SECURITY TESTING

What is Security Testing?

Security testing is a testing technique to determine if an information system protects data and maintains functionality as intended. It also aims at verifying 6 basic principles as listed below:

- Confidentiality
- Integrity
- Authentication
- Authorization
- Availability
- Non-repudiation

Security Testing - Techniques:

- Injection
- Broken Authentication and Session Management
- Cross-Site Scripting *XSS*
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery *CSRF*
- Using Components with Known Vulnerabilities
- Unvalidated Redirects and Forwards

Open Source/Free Security Testing Tools:

Product	Vendor	URL
FxCop	Microsoft	https://www.owasp.org/index.php/FxCop
FindBugs	The University of Maryland	http://findbugs.sourceforge.net/
FlawFinder	GPL	http://www.dwheeler.com/flawfinder/
Ramp Ascend	GPL	http://www.deque.com

Commercial Security Testing Tools:

Product	Vendor	URL
Armorize CodeSecure	Armorize Technologies	http://www.armorize.com/index.php?link_id=codesecure

GrammaTech	GrammaTech	http://www.grammatech.com/
Appscan	IBM	http://www-03.ibm.com/software/products/en/appscan-source
Veracode	VERACODE	http://www.veracode.com

Loading [MathJax]/jax/output/HTML-CSS/jax.js