A1: Injection

A1:2017-Injection is the first item that you can see in OWASP’s list. OWASP stands for Open Web Application Security Project. In making web applications you need to have a database where you can store all data including the sensitive data. Injection is an attacker that we can often encounter in web application that uses database queries or what we called SQL Injection. To be able to communicate with the database we uses SQL (Structured Query Language) this is the language used to talk or communicate to the database. The attackers will have the power to change the meaning of the commands sent to an interpreter by sending other command to get data to a web application. The main target of this attacker will be the web application that uses a command to function. The attackers can trick the back end database that results into entering the off limits data without proper authorization. If the attack was successful the outcome or the effect could be data breaks and loss of controls to the web application.

Medication

So the question is how can we medicate this kind of threat, what are the things that we should do or follow? What are the ways that we can guard our web application? So we’ve done a research on how to prevent this kind of threat. According to our researched here are some ways. First, when building a web application you should have an assurance that you built it with proper access controls and proper defense mechanism in place to make sure that the website you are building is safe from threats like injection. Second, Query Parameterization it is also known as prepared query, this is execution of query that separates the query string from parameter values of query. Third, make sure that you require all the users to validate all information that they’re inputting when signing in on your web application. The last thing that we can recommend is to use limit in SQL statement in database so that you’ll limit the exposure.

Example

The first thing that popped out in our screen while doing the research is Yahoo, we are all familiar in Yahoo, it works like Google. According to our research it happened on 2013 – 2014. But in September 2016 they announced that they had been the victim of data breach in 2014 and 500 million users are affected, the attacker compromised information like email addresses, dates of birth, real name and telephone numbers. But 3 months later Yahoo claimed that they had been breach in 2013 by a group of hackers and compromised 1 billion accounts, beside their basic information they also compromised the passwords of the users. In October 2017 Yahoo revised their estimate, they’re saying that in 2013 – 2014 3 billion user accounts had been compromised.