

1. Inference Attack adalah sebuah teknik *data mining* dengan cara menyimpulkan informasi-informasi publik atau umum untuk mendapatkan informasi yang bersifat privat atau private. Hasil dari attack ini adalah sebuah data breached atau kebocoran informasi.

Metode Inference Attack :

- a) Teknik Agregasi :
- b) Teknik Deskriptif
- c) Teknik Data Mining

2 . Kesimpulan yang didapat :

Nama Tabel : Nilai

Nama Kolom : uas

Jumlah baris : 100

Nilai rata-rata dari 20 orang : 78,96

Nilai rata-rata dari 19 orang : 78,27

$$20 \times 78,96 = 1,579.2$$

$$19 \times 78,27 = 1,487.13$$

$$1,579.2 - 1,487.13 = 92.07$$

3 . Jelaskan secara ilmiah mengapa kita harus melakukan serangan SQL injection manual ketimbang menggunakan tool seperti SQL Map dan sejenisnya!

Melakukan serangan SQL Injection secara manual akan membuat kita memiliki lebih banyak pengalaman dan pengetahuan dimana Sebuah Tools tidak memiliki pengalaman dan pengetahuan seperti manusia, sebuah tools memiliki batasan dalam melakukan serangan SQL Injection yang berbeda dan unik.

Untuk menggunakan sebuah tools seperti SQL Map dan sejenis nya harus memiliki pengetahuan bagaimana cara menggunakan tools tersebut sebelumnya, karena dapat menyebabkan sebuah risiko apabila tidak dapat mengonfigurasi SQLMap dengan benar.

4. Jelaskan seperti apa Aplikasi blockchain yang mungkin Anda berpikiran untuk dikembangkan! Jelaskan secara ringkas mekanisme cara kerjanya!

Aplikasi Medical Chain, dimana aplikasi tersebut menggunakan teknologi blockchain dalam memfasilitasi penyimpanan dan pemanfaatan catatan kesehatan elektronik pasien. Sistem tersebut digunakan agar, tidak dapat terjadinya seseorang yang ingin melakukan perubahan pada catatan kesehatan, selain itu receipts of surgeries atau tanda terima operasi dapat disimpan di blockchain dan secara otomatis dikirim ke penyedia asuransi sebagai bukti penhirman.

5. Jelaskan apa yang Anda ketahui tentang:

- a. Smart Contract
- b. Proof of Work
- c. Proof of Stake
- d. Consensus Based Algorithm.

a.) Smart Contract

Adalah sebuah pengaplikasian kode yang digunakan pada blockchain untuk mengikat perjanjian atau sebuah kesepakatan antara beberapa pihak.

b.) Proof of Work

Adalah sebuah algoritma konsensus yang digunakan oleh pengguna blockchain untuk mengonfirmasi sebuah transaksi dan menghasilkan sebuah blok baru pada rantai (*chain*)

c.) Proof of Stake

Adalah sebuah algoritma konsensus alternatif selain PoW, digunakan untuk menemukan Node yang berbeda untuk mencapai sebuah kesepakatan, PoS memiliki kelebihan yaitu memiliki percepatan suatu proses validasi.

d.) Consensus Based Algorithm

Algoritma Konsensus merupakan sebuah mekanisme dimana jaringan blockchain mencapai konsensus, terdapat 3 Jenis Algoritma Konsensus yaitu PoW (proof of work) , PoS(Proof of Stake) dan dPoS (Delegate Proof of Stake)

6. SQL Injection Boolean Based Attack dapat digunakan ketika tidak terjadinya sebuah perubahan pada sebuah web namun memiliki kerentanan sehingga dapat diserang. Serangan ini, hampir sama dengan Normal SQL Injection namun terdapat perbedaan dalam bagaimana data tersebut diambil dari database

7. Saat ini terutama di Indonesia teknologi blockchain belum banyak dimanfaatkan, menurut Anda apa penyebabnya! Sertakan saran Anda terkait hal tersebut!

- a.) Belum banyak nya pengguna yang mengerti terkait Teknologi Blockchain,
- b.) Masih banyak nya masyarakat yang tidak percaya (trust) terkait teknologi blockchain

Saran : Melakukan sosialisasi terkait teknologi blockchain terhadap masyarakat luas.

8. Jelaskan apa saja kelebihan dan kekurangan basis data desentralisasi ketimbang basis data sentralisasi!

a) Kelebihan Basis Data Desentralisasi :

- 1) Repositori yang digunakan lebih kecil dan lebih mudah karena setiap database hanya berisi komponen meta data yang menarik.
- 2) Lokasi penyimpanan data yang dibuat oleh gateway lebih transparan terhadap akses data.
- 3) Setiap repository meta data dapat memiliki meta sendiri seperti model dan desain yang disesuaikan.

b) Kekurangan Basis Data Desentralisasi :

- 1) Pengontrol reduksi di repositori dan menjaga meta data yang konsisten sulit.
- 2) Memakan waktu yang lebih lama untuk memelihara dan mengelola database multipel pada berbagai platform.
- 3) Kaitan meta data diberbagai database mungkin lebih sulit karena meta data tidak otomatis terkait dengan meta data lain yang berada pada database yang lain.
- 4) Pemecahan masalah perbedaan informasi lebih sulit karena menggunakan database multipel dan potensi perbedaan sangat tinggi.

9 . Jelaskan bagaimana cara kita untuk dapat mengubah (tamper) isi data pada sebuah Blockchain :

Salah satu sifat blockchain adalah immutable (tidak bisa diubah) dan append only (hanya bisa ditambahkan) sehingga untuk melakukan perubahan pada isi blockchain adalah dengan cara harus memiliki persetujuan dari pengguna lainnya minimal 51% dari total pengguna lainnya untuk melakukan sebuah perubahan atau modifikasi pada blockchain.

10 . Jelaskan dengan contoh bagaimana cara kerja SQL Injection Time Based Attack!

Merupakan teknik inferensia yang bergantung pada pengiriman query SQL ke database yang memaksa database untuk menunggu dalam rentang waktu tertentu (dalam detik) sebelum melakukan response. Waktu respon tersebut akan mengindikasikan kepada penyerang hasil query yang dilakukan TRUE atau FALSE.

Contoh cara kerja SQL Injection :

SQL Injection Time Based Attack dapat digunakan untuk menyerang kolom search, dimana pada kolom tersebut dituliskan query yang secara umum seperti ini “if (kondisi, yes, no)”
Contoh nya :

Pada kolom search akan dituliskan “if(1=1, sleep(3), 0) - -” apabila statement atau kondisi yang dituliskan pada query benar maka web yang diserang akan melakukan sleep selama 3 detik, dan apabila salah maka tidak terjadi sebuah perubahan.