Pushing Left, Like a Boss — Part 5.2- Use Safe Dependencies

SheHacksPurple [Follow]

Oct 23, 2018 · 2 min read

The previous article in this series was Part 5.1 — Input Validation, Output Encoding and Parameterized Queries.

According to many sources between 70–90% of application code is contained within libraries and other 3rd party components. When we use libraries, frameworks and other 3rd party components, we are accepting all of the risks that come with them (including vulnerabilities). Luckily for us, when security researchers find security vulnerabilities in products (including libraries, frameworks and other components) they often report them to **Mitre**, who log them in the **Common Vulnerability Enumerator (CVE) database**, a publicly searchable database containing all publicly-disclosed known vulnerabilities**. Using the CVE database either manually or (preferably) through use of an automated tool, to verify if your application is using known-vulnerable components is a key strategy to improve the security of your custom-built applications. There are *many* free and premium tools on the market (listed below), and I would suggest that you use *at least* one of them to ensure that the 3rd party code you are using is safe.