temuan 4: Cloud Leak	Konfigurasi Cloud & Kontrol Akses	Pelanggaran privasi massal: Pengunduhan arsip data lengkap semua pengguna (termasuk riwayat pesan pribadi) melalui kombinasi server logging terbuka dan celah IDOR.

Temuan Teknis Detail (Detailed Technical Findings)

5.1. Temuan 1: Serangan dari Titik Buta (The Forgotten Blog)

Peringkat Risiko	**Critical**
Deskripsi	Serangan dimulai dari subdomain blog.connectsphere.id, yang menjalankan WordPress versi usang. Tim berhasil memanfaatkan kerentanan file upload pada plugin 'Super Uploader v1.2' untuk mengunggah web shell dan mendapatkan eksekusi kode jarak jauh (RCE) pada server web. Dari server web, tim melakukan pivot dan menemukan file share internal yang terbuka tanpa kata sandi. Di dalamnya, ditemukan file konfigurasi yang berisi kredensial service account dalam format plain text. Kredensial ini digunakan untuk login ke server staging.
Dampak	Kompromi penuh server web dan pencurian kredensial sensitif. Penyerang mendapatkan akses penuh ke lingkungan staging yang berisi data-data pengembangan fitur baru ConnectSphere. Misi dinyatakan berhasil.
Rekomendasi	Segera decommission atau patch total blog.connectsphere.id dengan menghapus atau menonaktifkan plugin 'Super Uploader v1.2'. Terapkan otentikasi yang kuat pada file share internal. Rotasi segera semua kredensial service account yang terekspos dan pastikan kredensial tidak disimpan dalam bentuk plain text.

5.2. Temuan 2: Jejak Kredensial yang Terlupakan (The Developer's Mistake)

Peringkat Risiko	**Critical**
Deskripsi	Ditemukan bucket S3 yang salah konfigurasi, terbuka untuk publik, mengekspos source code versi awal yang memuat kunci API hardcoded. Kunci API tersebut mengarahkan ke nama pengembang. Tim menemukan pengembang tersebut menggunakan kembali kata sandi dari kunci API yang bocor untuk akun GitHub pribadinya, memberikan akses ke private repository. Pemeriksaan riwayat commit menemukan sebuah commit lama yang secara tidak sengaja menyertakan kredensial database produksi ConnectSphere.

Dampak	Kompromi total: Kredensial database yang diekstrak berhasil digunakan untuk terhubung langsung ke database utama, membuktikan kompromi total atas seluruh data pengguna dan pesan pribadi mereka.
Rekomendasi	Rotasi segera semua kredensial database produksi dan kunci API yang sensitif. Hapus kredensial dari riwayat Git (Git History). Konfigurasi bucket S3 menjadi privat. Terapkan kebijakan Secret Management untuk mencegah hardcoding kredensial dalam kode.

5.3. Temuan 3: Eskalasi dari Dalam (The Internal Pivot)

Peringkat Risiko	**Critical**
Deskripsi	Mensimulasikan serangan dari dalam dengan akses setara karyawan magang. Pemindaian jaringan internal mengidentifikasi PC Windows 7 tua tanpa patch di departemen marketing. Sistem ini rentan terhadap eksploitasi MS17-010 (Eternal Blue). Tim berhasil mendapatkan hak akses Administrator pada mesin tersebut. Alat Mimikatz digunakan untuk mengekstrak kredensial dari memori, yang secara kebetulan menyimpan kredensial Domain Admin yang baru login.
Dampak	Kendali penuh atas seluruh infrastruktur DKN. Dengan kredensial Domain Admin, tim berhasil terhubung ke Domain Controller, membuat akun admin persisten baru, dan menguasai server-server yang menjalankan platform ConnectSphere.id.
Rekomendasi	Segera patch semua sistem internal terhadap kerentanan MS17-010 dan decommission sistem operasi usang (Windows 7). Terapkan pemisahan tugas ketat; Domain Admin tidak boleh login ke workstation pengguna biasa.

5.4. Temuan 4: Bencana di Awan (The Cloud Leak)

Peringkat Risiko	**Critical**
Deskripsi	Ditemukan server Elasticsearch yang digunakan untuk logging aktivitas aplikasi ConnectSphere.id yang terbuka untuk publik tanpa autentikasi. Pencarian log mengungkapkan ratusan session token pengguna yang masih aktif. Token ini digunakan untuk session

	hijacking. Setelah login, ditemukan fitur 'Download Arsip Data Anda' memiliki celah Broken Access Control (IDOR) pada parameter userID (/export?userID=1138), yang memungkinkan manipulasi parameter.
Dampak	Pelanggaran privasi massal: Dengan memanipulasi userID, tim berhasil mengunduh arsip data lengkap semua pengguna di platform ConnectSphere, termasuk riwayat pesan pribadi, daftar koneksi, dan informasi profil.
Rekomendasi	Blokir akses publik ke server logging (Elasticsearch) dan terapkan autentikasi yang kuat. Invalidaasi segera semua session token yang terekspos. Perombakan endpoint /export untuk menerapkan Kontrol Akses Berbasis Objek (Object-Level Access Control) yang memverifikasi kepemilikan data di sisi server.

Kesimpulan & Rekomendasi Umum

Kesimpulan Penilaian Keseluruhan

Kegagalan keamanan pada ConnectSphere berakar pada empat kategori utama yang harus segera diperbaiki: Tata Kelola Aset yang Lalai (Temuan 1), Disiplin Kredensial Nol (Temuan 2), Manajemen Patch yang Akut (Temuan 3), dan Kontrol Akses yang Rusak (Temuan 4). Kerentanan ini memungkinkan penyerang eksternal maupun internal untuk mencapai kompromi total atas aset data terpenting dan infrastruktur inti.

Prioritas

1. **Fase 1 (Segera): Perbaikan Kritis dan Rotasi Kredensial.**
    - Lakukan semua tindakan Remediasi Prioritas (P1) dari Temuan 1 hingga 4.
    - Fokus pada rotasi total semua kredensial produksi dan menutup celah akses publik (blog lama dan Elasticsearch).
2. **Fase 2 (Jangka Pendek): Penguatan Akses dan Infrastruktur.**
    - Terapkan kebijakan manajemen *patch* ketat untuk semua sistem, terutama internal.
    - Terapkan kontrol akses (otentikasi dan *firewall*) pada semua *file share* dan *logging server*.
    - Hentikan praktik berbahaya (seperti *login* Domain Admin ke *workstation* pengguna).

3. **Fase 3 (Jangka Panjang): Transformasi SDLC dan Tata Kelola Aset.**
    - Terapkan *Secret Management Vault* untuk menyimpan kredensial dan kunci.
    - Tinjau dan perbaiki semua kode aplikasi yang rentan terhadap *Broken Access Control* (IDOR) dan pastikan verifikasi kepemilikan data selalu dilakukan di sisi *server*.
    - Lakukan inventarisasi dan pemantauan aset secara berkelanjutan untuk mencegah munculnya kembali aset yang terlupakan (Shadow IT).