International Journal of Science and Technological Research
ISSN: 2815-052X Volume: 2 Issue: 1
***Article Received**: 25 March 2022 **Revised**: 21 April 2022 **Accepted**: 14 May 2022 **Publication**: 30 June 2022*

Analysis of Dynamic Application Security Testing and A Comparison of Its Benefits to SAST

Vikash Soni
Research Scholar,
Jaipur National University
Rajasthan, India

Abstract: - By simulating attacks on the applications, DAST is a technique for dynamic application security testing that is used to identify weaknesses in web-based applications. The goal of this type of approach is to find application errors by reviewing the application from the outside in. To do this, the developers will act like a malicious intruder and launch various attacks against the application to see if they can break the code or not. On this basis, the programmers can identify the application's and the code's weak points and use stronger, more complex algorithms that are difficult for an attacker to defeat. In this manner, the code that is created will be effective and offer adequate security for web-based applications. After the DAST scan is finished, the results will be compared to what was anticipated, and if there are any discrepancies, the vulnerabilities will be found and fixed. It is one of the black box testing techniques which is used to evaluate the application from attacker's view point without bothering about the source code or architecture of the application or software. Another advantage of DAST is to identify the configuration errors, etc and also find out the vulnerabilities against the SQL injection and cross scripting related errors.

Keywords: - description of DAST, DAST's mechanism of operation, DAST's implementation procedure, advantages, and drawbacks, DAST application use.

Introduction: -

SAST and DAST both are the application security testing techniques which are used to test the vulnerabilities of the application against the intruder and malicious attacks. SAST is performed on the source code of the software in initial stages of the development of the software whereas as DAST is performed from outside in to evaluate the software. SAST is white box testing technique which uses the source code to detect the errors before the actual compilation of the code. DAST is black box testing technique which is used to detect the vulnerabilities by performing simulation attacks from the tool itself. The process will perform malicious attacks from the tool and then will compare the output results with the defined set of output results. This means that if the application is giving results which are different from the expected output then there are points from where the intruder can attack and get access to the application. This way the developers will get chance to identify those spots and write more complex code which cannot be intruded by the attacker. A variety of DAST tools are available which can be selected based on the type of programming used for the software. Few DAST tools combines the features of API scanning, pen testing as well as fuzz testing to get efficient DAST scan results. The malicious attacked done by the tool are the automated attacks which are already there in the tool. The attacks performed by the DAST tools does not require any information about the source code or internal coding of the system as is with the case of SAST testing. DAST will only need to attack the application by mimicking attackers with minimum knowledge about the application and will evaluate the outputs and compare with the expected outputs and then resolve the issues.

Working Mechanism of DAST: - [1]

Following are the steps which explains the working mechanism of the DAST tool: -

- To start the DAST testing, first of all the tool will perform penetration testing on the application to identify the vulnerabilities of the software.

- It is different form the SAST technique which does not require running code for identifying the vulnerabilities but DAST tool requires the running code which is used to determine the weak points of the web application.

- Penetration testing means to test the software for security and make sure that it cannot be easily attacked by the intruder. This is done by attacking the software like attacker and exploit the weak points of the system to identify all the possible vulnerabilities and fix them.

- This can be done by giving some malicious data as input and then see the behaviour of the application which shows how it will respond to such attacks.
- All the HTTP and HTTPS requests will be tested by the DAST to see where it can be altered to gain access to the application.

- Running a SAST scan on the software application will identify the spots in the code which need to be fixed whereas DAST does not specifically identify the specific location in the code rather it will just explore the weak points from where the attacker can attack the system and exploit to their own interest.

- DAST instruments are generally utilized by security specialists who figure out the activity of the full application. They should know how the application functions. They additionally need to know about different assets that are utilized for building the entire application like the information base, application server, and web server.

Implementation process of DAST: - [2]
Like SAST, there are few points which should be kept in mind to implement the DAST tool in the environment. Following are the various implementation steps of the DAST. It can be executed manually as well as automated. The automation part used in DAST can be done by writing script or recording.

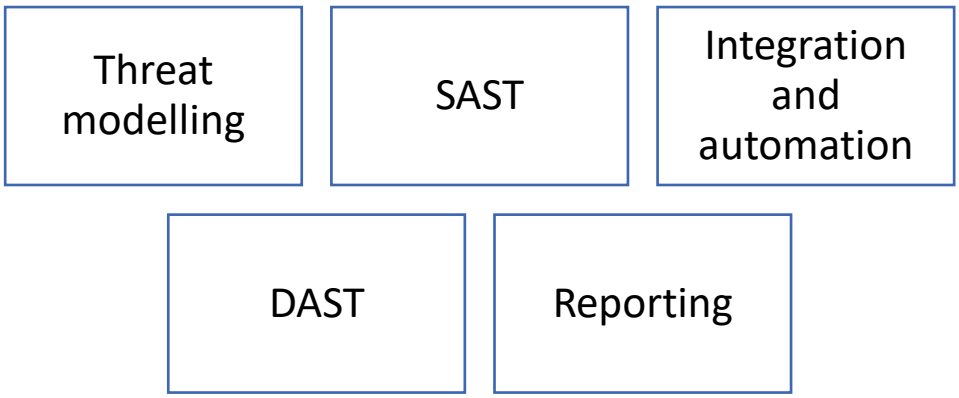

Figure 1. Implementation process of DAST.

1.Threat Modelling: -
> In this step, a threat model is developed based upon the interaction with the end user. The team will interact with the end user and try to understand that how the client will use the application.
> Everything will be recorded and will be used for developing a threats model.
> By doing so security experts will be able to identify the security attacks area and knows how to improve the complexity of those points so that they cannot be attacked easily.
> Other way to identify the vulnerabilities will be to perform functional application test which will show what are the issues and will provide ways to solve them.

2. SAST: -
> Once a threat model is made, first SAST scan will be done on the code to determine any loose ends. If so, then first they are fixed,
> It is to make sure that there is no issue with the code written to develop the software.
>If any security vulnerabilities are identified using this technique, then solutions to these are provided first before proceeding for the DAST test.

3. Integration and automation: -
> All the components are integrated and then the script will be written to test the application.
> Scripts written can be executed automatic and these are based upon the actions which a user will perform on the application.

International Journal of Science and Technological Research
ISSN: 2815-052X Volume: 2 Issue: 1
***Article Received**: 25 March 2022 **Revised**: 21 April 2022 **Accepted**: 14 May 2022 **Publication**: 30 June 2022*

4. Test scripts and CI/CD: -
> Once test scripts are written, then in this stage they are executed and results are evaluated to check for vulnerabilities.
> The test script will try to attack the application in all possible ways to detect all the points from where it can be attacked.
> Once these are identified then, the developers will identify the spots and will fix them by making the application strong by using complex and efficient algorithms which will protect the system to be attacked by the hacker.

5. Reporting: -
> The DAST scan must be carried out at regular intervals and it should also be made sure that the vulnerabilities detected should be reported properly as soon as they occur so that the developer can start the process of fixing or providing solutions for the issues.

Types of DAST process: -
The DAST process is of following two types: -

a. Manual application security testing: -
It is the manual process where the security testing based on proxy is used ot send requests manually to detect the response from the DAST scan.

b. Automated application security testing: -
This is the security testing where the testers will use the tool to automate the process of identifying the vulnerabilities of the application software.

Advantages of DAST: - [3]
Following are few advantages of DAST: -

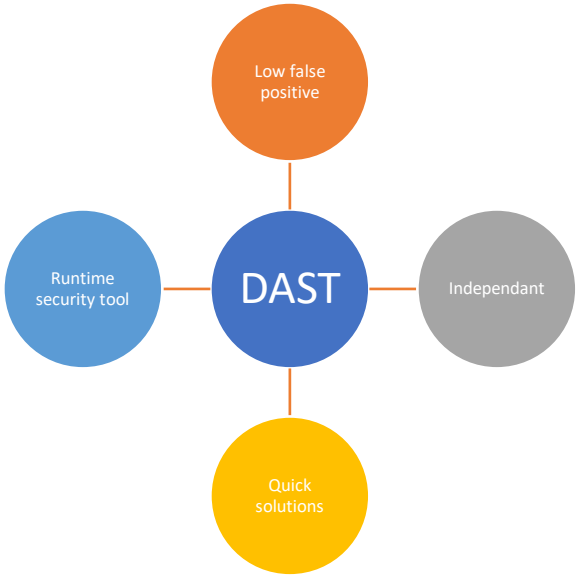

Figure 2 . Advantages of DAST.

1. Low false Positive: - DAST technique does not even test the whole software so it tends to give low false positives as compared to SAST. This in turn will help to provide quick solutions and also helps to validate if the alert is true or false.

2. Independent: - This tool is not dependant upon the type of programming language used or the type of technology used in the software. It will prove to be beneficial where there are number of programming language used.

3. Provides quick solutions: - It is one of the best tools which is used to identify the security vulnerability by performing regression testing. Once an issue is identified then it is recorded and also can be recreated to provide a solution for the issue so that it can be avoided in future.

4. Run time Security tool: - It is useful to detect the vulnerabilities which cannot be identified by other security testing techniques as it is used to perform simulation attack on the application and provides solutions to avoid the same.
5. Configuration related attacks: - It is also used to detect any configuration related faults which once identified can easily be rectified.

Disadvantages of DAST technique: - [5]
Besides various benefits, DAST also have some limitations which are explained below: -

1. Training of the tool: - DAST is carried out by security experts who knows how to automate the DAST testing using the too. If they do not have knowledge then everything will need to be performed manually which is a difficult task.

2. Shift right rule: - DAST tool is implemented towards the end of the development of the software or in production. The reason behind is that it will be time consuming and costly to wait for the complied version of code.

3. Cannot detect source code faults: - DAST is used only to detect the faults which are used upon the input given and output received. Therefore, it is not sufficient to detect the security vulnerabilities which lies inside the code.

Conclusion: - DAST is the unique application security testing procedure which is utilized to track down the weaknesses in thew electronic applications by performing reproduction assaults on the applications. The goal of this sort of approach is to distinguish the mistakes in the application by assessing the application from outside where implies the engineers will act like a pernicious gate crasher and will play out specific assaults on the application to check regardless of whether they can figure out the code. This way the engineers will actually want to figure out the flimsy part of the code and the application and afterward utilizes safer and complex calculations which won't be quickly broken by the interloper. This way the code composed will be proficient and will give sufficient security to the electronic applications. When the DAST examine is finished then the acquired outcomes will be contrasted and the normal arrangement of results and on the off chance that there are any distinctions, the weaknesses are recognized and fixed. It is one of the black box testing methods which is utilized to assess the application from assailant's view point without fretting over the source code or design of the application or programming. One more benefit of DAST is to recognize the arrangement mistakes, and so on and furthermore figure out the weaknesses against the SQL infusion and cross prearranging related blunders.

References: -

1.https://www.softwaretestinghelp.com/what-is-dast/
2.https://www.softwaretestinghelp.com/what-is-dast/
3.https://www.imperva.com/learn/application-security/sast-iast-dast/
4.https://www.parasoft.com/blog/dynamic-application-security-testing-dast-pros-and-cons/