Laporan komprehensif mengenai serangan suntikan SQL
Suntikan SQL ialah teknik suntikan kod yang digunakan untuk menyerang aplikasi berasaskan SQL
Pernyataan SQL berniat jahat dalam medan input, memintas langkah keselamatan.
Jenis serangan suntikan SQL:
Skala keterukan adalah antara 1 hingga 5
1 adalah yang paling rendah, 5 adalah yang tertinggi
1. In-Domain SQL Injection: Jenis yang paling biasa di mana penyerang menggunakan perkara yang sa
Saluran komunikasi untuk melancarkan serangan dan mengumpul hasil.
Keamatan: 3
2. Suntikan SQL berasaskan ralat: mengeksploitasi mesej ralat yang dijana daripada pangkalan data u
Pengumpulan data.
Keamatan: 4
3. Suntikan SQL Buta: Ia melibatkan penghantaran dan menentukan pertanyaan SQL ke pangkalan da
Kesahihan pertanyaan berdasarkan respons aplikasi.
Keamatan: 5
4. Suntikan SQL berasaskan kesatuan: Proses hasil pengendali UNION SQL untuk mengagregatkannya
Maklumat daripada pangkalan data.
Intensiti: 2
perlindungan:
Gunakan pertanyaan dengan parameter atau data yang disediakan.
Sahkan dan bersihkan input pengguna.
Gunakan prinsip keistimewaan paling sedikit dalam pengiraan pangkalan data.
Kemas kini dan tampal perisian anda dengan kerap.
Lakukan pengesahan input pada kedua-dua klien dan pelayan.
Gunakan Web Application Firewall (WAF) untuk menapis dan memantau trafik masuk.
Gunakan prosedur tersimpan atau rangka kerja ORM.
Laksanakan pengendalian ralat yang sesuai untuk mengelakkan pendedahan maklumat sensitif.
Gunakan amalan dan rangka kerja pengekodan berfokuskan keselamatan.
Menjalankan audit keselamatan dan ujian penembusan dengan kerap.