Secure Software Development November 2022

« Collaborative Discussion 1: UML flowchart

Uvaraj Balasubramaniam

Initial Post

29 days ago

1 reply

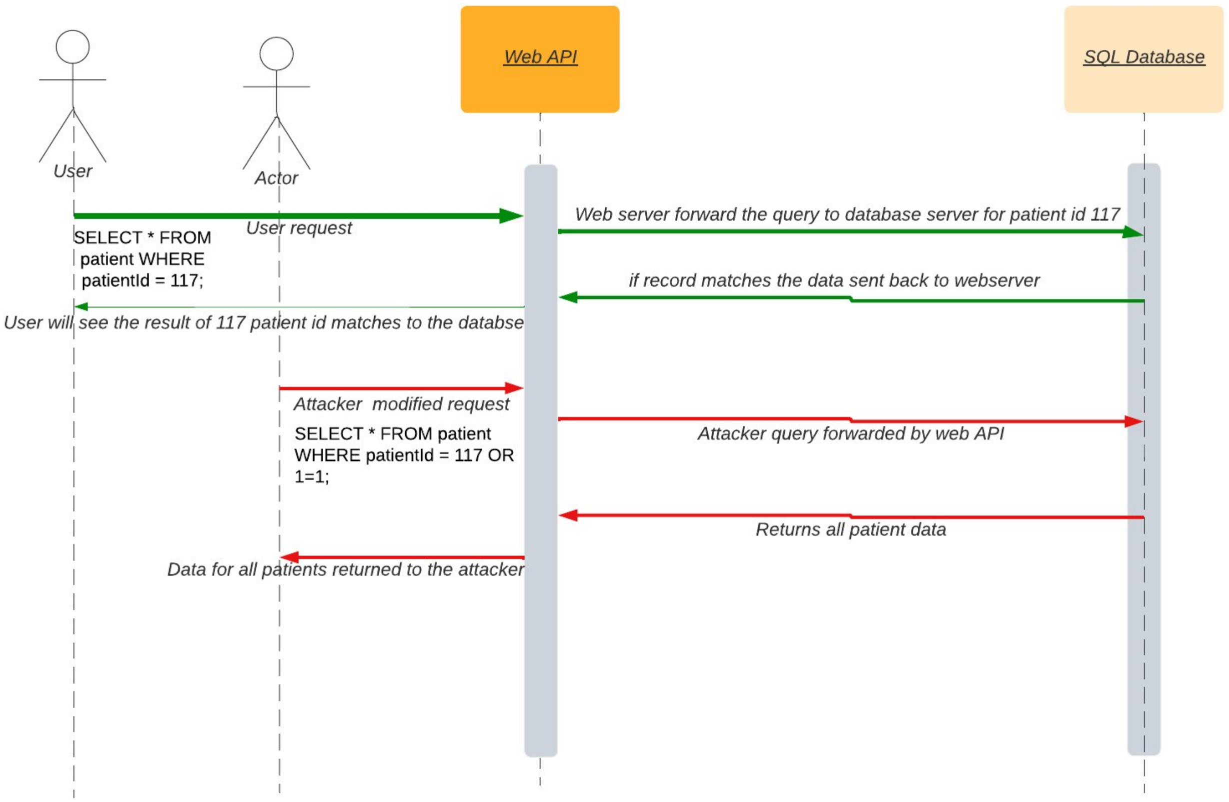
Last 1 hour ago

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)



Sequence diagram

Uvaraj Balasubramaniam | November 20, 2022

```
SELECT * FROM patient WHERE patientId = 117;
```

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

Web API
SQL Database
User
Actor
User request
Web server forward the query to database server for patient id 117
if record matches the data sent back to webserver
User will see the result of 117 patient id matches to the databse
Attacker modified request
Attacker query forwarded by web API
Returns all patient data
Data for all patients returned to the attacker

```
 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,

- Escape all users in input
- Use Stored procedures
- Least privilege

Reference:

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).

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).

SQL Injection Initial Post.pdf

Reply

1 reply

1

Post by **Ashok Kumar Shanmugam**

Peer response

1 hour ago

You have a great understanding about the SQL injection concept. General terms for Preventing SQL Injection: Depending on the subtype of SQLi vulnerability, the SQL database engine, and the programming language, different preventive strategies must be used. To protect your online application, you should adhere to a few broad strategic concepts. Step 1: Educate and maintain awareness - To make your online application secure, all parties engaged in its development must get training on how to handle the threats posed by SQL Injections. Step 2: Don't trust any user input; instead, treat every user input suspiciously. A danger of a SQL Injection is introduced by any user input utilised in a SQL query. The same rules that apply to public input also apply to input from authorised and/or internal users. Filtering in Step 3: Avoid using blacklists to filter user input. Almost usually, a c lever attacker can get around your blacklist. Verify and filter user input, if feasible, exclusively using stringent whitelists. Only ASCII characters are accepted by the white list filter, which rejects all other characters (this is only an example; it does not imply that permitting ASCII character set prevents

SQL Injection). White list filtering ought to be your first option when putting in place Web application filtering techniques, particularly when the input is highly precise, such credit card numbers. Adopt the newest technology and tried-and-true methods in Step 4. - SQLi protection is absent from earlier web development technologies. Use the most recent versions of the language and development environment that are connected with that language and environment. Most contemporary development technologies include safeguards against SQLi. Step 6: Regularly scan your online apps using a web vulnerability scanner like Acunetix. Step 7: Use parameterized queries, which are queries where only the parameters are allowed during query execution. Cybercriminals find it challenging to change the stated functions' intended purpose as a result. Before the S QL query is executed, parameterized queries correctly substitute arguments. It does away with the potential that "dirty" input may alter the meaning of your search.

Reply

Maximum rating: -

Add your reply

Your subject

Type your post

Choose Files No file chosen

Submit

Use advanced editor and additional options

Older discussion

Initial Post

Newer discussion

Initial Post