Laporan Komprehensif mengenai Serangan Suntikan SQL
Suntikan SQL ialah teknik suntikan kod yang digunakan untuk menyerang aplikasi dipacu data dengan mem
kenyataan SQL berniat jahat ke dalam medan input, memintas langkah keselamatan.
Jenis Serangan Suntikan SQL:
Julat Skala Keterukan dari 1 hingga 5

1 paling rendah, 5 paling tinggi
1. In-band SQL Injection: Jenis yang paling biasa di mana penyerang menggunakan perkara yang sama saluran komunikasi untuk melancarkan serangan dan mengumpul hasil.
Keterukan: 3
2. Injeksi SQL berasaskan ralat: Mengeksploitasi mesej ralat yang dijana daripada pangkalan data kepada mengumpul maklumat.
Keterukan: 4
3. Suntikan SQL Buta: Melibatkan penghantaran pertanyaan SQL ke pangkalan data, menentukan kesahihan pertanyaan berdasarkan respons aplikasi.
Keterukan: 5
4. Suntikan SQL berasaskan kesatuan: Memanipulasi hasil pengendali UNION SQL untuk dikumpulkan maklumat daripada pangkalan data.
Keterukan: 2
Pencegahan:
Gunakan pertanyaan berparameter atau pernyataan yang disediakan.
Sahkan dan bersihkan input pengguna.
Gunakan prinsip keistimewaan yang paling sedikit pada akaun pangkalan data.
Kemas kini dan tampal perisian anda secara kerap.
Laksanakan pengesahan input pada kedua-dua sisi klien dan pelayan.
Gunakan tembok api aplikasi web (WAF) untuk menapis dan memantau trafik masuk.
Gunakan prosedur tersimpan atau rangka kerja ORM.
Laksanakan pengendalian ralat yang betul untuk mengelakkan pendedahan maklumat sensitif.
Gunakan amalan dan rangka kerja pengekodan berfokuskan keselamatan.
Lakukan audit keselamatan dan ujian penembusan dengan kerap.