

PERATURAN PENGLIBATAN

Penglibatan Keselamatan Ofensif

Pelanggan: Tarikh Kuat Kuasa:

Tempoh: - Sulit

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

1 • TUJUAN

Peraturan Penglibatan ini ("ROE") mengawal pelaksanaan ujian keselamatan yang dibenarkan di bawah Penyata Kerja dan Borang Kebenaran yang mengiringi. Ia mentakrifkan apa yang boleh disentuh, bila, bagaimana, dan apa yang berlaku apabila perkara tidak dijangka berlaku.

2 • PIHAK & KAKITANGAN SAH

Penyedia perkhidmatan: REDTEAM —
.....

Titik hubungan pelanggan: •
.....

Hubungan kecemasan pelanggan: •
.....

3 • SKOP & TEMPOH DIBENARKAN

- Ujian terhad kepada sasaran yang disenaraikan dalam Borang Kebenaran yang ditandatangani. Tiada perkara lain boleh diimbis, dicuba, atau diakses.

- Tempoh ujian aktif:, kecuali dipersetujui sebaliknya secara bertulis.
- Peninjauan pasif boleh berjalan di luar tempoh kecuali Pelanggan membantah.

4 • AKTIVITI DIBENARKAN

- Peninjauan, pengiraan aset, dan penemuan kerentanan dalam skop.
- Eksploitasi dan pengesahan sehingga tahap yang dipersetujui dalam SOW, proof-of-concept sahaja.
- Ujian kelayakan menggunakan kelayakan yang disediakan oleh Pelanggan, di mana dipersetujui.
- Simulasi kejuruteraan sosial, hanya jika dipersetujui secara nyata dalam SOW.

5 • AKTIVITI DILARANG

Tiada kemusnahan. Memadam, merosakkan, atau memusnahkan data, konfigurasi, atau sistem adalah dilarang. Eksploitasi berhenti pada proof-of-concept.

Tiada pengekstrakan data. Tiada data peribadi, kewangan, atau produksi keluar dari persekitaran kecuali artifak bukti minimum yang diperlukan untuk laporan.

Tiada denial-of-service. Tiada gangguan sengaja terhadap ketersediaan melebihi had beban yang dipersetujui. Tiada tindakan terhadap infrastruktur pihak ketiga atau kongsi.

Tiada pengembangan skop. Pergerakan lateral terhad kepada menunjukkan objektif yang dipersetujui. Sebarang penemuan aset di luar skop menghentikan ujian terhadapnya serta-merta.

6 • PENGENDALIAN DATA (PDPA)

- Semua data yang ditemui dianggap sulit di bawah NDA.
- Data produksi dimask dan diminimumkan dalam semua deliverable; hanya apa yang diperlukan oleh bukti dikekalkan.

- Bukti dan log dikekalkan selama kemudian dimusnahkan dengan selamat, atau seperti dipersetujui.

7 • KOMUNIKASI & ESKALASI

- Penemuan kritikal dilaporkan kepada titik hubungan pelanggan dalam masa jam selepas pengesahan.
- Jika ujian secara tidak sengaja menjejaskan ketersediaan, penyedia perkhidmatan berhenti serta-merta dan memaklumkan hubungan kecemasan.
- Jika timbul kekaburan skop, ujian terhadap sasaran yang kabur dihentikan sehingga Pelanggan mengesahkan secara bertulis.

8 • PENGENDALIAN INSIDEN SEMASA UJIAN

Jika pemantauan Pelanggan mengesan aktiviti ujian sebagai mencurigakan, Pelanggan hendaklah mengesahkan dengan titik hubungan sebelum menyekat. Jika insiden sebenar disyaki, Pelanggan boleh menggantung ujian; penyedia perkhidmatan akan membantu membezakan aktiviti ujian daripada insiden.

9 • PENAMATAN

Sama ada Pihak boleh menggantung atau menamatkan penglibatan melalui notis bertulis. Selepas penamatan, ujian berhenti serta-merta dan bukti dipulangkan atau dimusnahkan mengikut NDA.

10 • PERSETUJUAN

Dengan menandatangani di bawah, Pihak-Pihak bersetuju dengan Peraturan Penglibatan ini, bersama Penyata Kerja, Borang Kebenaran, dan NDA yang mengiringi.

Untuk Pelanggan

Untuk REDTEAM

Nama: _____

Nama: _____

Jawatan: _____

Jawatan: _____

Tarikh: _____

Tarikh: _____



REDTEAM • redteam.alesa.my • redteam@alesa.my

Template RT-ROE BM v1.0 •