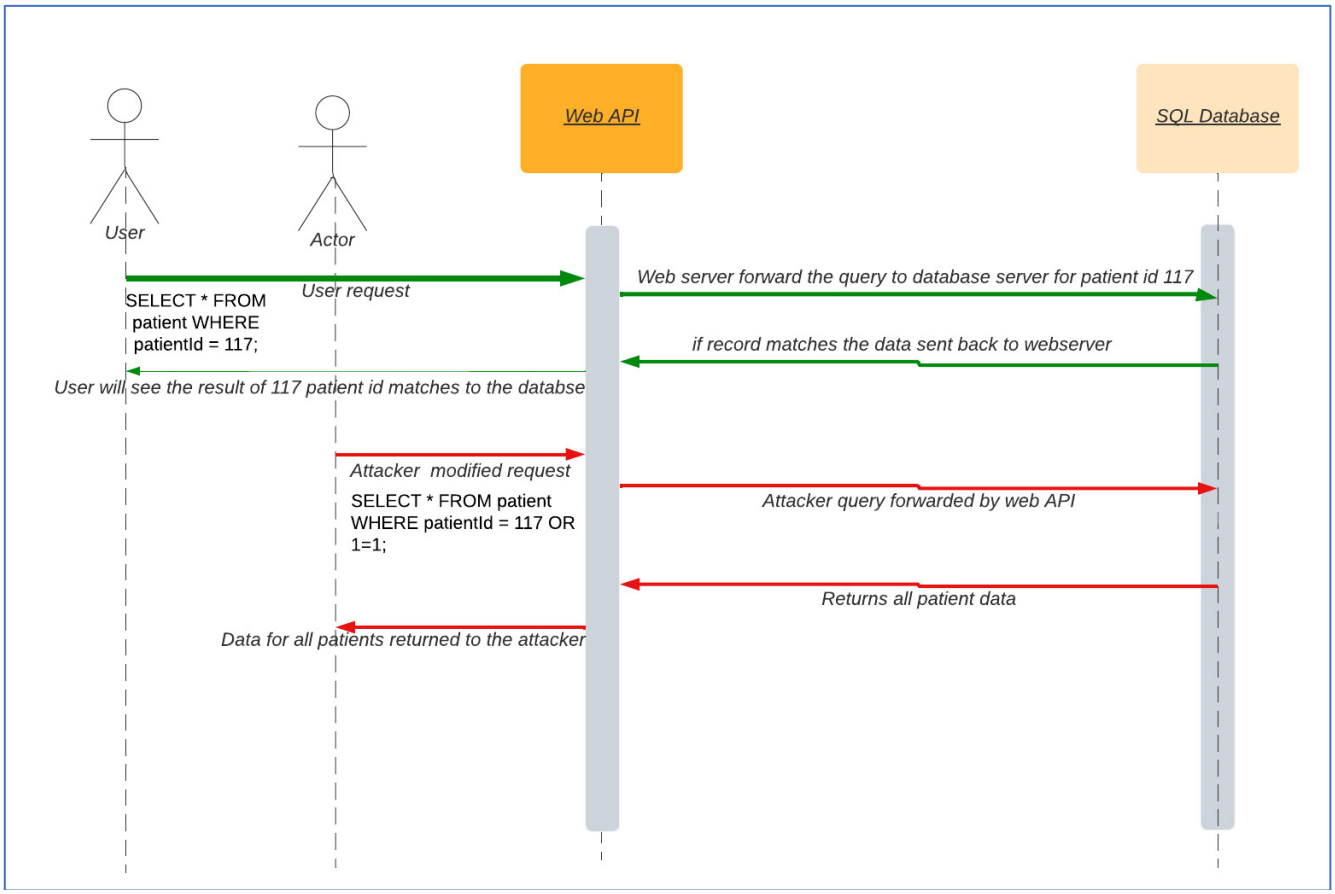
SQL Injection:

SQL injections A03:2021-Injection is one of the top 10 category of OWSAP.

Structured Query Language (SQL) Injection is a type of code injection that is used to change or get data from SQL databases. By putting special SQL statements into an entry field, an attacker can run commands that let them get data from the database, delete sensitive data, or do other things that aren't good for the database.

With the right SQL command, an unauthorised user can pretend to be a more powerful user, make themselves or other people database administrators, change existing data, change transactions and balances, and get and/or delete all server data. Williams, J. and kingthorin, J. (n.d.)

Following are a simple example how any attacker can modify a SQL query and extract data from the SQL database. (Cloudflare,N.D)



patientid = getRequestString("patientId");
lookupPatient = "SELECT * FROM patient WHERE patientId = " + patientId

Please enter your Patient ID number: 117
SELECT * FROM patient WHERE patientId = 117;

Attacker SQL Injection query will look like this:

Attacker use patient ID number: 117 OR 1=1

SELECT * FROM patient WHERE patientId = 117 OR 1=1;

SQL injection works by going after an API, which stands for Application Programming Interface. An API in this case is the software interface through which a server receives and responds to requests.

There are widely used tools that allow a bad actor to automatically search a website for forms and then try to use SQL queries that may cause a response that the website's software developers did not expect to exploit the database. (Cloudflare,N.D)

SQL injection can be prevented in few methods,

1. Escape all users in input
2. Use Stored procedures
3. Least privilege

Reference:

1. Williams, J. and kingthorin, J. (n.d.) *Injection theory*, *Injection Theory | OWASP Foundation*. Available from : https://owasp.org/www-community/Injection_Theory (Accessed: November 20, 2022).
2. Cloudflare (n.d.) *What is SQL injection? | cloudflare*, *What is SQL injection?* Available from : https://www.cloudflare.com/learning/security/threats/sql-injection/ (Accessed: November 20, 2022).