**SQL Injection (Summery Post)**

After researching Django and many popular frameworks and libraries such as Node.js and Laravel, they all seem to have solved the SQL injection problem from their side or provided the developers with tools that allow them to prevent this kind of attack.

For instance, the Laravel framework strongly recommends avoiding using raw queries and instead using its safe query functions that help in preventing SQL injections (laravel 2022). Another framework that has built-in functionality to help mitigate SQL injection is Django. Django (Django 2022) employs the usage of query parameterization to protect itself from SQL injection.

While both Larvael and Django have functions in place to help mitigate SQL injection, they also allow the user to use raw queries. However, the responsibility of preventing SQL injection and sanitizing user input falls on the developer's shoulders. This is why knowing how SQL injection is performed is vital to software security. It is essential that all developers know these attacks and how they are performed since preventing them is a trivial task in today's world. In addition, it is crucial not to take the framework developer at face value and conduct tests on whether their implementation of preventing SQL injection works correctly or not.

Black hat hackers are constantly fighting software engineers and their software to find a way to gain access to people's information, passwords, and credit card details. This is why all software developers must keep themselves up to date on cybersecurity issues and news. Additionally, it is important to constantly test and patch software once a vulnerability has been discovered. Finally, updating frameworks and libraries the software uses is crucial since most libraries release security patches from time to time.

In closing, SQL injection is a very well-known attack that can be easily prevented by reading the framework documentation the developer is using and taking appropriate actions to prevent it, such as employing user input sanitization.

References:

The PHP framework for web artisans (no date) Laravel. Available at: https://laravel.com/docs/9.x/queries#raw-expressions (Accessed: December 5, 2022).

Django (no date) Django Project. Available at: https://docs.djangoproject.com/en/3.1/topics/security/#sql-injection-protection (Accessed: December 5, 2022).