Security Testing Fundamentals

Presented by Cygnet Infotech Pvt. Ltd.
Overview

• Security Testing is deemed successful when the following attributes of an application are intact
  • Authentication
  • Authorization
  • Availability
  • Confidentiality
  • Integrity
  • Non-Repudiation

Goal is to make sure that the system/application does not have any loopholes/system fallbacks
Authentication

• To confirm that something or someone is authentic – true to the claims.
• The digital identity of a user is validated and verified.

Is the person / package being truthful about their identity?
Authorization

• To ensure that a person/program is authorized to see the contents or make changes in an application.
• User/Access rights are used.

Is the package/person allowed to do this operation?
Availability

• To ensure that an application is up and running; its services and information available as and when needed.
• Number of failures are reduced and backups are kept ready.

Will this service do me good any time of the day?
Confidentiality

• To make sure that the information and services are available only when requested by and for intended users.

• Penetration testing is done and defects are fixed.

Is the service and information safe from unauthorized prying eyes?
Integrity

- To ensure that the service provides the user with correct information.
- It is also essential to make sure that no obsolete or outdated information is presented.

Does the service provide only the correct information to the user?
Non-repudiation

- To ensure that the message was sent and received by authentic users only.
- The sender/receiver must not be able to deny their involvement.

Did the communication happen between two legitimate users?
When to start Security Testing?

• In general, testing must start early to minimize defects and cost of quality.

• Security testing must start right from the Requirements Gathering phase to make sure that the quality of end-product is high.

• This is to ensure that any intentional/unintentional unforeseen action does not halt or delay the system.
SDLC and Security Testing

- Requirements Gathering
- Design
- Development/Unit Testing
- Integration Testing
- System Testing
- Deployment
- Support/Maintenance

- Security Requirements Study
- Develop Security Test Plan
- White box Security Testing
- Black box Security Testing
- Vulnerability Scanning
- Penetration Testing
- Post-production analysis
Security Testing Types

Vulnerability Scanning
• Scanning a system to find vulnerable signatures and loopholes.

Penetration Testing
• An attack from a hacker is simulated on the system.

Ethical Hacking
• The system is attacked from within to expose all the security flaws in the system.

Risk Assessment
• Observing the security risks in the system, classifying them as high, medium and low.

Security Scanning
• Network/system weakness are studied, analyzed and fixed.

Security Review
• To check that security standards have been implemented appropriately through gap analysis and code/design reviews.