

STRUKTUR LAPORAN

Struktur Laporan Penglibatan Standard

Pelanggan: Penglibatan:

Klasifikasi: Sulit

Dokumen ini ialah terjemahan Bahasa Malaysia. Jika berlaku percanggahan, versi Bahasa Inggeris mengatasi. Draf template — perlu semakan undang-undang.

1 • KAWALAN DOKUMEN

MEDAN	NILAI
Rujukan laporan	RT-REP-..... -
Versi / Tarikh	 •
Disediakan oleh	
Disemak oleh	
Pengedaran	

2 • RINGKASAN EKSEKUTIF

- Objektif penglibatan dan tahap ujian dalam bahasa mudah.
- Postur risiko keseluruhan — risiko utama dalam istilah perniagaan, bukan hanya CVSS.
- Angka utama: penemuan mengikut keparahan, isu kritikal, aset terjejas.
- Keutamaan yang disyorkan untuk 30 / 60 / 90 hari akan datang.

3 • GAMBARAN KESELURUHAN PENGLIBATAN

- Skop dibenarkan (dari Borang Kebenaran) dan tempoh ujian.
- Kakitangan yang terlibat dan akses yang disediakan.
- Penyimpangan daripada SOW, jika ada, dan kelulusan.

4 • METODOLOGI

- Penjajaran rangka kerja: OWASP Top 10, ASVS, PTES, OSSTMM.
- Fasa dilaksanakan: peninjauan → pengiraan → eksploitasi (PoC) → pengesahan.
- Alat dan saluran paip bantuan AI yang digunakan (ber-governan, dalam skop, di-audit).
- Had: apa yang tidak diuji dan mengapa.

5 • RINGKASAN PENEMUAN

KEPARAHAN	BILANGAN
KRITIKAL	
TINGGI	
SEDERHANA	
RENDAH	
MAKLUMAT	

Setiap penemuan dinilai mengikut risiko perniagaan sebenar dan keboleh-eksplorasian — keparahan sahaja tidak menentukan keutamaan.

6 • PENEMUAN TERPERINCI

Setiap penemuan mengikut struktur yang sama untuk kebolehulangan:

- **Tajuk & ID** — rujukan unik, cth., RED-001
- **Keparahan** — KRITIKAL / TINGGI / SEDERHANA / RENDAH / MAKLUMAT dengan skor CVSS

- **Aset terjejas** — hos, titik akhir, atau komponen
- **Perihalan** — apa kelemahan itu dan mengapa ia penting
- **Langkah pembiakan** — langkah tepat untuk mengesahkan
- **Bukti** — artifak yang disanitasi (tanpa kelayakan langsung atau data sensitif)
- **Kesan** — kesan perniagaan dan teknikal jika dieksploitasi
- **Pemulihan** — panduan pembetulan konkrit dengan keutamaan
- **Rujukan** — CWE / OWASP / pautan vendor jika berkenaan

7 • KEPUTUSAN UJIAN SEMULA

- Status setiap penemuan selepas pemulihan: Diselesaikan / Diselesaikan Separata / Belum Diselesaikan / Belum Diuji Semula.
- Tempoh dan kaedah ujian semula.
- Risiko baki dan tindakan susulan yang disyorkan.

8 • LAMPIRAN

- Pengesahan skop penuh (sasaran dan tarikh).
- Alat dan versi yang digunakan.
- Garis masa penglibatan dan ringkasan log aktiviti.
- Indeks pakej bukti.

9 • PENGENDALIAN & PENGEKALAN

- Laporan ini sulit di bawah NDA dan untuk pengedaran yang dinamakan sahaja.
- Dikekalkan mengikut tempoh pengekalan dalam Peraturan Penglibatan, kemudian dimusnahkan dengan selamat.
- Pendedahan semula hanya dengan persetujuan bertulis.