There are five attributes of Security Testing as follows:-

* Authentication- is the process of determining whether someone or something is, in fact, who or what it is declared to be.
* Authorization:- is the process of giving someone permission to do or have something.
* Confidentiality- involves a set of rules or a promise that limits access or places restrictions on certain types of information.
* Availability- Information must be kept available to authorized persons when they need it.
* Integrity- Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people.
* non-repudiation**-** A measure intended to prevent the later denial that an action happened, or a communication that took place etc.In communication terms this often involves the interchange of authentication information combined with some form of provable time stamp.

Security testing approach-

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:** The tester can modify a parameter value in the querystring to check if the server accepts it. In such conditions any unusual behavior by application or web server is the doorway for the attacker to get into the application.
4. **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.
5. **Cross Site Scripting (XSS):** Any HTML e.g. <HTML> or any script e.g. <SCRIPT> should not be accepted by the application. Using cross-site scripting, attacker can use scripts like JavaScript to steal user cookies and information stored in the cookies
6. **Data Protection:** All the sensitive data must be encrypted to make it secure. When the information is being transmitted between client and server, it is not displayed in the address bar of web browser in understandable format.
7. **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).
8. **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.

**Test scenerios-**

- Password should be at least 8 character long containing at least one number and one special character.  
-Username should not be like “admin” or “administrator”.

- Error messages should be generic and should not mention specific error details like “Invalid username” or “Invalid password”. Internal system details should not be revealed in any of the error or alert messages.

- All files must be scanned before uploading to server.

- Verify if reset password functionality is secure.

- Verify user session ends upon log off.

**-** Verify memory leak and buffer overflow.