Automated- Web application scanning tools like those from [Watchfire](http://searchsoftwarequality.techtarget.com/news/1281638/AppScan-Web-application-security-scanner-enhanced) and[SPI Dynamics](http://www.spidynamics.com/) are good example of automated dynamic analysis tools. Automated tools are good for finding many common vulnerabilities such as [SQL injection](http://searchsoftwarequality.techtarget.com/definition/SQL-injection) and [cross-site scripting](http://searchsoftwarequality.techtarget.com/definition/cross-site-scripting) (XSS).

Manual-Manual testing of Web applications is typically performed using a Web browser and a Web proxy tool like [Paros](http://www.parosproxy.org/index.shtml) or OWASP's [WebScarab](http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project" \t "_blank).

 Dynamic analysis is performed against an actually running installation of an application, static analysis involves reviewing application assets like source code, configuration files and so on when they are static -- or at rest.

There are “Seven attributes of Security Testing” as follows, for more details check here:

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

**“URL manipulation”**

**“SQL injection”**

**XSS (Cross Site Scripting)**

**Spoofing”**

1. **Access to Application:**
2. **Password cracking:** If username or password is stored in cookies without encrypting, attacker can use different methods to steal the cookies and then information stored in the cookies like username and password.
3. **URL manipulation through HTTP GET methods:** when the application uses the HTTP GET method to pass information between the client and the server. The information is passed in parameters in the querystring. The tester can modify a parameter value in the querystring to check if the server accepts it. n such conditions any unusual behavior by application or web server is the doorway for the attacker to get into the application.
4. **SQL Injection:** Entering a single quote (‘) in any textbox should be rejected by the application. Instead, if the tester encounters a database error, it means that the user input is inserted in some query which is then executed by the application. In such a case, the application is vulnerable to SQL injection.

To check SQL injection entry points into your web application, find out code from your code base where direct MySQL queries are executed on database by accepting some user inputs.

1. **Cross Site Scripting (XSS):** Any HTML e.g. <HTML> or any script e.g. <SCRIPT> should not be accepted by the application. Attacker can use this method to execute malicious script or URL on victim’s browser. Using cross-site scripting, attacker can use scripts like JavaScript to steal user cookies and information stored in the cookies.
2. **Data Protection:** All the sensitive data must be encrypted to make it secure.  The tester should query the database for ‘passwords’ of user account, billing information of clients, other business critical and sensitive data and should verify that all such data is saved in encrypted form in the DB. tester should ensure that the encrypted data is properly decrypted at the destination. when the information is being transmitted between client and server, it is not displayed in the address bar of web browser in understandable format.
3. **Brute-Force Attack**: If, a specific number of consecutive attempts (mostly 3) fail to login successfully, then that account is blocked for some time (30 minutes to 24 hrs).
4. [**SQL Injection**](http://www.softwaretestinghelp.com/sql-injection-%E2%80%93-how-to-test-application-for-sql-injection-attacks/)**and XSS :**

For all input fields of the website, field lengths should be defined small enough to restrict input of any script. in such fields any html tags or script tag input must be prohibited.

1. **Service Access Points-- inter-network and intra-network access** to the application is from trusted applications. In order to verify that an open access point is secure enough, tester must try to access it from different machines having both trusted and untrusted IP addresses.