Cheat sheet: Top 10 Application Security Acronyms

snyk

1. SAST

Static Application Security Testing, or SAST, refers to analyzing source code for potential flaws that could lead to security vulnerabilities. SAST tools identify various kinds of vulnerabilities based on patterns in the code, such as the use of known insecure methods and objects.

2. DAST

Dynamic Application Security Testing, or DAST, refers to analyzing an application for exploitable security vulnerabilities through its various interfaces. DAST tools typically identify vulnerabilities by looking for anomalies or patterns in responses received from the application based on specifically crafted requests (often referred to as payloads).

3. SCA

Software Composition Analysis, or SCA, is the practice of analyzing the various components used within an application for known vulnerabilities and license issues. SCA tools will analyze the dependencies of an application and compare it to a database of known vulnerabilities that exist in various versions of the packages.

4. OWASP

The Open Web Application Security Project, or OWASP, is a non-profit group focused on the security of software. OWASP is known for their many community-driven projects, such as the OWASP Top 10, that are aimed at providing education and guidance on how to produce more secure software.

5. XSS

Cross-Site Scripting, or XSS, is one of the most common forms of web application vulnerability. It can allow an attacker to execute malicious script code within a user's, or many users', browsers. There are three forms of XSS that are typically discussed:

- **Reflected:** The attacker causes the user to send a request to the application that contains the attack payload which the application reflects back to the browser.
- **Stored:** The attacker sends the attack payload to the application and it is stored in a value that is returned to other users in future requests.
- **DOM-Based:** The attacker sends the malicious script to the user (usually in a malicious link) and it is directly executed in the DOM of the page without going through the application at all.

6. CSRF

Cross-Site Request Forgery, or CSRF, is another form of web application attack. In a CSRF attack, the attacker is able to take advantage of an already authenticated session between the user's browser and the application to execute functionality of that application through requests that are embedded in a malicious website controlled by the attacker.

7. RASP

Run-time Application Self Protection, or RASP, refers to capabilities built into an application or service to detect and stop attacks. RASP tools usually embed themselves in the application and monitor incoming requests and the application's behavior to spot and prevent attacks.

8. DOS

Denial-of-Service, or DoS, is an attack that causes an application, service, or system to become unresponsive. DoS attacks happen when an attacker can exploit a flaw in the code, system software, or network infrastructure of an application to make it unavailable to others. There are two specific types of DoS that are often discussed:

- **DDoS:** Distributed Denial of Service, is when an attacker uses a large number of systems to overwhelm a target with traffic causing it to become unavailable.
- **REDoS:** Regular Expression Denial of Service is a specific flaw commonly found in server side JavaScript apps where an attacker can cause the regular expression engine to consume large amounts of resources rendering the application unresponsive.

9. CSP

Content Security Policy, or CSP, is a countermeasure meant to prevent XSS attacks. It allows application developers to use an HTTP Header to instruct the browser to only load and execute script from specific sources.

10. SSRF

Server Side Request Forgery, or SSRF, is a form of application attack in which an attacker can cause the front-end application to send requests to send requests to arbitrary locations (such as other internal servers, external servers, or even back to itself). It can allow the attacker access to unauthorized data or functions.

www.snyk.io