# Using Components with Known Vulnerabilities Prevention in PHP

a) Many modern web developers use components such as libraries and frameworks in their web applications. These components are pieces of software that help developers avoid redundant work and provide needed functionality; common example include front-end frameworks like React and smaller libraries that used to add share icons or a/b testing. Some attackers look for vulnerabilities in these components which they can then use to orchestrate attacks. Some of the more popular components are used on hundreds of thousands of websites; an attacker finding a security hole in one of these components could leave hundreds of thousands of sites vulnerable to exploit.

b) Component developers often offer security patches and updates to plug up known vulnerabilities, but web application developers don't always have the patched or most-recent versions of components running on their applications. To minimize the risk of running components with known vulnerabilities, developers should remove unused components from their projects, as well as ensuring that they are receiving components from a trusted source and ensuring they are up to date.

## Prevention:

1- Toolkit will scan for the following if up to date:
   a. Checking PHP Version
   b. Checking XML Version
   c. Checking MySQL Server Version

   And will notify developer of any outdated versions

2- Some Verbal Advices
   a. Don't use any outdated or depricated services or plugins, make sure they are updated and patched.

To learn more, go here:
https://www.youtube.com/watch?v=IGsNYVDKRV0
https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A9-Using_Components_with_Known_Vulnerabilities