International Journal of Management and Engineering Research
ISSN: 2799-1997 Volume: 1 Issue: 1
***Article Received**: 20 March 2021 **Revised**: 25 April 2021 **Accepted**: 10 May 2021 **Publication**: 30 June 2021*

Learning the Idea Behind SAST (Static Application Security Testing) and How It Functions

Nouby Mahdy Ghazaly
Associate professor,
Mechanical Engineering Departments
Faculty of Engineering South Valley University Egypt

Abstract: - The Static Application Security Testing (SAST) technique is used to examine the source code, byte code, assembly code, etc. to look for vulnerabilities that could endanger the security of the software that is currently being developed. IT is one of the automation testing methods that examines code flaws without actually running the test code. It is a type of white box testing technique that is carried out prior to code compilation. This is advantageous since all errors found during testing may be addressed before the code is compiled, saving time and resources. It functions as a tool that is utilised throughout the software development.

Keywords: - introduction to SAST, its operational mechanism, SAST implementation procedure, Benefits of SAST, SAST's drawbacks Security flaws discovered by SAST

Introduction: -

The traditional testing techniques used to identify the bugs in the software being developed usually takes place when the complete code is written and compiled. This means, once the developers are done with the writing of the code and compiled then it is given to the testers to identify the bugs in the code. When the testers identify all the bugs then again, the developers will recreate them and then fix the code to make it bug free. It is time consuming task and takes a great number of efforts by the developers to identify the point in the code to resolve the issue. Also, the traditional testing methods are not efficient enough to detect the security vulnerabilities during the software development life cycle. Many latest technologies have come into existence to get rid of these issues. One such technology or we can say tool is Static application security testing which acts like an analysing tool whose objective is to detect the security check points in the software. This is one of the automation testing techniques which will test the source code before it is actually compiled. The developer will be able to fix all the bugs reported before the compilation of the code which saves a lot of time and effort. It also helps in on time delivery of the product since there will be less bugs and it will be easy to fix the errors before actual delivery of the product to the client. Since static application security testing apparatuses needn't bother with a running application to play out an examination, they can be utilized early and frequently in the execution period of the product improvement life cycle (SDLC). As an engineer is composing code, SAST can break down it continuously to educate the client regarding any standard infringement, so you can promptly manage issues and convey better applications out of the crate while forestalling issues toward the finish of the improvement interaction.

Working Mechanism of SAST: - [1]

SAST works by following steps and use them to identify the crucial weak point in the software code: -

- SAST uses the analysis process of the code evaluation process and identify if there are any vulnerabilities which could prove to be fatal. The goal of this technique is to identify majorly the security issues like SQL injections, error handling etc.

- It is used to implement various coding protocols and standards for the development team to follow and acts like application security tool which is used to identify issues related to security as well as functional bugs in the code of the software which is under the process of development.

- SAST technique gives its benefits only if it is implemented at the initial stages of the development process and will give quick results but if the whole code is written then it will be difficult to implement the technique as it will be time consuming process after the complete code is written.

- It uses the concept of white box testing technique to identify the bugs by analysis of the source code.

- SAST is dependent on the type of language used for the development of the project. It main focus will always be on the code and identify the code vulnerabilities.
- Following types of analysis is performed using SAST technique: -
  a. Semantic analysis: - To identify syntax error.
  b. Configuration analysis: - Identify vulnerabilities of the configuration files.
  c. Control flow analysis: - Identify bugs in the work flow process.
  d. Dataflow analysis: - To check the validity of the input given.
  e. Structural analysis: - Identify issues related to language specific code structure.

- The analysis technique used by SAST uses specific set of rules to identify the security issues that might occur in the software under development.

- It is used to identify the bugs in the application from inside out. It can be used during all the phases of the software development life cycle.

- The only requirement in this type of technique is that it needs to create a model which the tool can understand.
  Implementation process of SAST: - [2]
  Following are the stages of the implementation process of the SAST technique: -

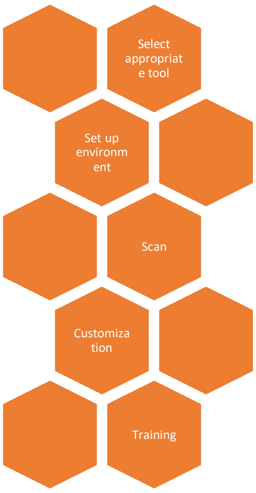

Figure 1 Stages of implementation process of SAST.

1. Select appropriate tool: -
   SAST has various tools which can be used to identify the issues in the code. The tool will give correct results only if it is right for the code in which language it is written. Therefore, the first step will be to identify the best SAST tool which will work best as per the coding language used in the development of the product or software.

2. Set up testing and deployment environment: -
   The benefit of using SAST tool is that it does not require setting up of extra resources for its installation. Once the testing and deployment environment is set up, the SAST tool can be installed in the same environment and then the testing and analysis of the application pipelined can be tested based upon their priorities.

3. Scanning process: -
   Another rule for the SAST tool is that it should be run regularly to give best results. The time interval can be fixed like it can be run on a daily basis, weekly or monthly. Basically, anytime code is written then the SAST scan must be initialised.

4. Customization: -
   The SAST tool can be customised as per the project's requirements. It can be used to represent the scan results, and also can be used to create online and offline reports.

***Article Received**: 20 March 2021 **Revised**: 25 April 2021 **Accepted**: 10 May 2021 **Publication**: 30 June 2021*

5. Training: -
   In order to achieve best results from the SAST tool, it is necessary that all the team members should be properly trained on the usage of the SAST tool. The rules and guidelines to be followed to use SAST tool must be available for the access anytime for everybody so that their tasks should not be delayed.

Vulnerabilities detected by SAST tool: -
Following are main vulnerabilities that be detected by the SAST tool used during the software development life cycle: - [3]

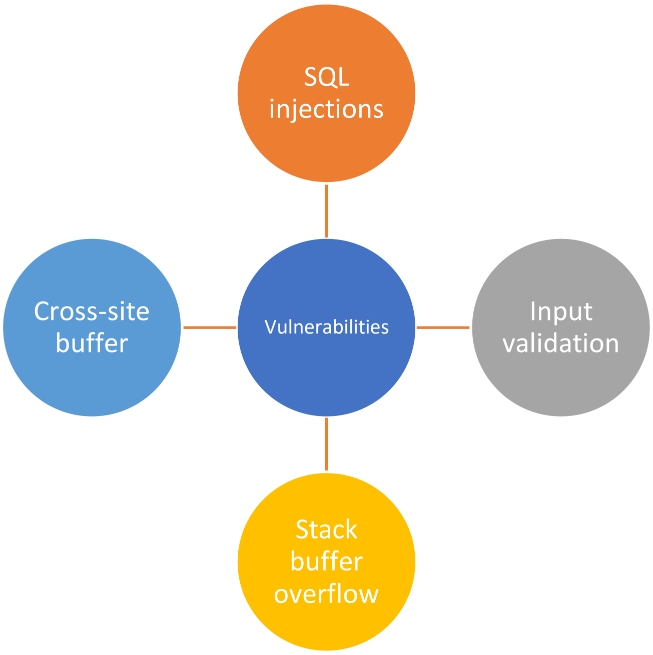

Figure 2. Vulnerabilities detected by SAST.

1. SQL Injections: -
   SQL injection is the attack on the data of the software to exploit the confidential information which is done by injecting SQL query into the database. With the use of SAST tool these kinds of attacks can be easily detected and fixed.

2. Input Validation: -
   This is common type of attack where the attacker notices the behaviour of the application by giving malicious input into the software application. SAST is a perfect tool which efficiently detect this kind of vulnerability in the coding section.

3. Stack- buffer overflow: -
   Stack buffer overflow happens when someone is trying to fit more data than it can accommodate. This causes the application to crash and also lead to data corruption.

4. Cross-site scripting: -
   In this type of attack the attacker send malicious data to the user of the application and acts like as if it is sent by the browser of the application. This happens when the code is not properly encoded. So, SAST helps to identify such attacks and helps to fix them.
   Benefits of SAST: - [4]
   Following are some of the advantages of SAST technology: -

1. Non- Execution tool: -
   It is the type of security tool which uses only the source code to find the issues and does not require the execution of the code. It gives faster results as it runs on the compiled code.
2. Line of problem: -
   It is used to not only identify the issues in the code but also identifies the location of the issue in the code so it could be easily located and then fixed as soon as it is detected.

3. Easy automation testing: -
   It is the technique which does not require any manual efforts for the testing and the automation process is very simple and has easy instructions to be followed.

4. Early SDLC: -
   Since SAST is used on the source code, so it can be implemented as early as possible in the software development life cycle process. The SAST scan can be initialised even before the complete code is written.

5. Defined rules: -
   SAST it will apply rules to the source code and these principles can be set physically or can be mechanized utilizing calculations utilized for the predefined rules in the SAST.

Limitations of SAST: - [5]
Following are the challenges or disadvantages of SAST: -
1.Difficult to set up initially: - Developers have discovered that the initial implementation of SAST in agile environment is challenging task.

2. Dependency: - The other limitation of the tool is that it is dependent upon the type of language used for writing the code of the software being developed.

3. False positives: - This is one of the biggest challenges of SAST where it gives false positives. This means the SAST tool will pick up code lines from the source code even though those are not the vulnerable points and does not act like threat to the application.

5. Usage of more than one SAST tool: - In some applications, there is requirement of more than one SAST tool to detect the issues.

Conclusion: -

SAST is the Static application security testing procedure which is utilized to break down the source code, byte code, gathering code and so on to check for the flimsy spots which could be a danger for the security of the product a work in progress. IT is one of the robotization testing's which examinations the weaknesses in the code without real execution of the test code. It is one of the types of white box testing procedure which is performed before the aggregation of the code. This is valuable as every one of the bugs detailed during this testing can be fixed before the code is gathered which assists with saving time and endeavours. It behaves like an apparatus which is utilized during the product improvement life cycle whose goal is to distinguish the bugs during the improvement interaction of the product in the improvement climate. It is well known among the designers as it assists engineers with recognizing practically every one of the significant weaknesses by investigating the code composed by them before it is gathered. That's what this will ensure on the off chance that there are any bugs then the engineers can correct them and make the code productive to safeguard them against the weaknesses.

References: -

1.https://snyk.io/learn/application-security/static-application-security-testing/
2.https://www.softwaretestinghelp.com/sast-tutorial/
3.https://www.mend.io/resources/blog/sast-static-application-security-testing/
4.https://cypressdatadefense.com/blog/sast-advantage/
5.https://www.traceable.ai/blog-post/does-sast-deliver-the-challenges-of-code-scanning