SAST and DAST are two application security testing methodologies which are used to find security vulnerabilities that could lead to attacks on the application in the future.

SAST is a white box method of testing I will examine the source code and it will find the software flaws and weaknesses such as SQL injection. It is tested from the inside out. It doesn’t require an actual working application it will only require the source code. The application wont need to be executed. This will find problems early on in development and doesn’t have to wait to the end to find problems this leads to lowering costs as problems don’t be as expensive.it doesn’t show any run-time problems but DAST will show the run-time problems and it can be used with almost all types of software. It is testing from the developers approach. This approach will check that it is working the way it is supposed to.

DAST is a black box testing method which examines the application when it is running to find the vulnerabilities which the attack could attack. It is tested from the outside in. SAST requires a running application and it analyses the application through the application that was executed. It doesn’t need the source code. This will find the problems near the end of development. Problems can be expensive as they are only discovered late in development.it will show run-time problems also. This testing is from the hackers approach because they wont see the code. It will check for areas where the application could break.

SAST is performed early for the files containing source code. DAST Is different because it is performed on running application In an environment which will be similar to production.

I would recommend that when making an application that both SAST and DAST is used because they are both used in different circumstances. We will use SAST to test the source code early on and find problems and we will use DAST later on to find problems in the application.

Some SAST examples are Fortify static code analyzer, Veracode, Coverity scan and findbugs.

Some DAST examples are Netsparker, Acunetix, PortSwigger and AppScan.