

Laporan Tahunan Cyber Assurance

Satu tahun langganan, satu laporan yang bisa dibaca direksi dan dipakai tim teknis: VA tiap kuartal dan penetration test tahunan.

KLIENT PT Contoh Nusantara fiktif	PERIODE Q1 – Q4 12 bulan langganan
CAKUPAN 5 IP + 4 aplikasi web Paket Bisnis	KLASIFIKASI RAHASIA Hanya untuk klien
FIKTIF Seluruh nama klien, alamat IP, domain, dan temuan disusun hanya untuk menunjukkan format dan kedalaman laporan. Bukti teknis disunting.	

Lebih aman, terbukti dengan angka.

Satu halaman untuk direksi: kondisi saat ini, apa yang paling penting, dan apa yang perlu diputuskan.



0 / 3

Temuan Critical terbuka. Ketiganya di Q1 dan satu temuan baru di Q3 sudah ditutup.

43

Celah ditutup sepanjang tahun, seluruhnya diverifikasi melalui VA atau retest.

12

Temuan baru dari pentest Q3 yang tidak terdeteksi oleh VA otomatis.

PRIORITAS UTAMA

- 01 Perbaiki kontrol akses API invoice.** Data tagihan pelanggan lain dapat diakses (AB-26-034, High).

- 02 Terapkan patch Windows Server** yang tertinggal lebih dari 90 hari (AB-26-052, High).

- 03 Nonaktifkan TLS 1.0/1.1** di web-01 dan web-02 (AB-26-047, Medium).

KEPUTUSAN YANG PERLU DIAMBIL MANAJEMEN

- ☐ Menyetujui **jendela pemeliharaan** untuk patching app-01 dalam 14 hari.

- ☐ Menunjuk **penanggung jawab dan tenggat 30 hari** untuk perbaikan AB-26-034.

- ☐ Menetapkan target **nol temuan High** sebelum VA #1 periode berikutnya.

Apa yang diuji, dan bagaimana.

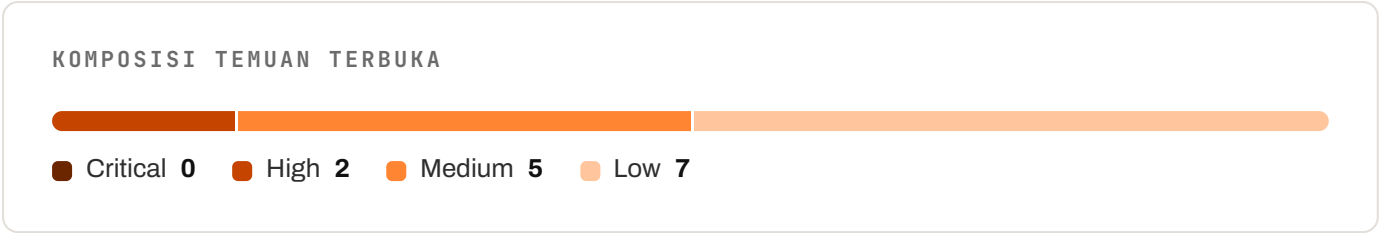
Pengujian dilakukan berdasarkan surat otorisasi dan dokumen ruang lingkup yang telah ditandatangani.

ASET		JENIS	KEGIATAN	WAKTU	METODE
203.0.113.█ • web-01		Ubuntu 22.04 • Nginx	VA #1	Q1	Authenticated & external scan
203.0.113.█ • web-02		Ubuntu 22.04 • Nginx	VA #2	Q2	Authenticated & external scan
203.0.113.█ • app-01		Windows Server 2022 • IIS	VA #3 + Penetration Test	Q3	OWASP WSTG, PTES, grey-box
203.0.113.█ • db-01		PostgreSQL 15	Retest	Q3-Q4	Verifikasi perbaikan
203.0.113.█ • fw-01		Firewall perimeter	VA #4	Q4	Authenticated & external scan
portal.█.co.id		Portal pelanggan			
api.█.co.id		REST API			
hr.█.co.id		Aplikasi HR internal			
vendor.█.co.id		Portal vendor			

Tingkat risiko mengacu pada CVSS v3.1 dan disesuaikan dengan konteks bisnis klien: Critical (9.0–10.0), High (7.0–8.9), Medium (4.0–6.9), Low (0.1–3.9).

14 terbuka. Nol Critical.

Status per akhir Q4. Temuan Low dirinci di lampiran.



ID	TEMUAN	ASET	RISIKO	CVSS	STATUS
AB-26-031	SQL Injection pada endpoint login	api	CRITICAL	9.8	Ditutup • retest lulus
AB-26-034	Broken access control (IDOR) pada API invoice	api	HIGH	8.1	Terbuka
AB-26-052	Patch keamanan kumulatif tertinggal > 90 hari	app-01	HIGH	7.8	Terbuka
AB-26-036	Akun admin tanpa MFA pada portal vendor	vendor	HIGH	7.5	Ditutup • retest lulus
AB-26-047	TLS 1.0/1.1 masih diaktifkan	web-01, web-02	MEDIUM	5.9	Terbuka
AB-26-048	SMB signing tidak diwajibkan	app-01	MEDIUM	5.3	Terbuka
AB-26-039	Pesan error menampilkan stack trace	hr	MEDIUM	5.3	Terbuka
AB-26-041	Session timeout lebih dari 8 jam	portal	MEDIUM	4.8	Terbuka
AB-26-044	Security header (CSP, HSTS) belum diterapkan	portal, vendor	MEDIUM	4.3	Terbuka

Bukti, dampak, perbaikan.

Setiap temuan ditulis supaya tim teknis bisa langsung bekerja. Berikut tiga contoh.

AB-26-031

SQL Injection pada endpoint login

CRITICAL • 9.8

Ditutup

ASET

api. .co.id • POST /v1/auth/login

REFERENSI

CWE-89 • OWASP A03:2021 • ISO 27001 A.8.28

DESKRIPSI

Parameter **username** dirangkai langsung ke query SQL tanpa parameterisasi. Respons aplikasi berbeda bergantung pada kondisi boolean yang disisipkan, sehingga isi database dapat diekstraksi.

BUKTI (DISUNTING)

● ● ● request • response

POST /v1/auth/login HTTP/1.1
Host: api. .co.id
Content-Type: application/json

{"username":"admin[payload boolean-based disunting]","password":"x"}

HTTP/1.1 200 OK ← kondisi TRUE (412 byte)
HTTP/1.1 401 ← kondisi FALSE (96 byte)

DAMPAK

Penyerang tanpa akun dapat membaca tabel pengguna, termasuk data pribadi dan hash kata sandi pelanggan.

REKOMENDASI

Gunakan parameterized query atau ORM, validasi input di sisi server, dan batasi hak akun database aplikasi.

RETEST

Diperbaiki dengan prepared statement. Retest Q4 tidak lagi menunjukkan perbedaan respons: **lulus**.

AB-26-034

Broken access control (IDOR) pada API invoice

HIGH · 8.1

Terbuka

ASET

api.██████.co.id · GET
/v1/invoices/{id}

REFERENSI

CWE-639 · OWASP A01:2021 · ISO 27001
A.8.3, A.8.28

DESKRIPSI

API hanya memeriksa apakah token valid, tetapi tidak memeriksa apakah invoice tersebut milik pengguna yang meminta. Dengan mengganti nilai `id`, pengguna A dapat membuka invoice pengguna B.

BUKTI (DISUNTING)

● ● ● request · response

```
GET /v1/invoices/10482 HTTP/1.1      ← invoice milik akun uji A
Authorization: Bearer ██████████
→ 200 OK
```

```
GET /v1/invoices/10483 HTTP/1.1      ← invoice milik pelanggan lain
Authorization: Bearer ██████████      (token akun uji A yang sama)
→ 200 OK {"customer_name":"██████","address":"██████", ...}
```

DAMPAK

Kebocoran nama, alamat, dan riwayat tagihan pelanggan. Berpotensi menjadi insiden data pribadi yang wajib dilaporkan berdasarkan UU PDP.

REKOMENDASI

Terapkan pemeriksaan kepemilikan objek di setiap endpoint, gunakan ID yang tidak dapat ditebak, dan tambahkan uji otorisasi otomatis di pipeline.

TARGET PERBAIKAN

30 hari · Penanggung jawab: Tim Pengembang API (menunggu penetapan manajemen).

AB-26-047

TLS 1.0/1.1 masih diaktifkan

MEDIUM · 5.9

Terbuka

ASET

web-01, web-02 · port 443

REFERENSI

CWE-327 · ISO 27001 A.8.24 · PCI DSS 4.2.1

BUKTI (DISUNTING)

● ● ● terminal

```
$ sslscan 203.0.113.█:443
SSLv3      disabled
TLSv1.0    enabled
TLSv1.1    enabled
TLSv1.2    enabled
TLSv1.3    enabled
```

DAMPAK

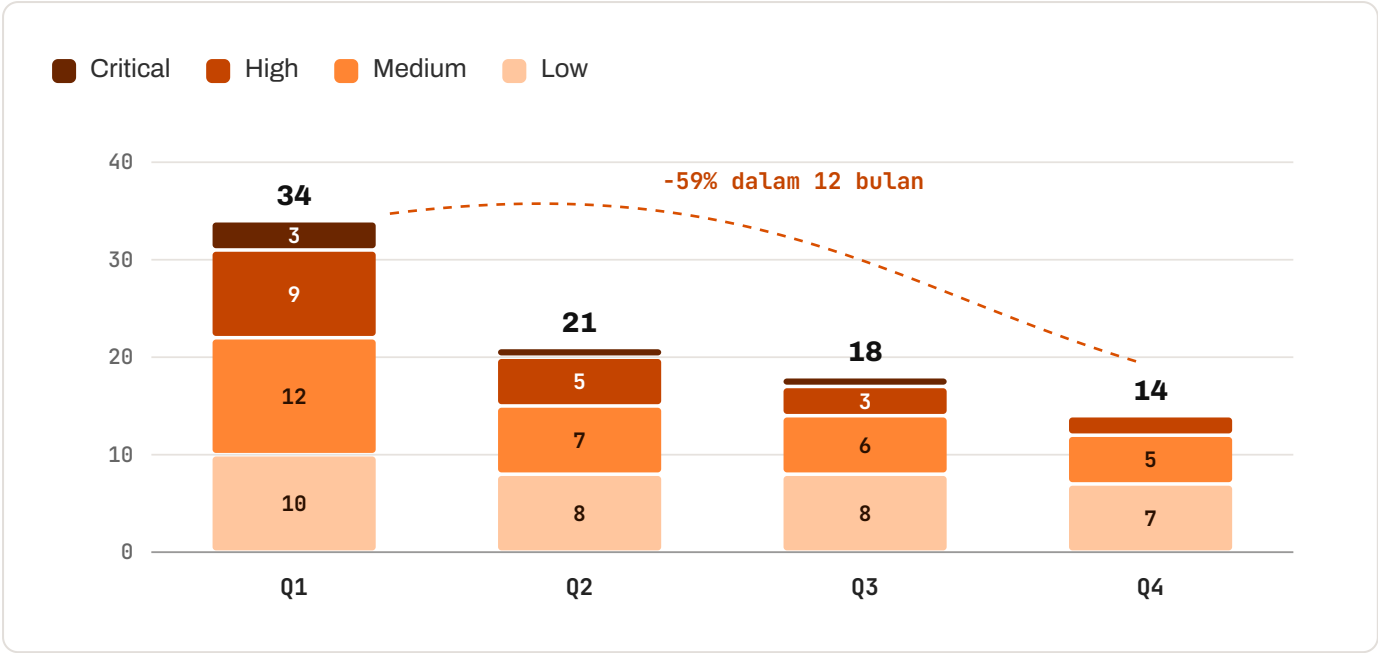
Protokol usang memungkinkan downgrade dan tidak memenuhi persyaratan standar seperti PCI DSS.

REKOMENDASI

Nonaktifkan TLS 1.0/1.1 pada konfigurasi Nginx: `ssl_protocols TLSv1.2 TLSv1.3;` lalu muat ulang layanan.

Setiap kuartal, makin sedikit celah.

Jumlah temuan terbuka di akhir setiap kuartal, berdasarkan tingkat risiko.



KUARTAL	CRITICAL	HIGH	MEDIUM	LOW	TERBUKA	BARU	DITUTUP
Q1 · VA #1	3	9	12	10	34	34	—
Q2 · VA #2	1	5	7	8	21	6	19
Q3 · VA #3 + Pentest	1	3	6	8	18	12	15
Q4 · VA #4	0	2	5	7	14	5	9

Q3 mencatat 12 temuan baru karena penetration test menguji logika aplikasi lebih dalam daripada VA. Hal ini wajar dan menunjukkan nilai pentest tahunan.

Bukti siap untuk auditor.

Setiap temuan dipetakan ke kontrol yang ditanyakan saat audit.

ISO 27001:2022

1/3 kontrol

terpenuhi

A.8.8 terpenuhi. A.8.24 dan A.8.28 sebagian.

UU 27/2022 PDP

Sebagian

Pasal 35 · bergantung pada perbaikan AB-26-034.

PCI DSS v4.0

2/2 kontrol

terpenuhi

11.3 pemindaian kuartalan, 11.4 penetration test.

STANDAR	KONTROL	BUKTI DARI LAYANAN	STATUS
ISO/IEC 27001:2022	A.8.8 Pengelolaan kerentanan teknis	VA 4× setahun, tren perbaikan, retest	Terpenuhi
ISO/IEC 27001:2022	A.8.24 Penggunaan kriptografi	Temuan AB-26-047 (TLS usang)	Sebagian
ISO/IEC 27001:2022	A.8.28 Secure coding	Pentest aplikasi, AB-26-031 dan AB-26-034	Sebagian
UU No. 27/2022 (PDP)	Pasal 35 · Keamanan data pribadi	Pengujian aset yang memproses data pelanggan	Sebagian
PCI DSS v4.0	11.3 Pemindaian kerentanan	VA per kuartal	Terpenuhi
PCI DSS v4.0	11.4 Penetration testing	Pentest tahunan + retest	Terpenuhi

Status pemetaan adalah penilaian teknis berdasarkan ruang lingkup layanan, bukan opini audit atau sertifikasi.

90 hari ke depan.

Disusun berdasarkan risiko, bukan urutan ditemukan.

0-14 hari	0-30 hari	30-60 hari	60-90 hari	Q1 berikutnya
Patch app-01 dalam jendela pemeliharaan, wajibkan SMB signing. AB-26-052 · AB-26-048	Perbaiki pemeriksaan kepemilikan objek di API invoice. AB-26-034	Nonaktifkan TLS 1.0/1.1, terapkan CSP dan HSTS, batasi session timeout. AB-26-047 · 044 · 041	Sembunyikan stack trace di aplikasi HR dan tutup sisa temuan Low. AB-26-039 · Low	VA #1 periode baru memverifikasi seluruh perbaikan. —