## Cosa si intende per API REST ?

Una API è un'interfaccia per la programmazione e ha l'obiettivo di esporre delle funzionalità verso altro software. Un'interfaccia è definita nel modo con cui le funzionalità sono esposte e con cui i dati vengono scambiati. REST è uno stile architetturale per API che prevede, in breve:

- la presenza di entità client e server;
- la rappresentazione in risorse delle funzionalità da esporre e l'accesso a esse mediante endpoint URL;
- la possibilità di mantenere uno stato/sessione nel client ma non nel server (ne consegue che durante uno scambio di più richieste tra un client e un server, quest'ultimo può sempre processare ognuna di esse senza ricordarsi delle richieste precedenti);
- lo scambio di dati in formato testuale, HTML, JSON o XML.

Lo stile REST non va identificato con il protocollo HTTP, il quale definisce i dettagli della trasmissione, le azioni che si possono eseguire sugli endpoint e i metodi di autenticazione.

## Cosa si intende per servizio SOAP ?

SOAP è un protocollo di messaggistica standardizzato e definisce il formato dei messaggi e l'interfaccia per esporre funzionalità. Un servizio SOAP espone funzionalità mediante un interfaccia WSDL, la quale si basa sul formato XML, e non mediante endpoint URL. I client richiedono una funzionalità e scambiano dati con messaggi in formato XML.
Il protocollo SOAP può utilizzare come tecnologia di trasmissione il protocollo HTTP e si pone come alternativa agli stili REST e RPC.

## Cos'è un database relazionale ?

Un RDBMS fonda la sua rappresentazione logica dei dati nel concetto di relazione basata sui valori.
Il termine relazione va inteso in questo caso in senso matematico, cioè, come prodotto cartesiano o sottoinsieme del prodotto cartesiano di due o più insiemi.
Solitamente si parte da una rappresentazione concettuale in un modello E-R e da essa si deriva una rappresentazione logica dei dati. Indipendentemente dal modello concettuale usato, il modello relazionale prevede la codifica dell'informazione mediante tabelle/relazioni: ogni tabella/relazione identifica un set omogeneo di dati, ogni riga/tupla rappresenta un dato e ogni colonna identifica un attributo per quei dati.
La caratteristica fondamentale è che le associazioni tra dati in tabelle/relazioni diverse si basano solo sui valori delle tuple e l'ordinamento delle righe e delle colonne invece è irrilevante.

## Cos'è un database NoSQL ?

Per database NoSQL si intende un database che implementa uno scherma logico diverso dal modello relazionale tabellare e dal linguaggio SQL. Le soluzioni della famiglia NoSQL sono di vario tipo, identificate a seconda del pattern architetturale utilizzato: chiave-valore, grafo, famiglia di colonne o gerarchia di documenti (MongoDB per esempio).
Essi rispondono principalmente alle esigenze crescenti negli ultimi anni per la gestione di big data, i quali non sono solo tanti e prodotti velocemente ma sono anche eterogenei e destrutturati. Gli schemi logici della famiglia NoSQL, sia perché meno rigidi (gerarchia di documenti) o perché adatti per contesti particolare (database a grafo), inseme all'approccio open source e alla modularità delle soluzioni, favoriscono l'adozione di queste tecnologie per processi di business agili o con esigenze specifiche.

## Cos'è un ORM ? Fai almeno un esempio.

Un ORM è il layer software che si occupa di tradurre il modello a oggetti, usato in un linguaggio di programmazione, nel modello logico utilizzato in una base di dati relazionale.
Prendiamo un oggetto o un dizionario in un linguaggio a oggetti, che vogliamo salvare in un database SQL: il software ORM offre un'interfaccia con la quale tradurre le operazioni in query specifiche dell'implementazione

SQL e con cui codificare l’informazione strutturata del linguaggio a oggetti in uno o più dati organizzati in tabelle. Un’interfaccia può essere costituita per esempio da metodi di “salva_record”, “leggi_record_con_condizione”, “aggrega_dati” e così via. Uno strato ORM può essere scritto manualmente oppure possono essere usate soluzioni standard, come per esempio Hibernate per Java.

## Cos'è la SQL Injection ?

Una SQL Injection può essere compiuta da un malintenzionato quando un sito web prevede l’inserimento i dati che verranno utilizzati dal backend per effettuare delle query su un database SQL. Di base i valori inseriti dagli utenti vengono concatenati e inseriti dal backend all’interno della stringa query per il database. SQL Injection consiste nell’inserire degli operatori del linguaggio SQL all’interno del dato di ingresso, modificando così la query stessa (aggiungendo per esempio condizioni o altri statement per leggere tutti i dati o modificare dati senza permesso). Il tipo di dato fornito in ingresso è trattato come stringa dal backend, per realizzare l’attacco quindi sarà sufficiente inserire un carattere del tipo “ oppure ‘ per uscire dal contesto della stringa e modificare lo statement SQL.

## Cos'è l'autenticazione a 2 fattori? Descrivi brevemente un esempio.

Un’autenticazione a due fattori prevede, per validare un’operazione, l’utilizzo di due metodi di autenticazione anziché uno. Se il primo metodo di autenticazione è una password, il secondo può essere il possesso di un certo dispositivo. Il possesso di quel dispositivo permette l’invio di un OTP mediante un canale sicuro o l’esecuzione di procedure software prestabilite (per esempio con uno smartphone autenticato) oppure presenta dei componenti specifici per validare l’operazione (come un chip leggibile mediante NFC in una carta di identità elettronica).

## Descrivi brevemente un metodo sicuro per salvare le password degli utenti sul DB.

Un metodo sicuro è quello di salvare l’hash della password e non le password in chiaro. La proprietà di unidirezionalità delle funzioni hash garantisce che, se la funzione è crittograficamente forte e non obsoleta, anche leggendo i record delle password in un database, sia impossibile risalire alla password in chiaro. In fase di inserimento della password per ottenere dei permessi, viene calcolato l’hash mediante lo stesso algoritmo e fatta la verifica. Questo è lo stesso metodo utilizzato nei sistemi operativi per le password degli utenti.

## Cos'è una Sticky Session in un sistema con Load Balancing?

Sticky Session vuol dire associare un utente, mediante un ID, a un server specifico per la durata di una sessione. Questa funzionalità ha particolarmente senso quando il server ha il compito di mantenere uno stato rispetto alla sessione e ha anche il vantaggio di favorire l’utilizzo della cache in RAM.