Seven attributes of Security Testing

Security testing is to be carried out to make sure that whether the system prevents the unauthorized user to access the resource and data. In web applications & client server application the Security testing plays an important role. In the previous article we have learn about the Security Testing and in today's article we are concentrating on the "**Seven attributes of the security testing**".

Security Testing needs to cover the seven attributes of Security Testing: Authentication, Authorization, Confidentiality, Availability, Integrity, Non-repudiation and Resilience. So let's discuss one by one below:

1) Authentication:

Authentication is a process of identifying the person before accessing the system. It allows user to access the system information only if authentication check got passed. Apart from Username & password combination, the authentication can be implemented in different ways like asking secret question and answer, OTP (One Time Password) over SMS, biometric authentication, Token based authentication like RSA Secure ID token etc. It is also possible to use combinations of above options for authentication.

2) Authorization:

Once the Authentication passed the Authorization comes in the picture to limit the user as per the permission set for the user. The Authorization is generally implemented on Access control list, user role based, user group based and define the permissions & restrictions to specific user group or granting or revoking the privileges for the users.

3) Confidentiality:

Confidentiality is to be carried out to check if unauthorized user and less privileged users are not able to access the information. It is to check that the protection of information and resources from the users other than the authorized and authenticated. The confidentiality of information is carried out at all stages like processing, storage and displays the information. It is checked that the information stored in the database in the encrypted format & not stored in the plain format. Also check if while accessing the information by administrator or developer all information should be displayed in encrypted format or not.

4) Availability:

The availability of system is to check the system is available for authorized users whenever they want to use except for the maintenance window & upgrade for security patches. Downtime of the system should be minimum but the downtime can be due to natural disasters or hardware failure. Most of the time backup failover site is parallel running with main site. Once the main site down due to some reason then the all requests to main site are redirected to backup site. One more example of availability is the mirroring of the databases. In this concept there are two databases one is main primary database other is secondary (mirroring) database. Once the new record is added or updated or deleted from system then this action is taken in the main primary database, once any action is taken in this primary database then the updated data gets reflected on secondary database. In this way both Primary & secondary databases are mirrored to each other. Once the failure of Primary database is observed then the secondary database comes in the picture and reduces the downtime & increase the availability of the system.

5) Integrity:

Integrity is to make sure that the information received is not altered during the transit & check if correct information presented to user is as per the user groups, privileges & restrictions.

6) Non-repudiation:

Tracking who is accessing the systems and which of the requests were denied along with additional details like the Timestamp and the IP address from where the requests came from. Means confirmation sent by receiver to sender that the requested services or information was successfully received as Digital confirmation e.g. Digital Certificates, this not only serves as acknowledgement but also helps to validate both sender and receiver is genuine.

7) Resilience:

Resilience is to check the system is resistance to bear the attacks, this can be implemented using encryption, use OTP (One Time Password), two layer authentication or RSA key token.

Source:

http://www.softwaretestingclass.com/seven-attributes-of-security-testing/