Tyler O’Riley

CSD370 Assignment 5.2

08/30/2023

DAST – Dynamic Application Security Testing

DAST is a form of testing, like how you may test a copy of a code outside of a main branch. With code testing, we test its functionality on a copy of the branch we are working with before we implement it to the master branch. DAST is similar in that software is executed in an emulated environment with the intent of evaluating behaviors based on inputs.

Invicti is a resource that utilizes DAST in an automatic fashion. The flare of this product is to offer a customer the ability to run DAST functions automatically without the need for manual configuration.

[Invicti\_Website](https://www.invicti.com/plp/dast/?utm_term=dast%20tools&utm_campaign=11999390822&utm_content=111196403730&utm_source=google&utm_medium=cpc&gad=1&gclid=Cj0KCQjw0bunBhD9ARIsAAZl0E2pAR3l5JsLeMbRbaNgBhkkjqAi2x_mSR7jL-9af4cC979TuhdzKagaAqZ4EALw_wcB)

SAST – Static Application Security Testing

This term covers the idea of performing maintenance on code without running it in an active environment. You can think of this method as building a computer. When all the parts are assembled, you want to turn on the PC to ensure all parts activate, but you don’t run any kind of setup. SAST is similar to the idea you want to evaluate the code either by hand or with tools, but you do not put the software in an active status to do so.

Spectral is a tool for SAST that works a bit like Invicti. It is an automated scanning software that actively checks your source code for vulnerabilities and flaws.

[Spectralops\_Website](https://spectralops.io/sast-tool/?utm_term=sast&utm_campaign=SAST&utm_source=google&utm_medium=ppc&hsa_acc=1287660619&hsa_cam=12806277107&hsa_grp=122562209938&hsa_ad=516283711373&hsa_src=g&hsa_tgt=kwd-297318662609&hsa_kw=sast&hsa_mt=e&hsa_net=adwords&hsa_ver=3&gclid=Cj0KCQjw0bunBhD9ARIsAAZl0E25O48ZJTI-DzPGBK8DpQI2q-dcS66ekFAlUF095jSkkZFvnO5wDeEaApXREALw_wcB)

IAST – Interactive Application Security Testing

Being one of the more expensive processes, IAST is a complete testing environment that aims to review all processes of an application. Whereas the other methods use specific techniques to review software, IAST will use specific sensors that match the function it is evaluating.

Contrast Security was one of the few tools I could find that primarily used IAST. It embeds security analysis functionality into an application and reports security vulnerabilities in a way that a developer can easily implement patch code.

[Contrast\_Security](https://www.contrastsecurity.com/devsecops)

RASP – Runtime Application Self-Protection

This technology is the newest and most unique of our four terms. Unlike the other concepts, RASP is not a testing environment and instead is an active tool that runs side-by-side as the application is in active runtime. It reports incidents as they occur and can run prevention functions so detected vulnerabilities cannot attempt harm.

While not a direct tool, Amazon Web Services (AWS) has a very complex and detailed RASP system that covers a lot of the services’ footprint.

[Amazon](https://wa.aws.amazon.com/serv.question.SEC_3.en.html)