

Laporan Penetration Testing

Web Application Security Assessment

Dokumen ini adalah CONTOH laporan untuk keperluan ilustrasi.
Nama klien, temuan, dan data di dalamnya bersifat fiktif.

KLIEN

PT Contoh Klien Sejahtera (Data Sampel)

TANGGAL LAPORAN

23 Januari 2026

PERIODE ASSESSMENT

5 – 16 Januari 2026

DOCUMENT ID

PT-RPT-2026-DEMO-081

01 • RINGKASAN EKSEKUTIF

Ringkasan Eksekutif

SkyCyber melaksanakan penetration testing terhadap aplikasi web milik **PT Contoh Klien Sejahtera (Data Sampel)** pada periode 5 – 16 Januari 2026, dengan metodologi black-box dan grey-box mengacu pada OWASP Testing Guide v4.2 serta PTES (Penetration Testing Execution Standard). Tujuan assessment ini adalah mengidentifikasi kerentanan keamanan pada aplikasi sebelum dapat dieksploitasi oleh pihak yang tidak berwenang, serta memberikan rekomendasi remediasi yang dapat langsung ditindaklanjuti oleh tim teknis klien.

Catatan: dokumen ini adalah contoh/sample yang dibuat untuk keperluan ilustrasi kualitas laporan SkyCyber. Nama klien, target, dan seluruh temuan yang tercantum bersifat fiktif dan tidak merepresentasikan sistem atau data nyata.

Ringkasan Temuan

Tingkat Keparahan	Jumlah Temuan	Status Remediasi
Critical	1	Menunggu Perbaikan
High	2	Menunggu Perbaikan
Medium	3	Menunggu Perbaikan
Low	4	Menunggu Perbaikan
Informational	5	Dicatat

Postur Keamanan Keseluruhan

Aplikasi menunjukkan sejumlah kontrol keamanan dasar yang sudah diterapkan dengan baik (otentikasi berbasis token, validasi input pada sebagian besar endpoint, dan penggunaan HTTPS secara menyeluruh). Namun demikian, tim SkyCyber menemukan **1 kerentanan Critical** yang memungkinkan eksfiltrasi data melalui SQL Injection, serta beberapa kerentanan High dan Medium terkait kontrol akses dan konfigurasi keamanan yang perlu segera ditindaklanjuti sebelum aplikasi diakses oleh pengguna dalam skala produksi penuh.

02 · RUANG LINGKUP & METODOLOGI

Ruang Lingkup Pengujian

Item	Detail
Target Aplikasi	app.contohklien-demo.co.id (Web Application)
Jenis Pengujian	Black-box & Grey-box Penetration Testing
Metodologi	OWASP Testing Guide v4.2, PTES, NIST SP 800-115
Tim Penguji	2 Senior Penetration Tester (OSCP, eWPTX bersertifikat)
Durasi Pengujian	5 – 16 Januari 2026 (10 hari kerja)
Environment	Staging (replika produksi, atas persetujuan klien)

Batasan Pengujian (Out of Scope)

- Serangan Denial of Service (DoS/DDoS) tidak dilakukan untuk menjaga stabilitas layanan.
- Social engineering terhadap karyawan klien tidak termasuk dalam ruang lingkup ini.
- Infrastruktur pihak ketiga (CDN, payment gateway) diuji secara terbatas pada titik integrasi saja.

Metodologi Pengujian

- Reconnaissance** — Pengumpulan informasi publik terkait target — subdomain enumeration, teknologi yang digunakan, dan permukaan serangan (attack surface).
- Vulnerability Mapping** — Pemetaan potensi kerentanan menggunakan kombinasi automated scanning dan manual testing berbasis OWASP Top 10.
- Exploitation** — Upaya eksploitasi terkontrol terhadap kerentanan yang teridentifikasi untuk memvalidasi dampak nyata (proof of concept), tanpa merusak data produksi.
- Post-Exploitation** — Analisis dampak lanjutan apabila kerentanan dieksploitasi pihak tidak berwenang — termasuk potensi lateral movement dan eskalasi privilege.
- Reporting** — Penyusunan laporan lengkap berisi temuan, tingkat risiko (CVSS v3.1), bukti (evidence), dan rekomendasi remediasi yang actionable.

03 · TEMUAN DETAIL

Temuan Kerentanan

Berikut adalah rincian temuan kerentanan yang paling signifikan, diurutkan berdasarkan tingkat keparahan (severity) menggunakan skor CVSS v3.1. Setiap temuan dilengkapi deskripsi teknis, bukti (evidence), dampak bisnis, dan rekomendasi remediasi.

PT-2026-001 — SQL Injection pada Endpoint Pencarian Produk

Critical

CVSS v3.1: 9.8 · Lokasi: GET /api/v1/products/search?q=

Deskripsi

Parameter **q** pada endpoint pencarian produk tidak melakukan sanitasi input sebelum dikonstruksi menjadi query SQL. Penguji berhasil melakukan ekstraksi seluruh data pada tabel **users** (termasuk hash password) menggunakan teknik UNION-based SQL Injection, tanpa memerlukan otentikasi.

Dampak Bisnis

Eksfiltrasi penuh basis data, termasuk data kredensial dan informasi pribadi pengguna (PII). Berpotensi melanggar UU Perlindungan Data Pribadi (UU PDP) dan menyebabkan kerugian reputasi serta finansial yang signifikan.

Rekomendasi Remediasi

Gunakan parameterized query / prepared statement pada seluruh interaksi database. Terapkan Web Application Firewall (WAF) sebagai lapisan mitigasi tambahan, dan lakukan code review menyeluruh pada modul pencarian.

PT-2026-002 — Broken Access Control pada API Manajemen Pesanan

High

CVSS v3.1: 8.1 · Lokasi: GET /api/v1/orders/{order_id}

Deskripsi

Endpoint tidak memvalidasi kepemilikan resource (Insecure Direct Object Reference / IDOR) — pengguna yang terotentikasi dapat mengakses data pesanan milik pengguna lain hanya dengan mengganti nilai **order_id** secara berurutan.

Dampak Bisnis

Kebocoran data transaksi dan informasi pribadi pelanggan lain, termasuk alamat pengiriman dan riwayat pembelian.

Rekomendasi Remediasi

Terapkan pengecekan otorisasi (ownership check) di sisi server pada setiap akses resource berbasis ID, serta pertimbangkan penggunaan UUID non-sequensial sebagai identifier.

PT-2026-003 — Reflected Cross-Site Scripting (XSS) pada Form Kontak

High

CVSS v3.1: 7.4 · Lokasi: POST /kontak (parameter: nama)

Deskripsi

Input pada field **nama** ditampilkan kembali ke halaman konfirmasi tanpa proses output encoding, memungkinkan eksekusi JavaScript arbitrer di sisi korban melalui tautan yang direkayasa (crafted URL).

Dampak Bisnis

Pencurian session cookie, aksi atas nama korban (session hijacking), dan potensi phishing terhadap pengguna aplikasi.

Rekomendasi Remediasi

Terapkan output encoding (contextual escaping) pada seluruh data yang berasal dari input pengguna, serta aktifkan Content-Security-Policy (CSP) header yang ketat.

PT-2026-004 — Missing Security Headers (CSP, HSTS, X-Frame-Options)

Medium

CVSS v3.1: 5.4 · Lokasi: Seluruh endpoint aplikasi

Deskripsi

Response header keamanan standar seperti **Content-Security-Policy**, **Strict-Transport-Security**, dan **X-Frame-Options** tidak diterapkan secara konsisten pada seluruh halaman aplikasi.

Dampak Bisnis

Meningkatkan permukaan serangan terhadap clickjacking, downgrade HTTPS ke HTTP, dan eksekusi skrip pihak ketiga yang tidak sah.

Rekomendasi Remediasi

Konfigurasi security header secara global di level reverse proxy / load balancer, dengan kebijakan CSP yang whitelist domain terpercaya saja.

PT-2026-005 — Rate Limiting Tidak Memadai pada Endpoint Login

Medium

CVSS v3.1: 5.3 · Lokasi: POST /api/v1/auth/login

Deskripsi

Endpoint login tidak menerapkan pembatasan jumlah percobaan (rate limiting) yang efektif, memungkinkan serangan brute-force / credential stuffing dalam skala besar.

Dampak Bisnis

Kompromi akun pengguna melalui percobaan kata sandi otomatis dalam jumlah besar.

Rekomendasi Remediasi

Terapkan rate limiting berbasis IP dan akun, CAPTCHA setelah beberapa kali percobaan gagal, serta mekanisme account lockout sementara.

04 · MATRIKS RISIKO & REKOMENDASI

Prioritas Remediasi

Rekomendasi berikut disusun berdasarkan kombinasi tingkat keparahan (severity) dan estimasi usaha perbaikan (effort), untuk membantu tim teknis klien memprioritaskan pekerjaan remediasi.

Prioritas	Temuan	CVSS	Estimasi Perbaikan
P0 — Segera	SQL Injection pada Endpoint Pencarian Produk	9.8	2–3 hari
P1 — Tinggi	Broken Access Control pada API Pesanan	8.1	3–5 hari
P1 — Tinggi	Reflected XSS pada Form Kontak	7.4	1–2 hari
P2 — Sedang	Rate Limiting Tidak Memadai pada Login	5.3	2–3 hari
P3 — Sedang	Missing Security Headers (CSP, HSTS)	5.4	1 hari

Rekomendasi Strategis Jangka Panjang

- Terapkan Secure Software Development Lifecycle (SSDLC) dengan security code review pada setiap rilis.
- Lakukan penetration testing berkala minimal setiap 6–12 bulan, atau setiap ada perubahan arsitektur signifikan.
- Implementasikan program bug bounty atau vulnerability disclosure untuk deteksi dini kerentanan.
- Bangun kapabilitas incident response internal, lengkap dengan playbook dan simulasi tabletop exercise.
- Berikan security awareness training rutin kepada tim engineering terkait secure coding practices.

Disclaimer: Dokumen ini adalah CONTOH laporan (sample) yang disusun oleh SkyCyber untuk menunjukkan format dan kedalaman analisis laporan penetration testing kami kepada calon klien. Nama klien, target sistem, serta seluruh temuan kerentanan yang tercantum di dalamnya adalah FIKTIF dan dibuat semata untuk keperluan ilustrasi — tidak merepresentasikan sistem, data, atau insiden keamanan yang sebenarnya. Untuk mendapatkan penawaran penetration testing pada sistem Anda, silakan hubungi tim kami di sales@skycyber.co.id.