SECURITY TESTING TOOLS

Security testing tools are used to make sure that the data is saved and not accessible by any unauthorized user, to protect our application data from the threats, we will use the tools

These tools helps is find the flaws and security leakage of the system in the earlier stages and fix it and test whether the application has encoded security code and not accessible by unauthorized users

Testing tools

Sonar Qube:

looks at the code and find mistake and areas where you can improve

It can be integrated with multiple testing environments

Supports external tools such as gather, LDAP, Active Directory

It checks for bugs, vulnerabilities, code quality and issue helps you write better cleaner code

Zap (OWASP ZAP):

Zap as a security expert who test the website to find the weak spot that hacker might exploit, its scans your web application to identify security vulnerabilities and suggest way to fix them

It can be used as scanner

Its supports different operating system

Nets parker: nets parker is a detective that examine your security flaws, it automatically finds and reports vulnerabilities like broken links, insecure code or potential exploits

Scan modern web application like web 2.0, html etc.

We can generate custom reports with the help of templates

Arachnid: tools for finding security issue in website

Provide vulnerability exposure, test coverage and correctness of the web application

Its supports various platforms such as Linux, Mac so, Ms Windows

It will support different technologies like html 5, JavaScript etc.

Iron Wasp:

Find security issue in web application

Supporting recording login sequence

Guy based tools

Support false positive and negative detection