SOFTWARE SECURITY

A.Divya
Department of Pharmaceutics, Ratnam Institute of Pharmacy, Nellore, India
Divyapharma15@gmail.com

INTRODUCTION

Security testing helps in securing application. It’s a complicated version of software testing. Software Testing mainly focuses on testing of software’s practicality. Functions enforced in package area unit analyzed to ensure whether software system produces calculable response. Software testing resembles system’s functional aspect. Security testing a lot of advanced than software testing because it considers security, a non-functional system’s property. It depicts system’s ability to form it secure. The system is made secure by implementing functions which prevent an unauthorized user to access system’s valuable and confidential information [1-5]. The developer must code security imposing functions to shield system by preventing it from being exploited. System will be secured if it is well functioned, even in presence of vulnerable code or activity which will exploit system, and does not have any effect on it [6-11].

Providing security to system is incredibly advanced as compared to easy software package testing method that involves recording machine and white box testing. For securing system, we want to ascertain system’s two important things: First, validity of enforced security measures that provide functionality and security to system [12-17]. Security measures conjointly include features like cryptography, robust authentication, and management measures. And second, system’s behavior when it gets attacked by attackers, leading to destruction by accessing secured and confidential guidance. Attackers will prohibit attacker’s exploitable activities for hacking system.

Security testing is incredibly important for software application because it takes care of confidential information. It ensures that confidential information does not get unnoticed by unauthorized entity. It works on the farside purposeful (i.e. black box) and implementation (i.e. white box) testing. Security tester might use several techniques to locate system’s vulnerabilities. Testing system’s security checks the loopholes or vulnerabilities in system which may cause failure of security functions of system ultimately resulting to great losses to organization [18]. Therefore, security testing is used to confirm that developed software is free from flaws and hence, the system is safe from unauthorized individual, be it an employee or an outsider.

Security testing identifies threats and calculates its result on system. The impact is analyzed by developers or testers. They place their efforts to interrupt the system or to urge into it to find bugs. So, security testing is extremely essential in IT sector for information protection. Security testing is said to risk primarily based testing approach that analyzes risk in each stage. Proper measures are taken to eliminate risk to create system secure. So, Testers should incorporate a risk-based testing approach by keeping system’s subject area reality and attacker’s mindset into thought for applying software security adequately [19-22]. During this approach, risk affected areas are known for testing. Developers/Tester need to develop check cases to reveal issues if any. The approach provides high level of software security as compared to black-box testing. Security testing deals with system’s security. It observes system’s behavior in presence of malicious attack. It tries to construct and execute test cases to create code work properly in attack part as well [23-28].

Software security is explained through varied perspectives, a user needs his system to figure and to way the developers ought to use their inventive minds towards making a secured software system.

REFERENCES


© JGRCS 2015, All Rights Reserved 3


