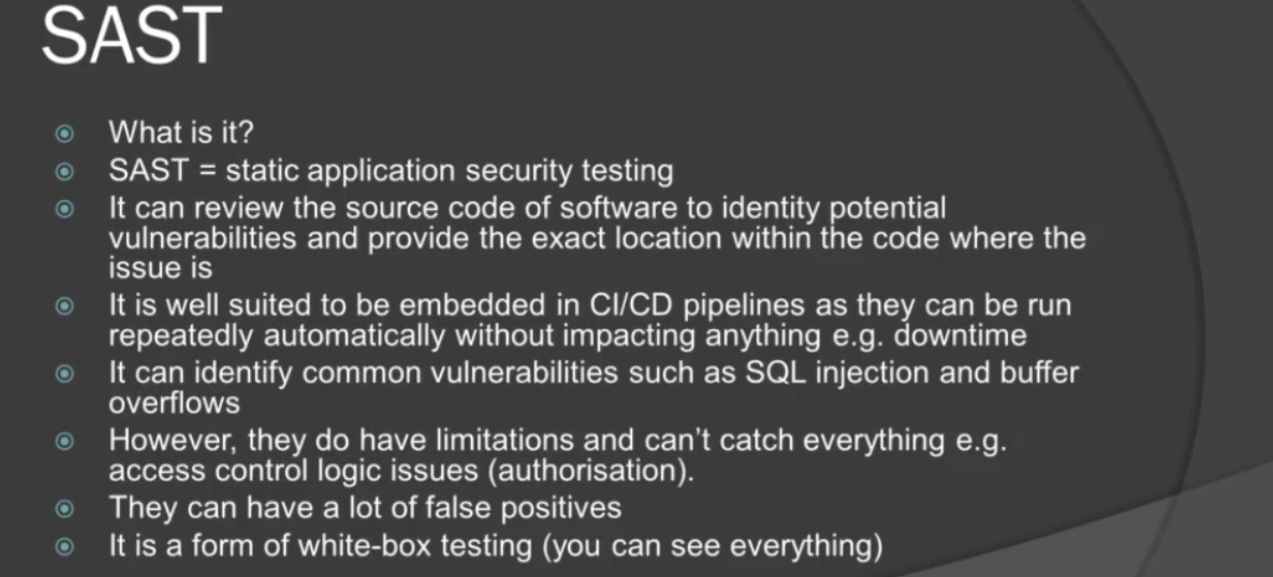
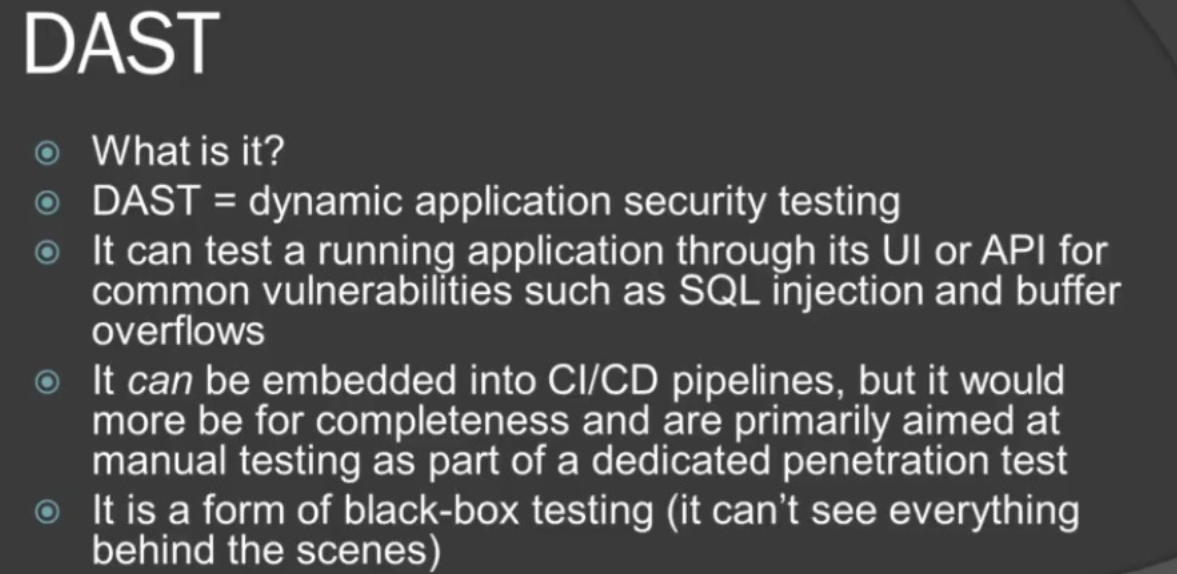
**Dependency in Code**

* Any application which developers code, they rely on open-source libraries or packages or frameworks for
  + web applications
  + Database connections and query executions (ORM Frameworks)
  + Logging
  + Authentication and Authorizations
  + Notifications.
* Scanning Dependencies for security risks is a mandatory operation as part of DevSecOps.
* If we need to scan dependencies from security issues, we need a database of possible vulnerabilities => CVE and NVD

**Static vs Dynamic Security Testing**

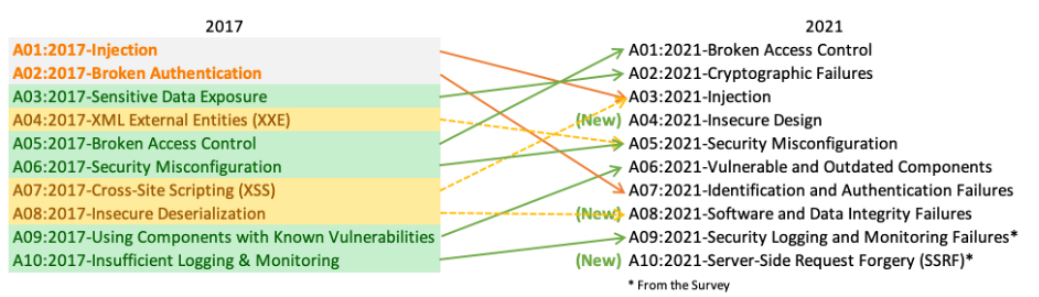
* Two possible ways to test for security
  + Static:
    - When the tool scans the application with the knowledge of code and reports vulnerability
    - This is called as SAST
  + Dynamic:
    - When the tool scans the application which is running and doesn’t have access to source code.
    - This is called as DAST

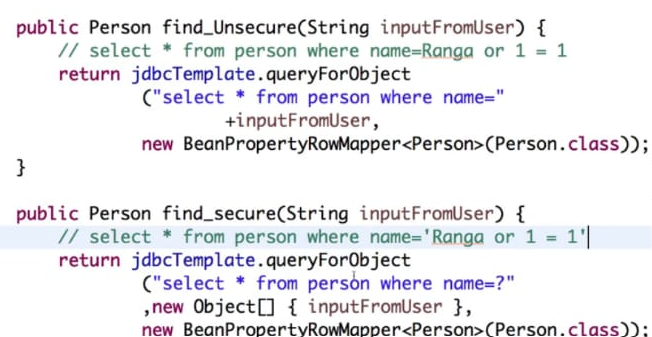




**OWASP (Open Web Application Security ProjectÂ® (OWASP))**

* This organization publishes top issues to be concerned with early.
* They also give necessary tools to scan
* <https://owasp.org/Top10/> for OWASP 10:2021
* As a DevSecOps Engineer, We will be
  + performing SAST during packaging/building the application
  + performing DAST post application deployment
  + Ensuring our application doesnot have any issues mentioned/listed in OWASP TOP 10 (latest year)





GDPR: The **General Data Protection Regulation** (**GDPR**) is a [European Union regulation](https://en.wikipedia.org/wiki/European_Union_regulation) on [data protection](https://en.wikipedia.org/wiki/Data_protection) and privacy in the EU and the [European Economic Area](https://en.wikipedia.org/wiki/European_Economic_Area) (EEA)

PCI-DSS: The Payment Card Industry [Data Security Standard](https://www.imperva.com/learn/data-security/information-security-infosec/) (PCI DSS) is a set of security standards formed in 2004 by Visa, MasterCard, Discover Financial Services, JCB International and American Express. Governed by the Payment Card Industry Security Standards Council (PCI SSC), the compliance scheme aims to secure credit and debit card transactions against data theft and fraud.

OWASP Organisation list down all the security attack happen for the year, categorized them, and provide guideline to develop software.