WHITE PAPER ON SECURITY TESTING

http://www.360logica.com
info@360logica.com

White Paper

Introduction

Owing to the ever changing business dynamics more and more organizations are shifting to the web. This shift is not just customer centric but internal as well. In terms of customer, be it business to business or business to customer everything is being nearly transacted via web. Even from internal infrastructure perspective companies are shifting to cloud, taking SaaS model etc to ease their operations and availability. In all this dynamics the security becomes an utmost factor to be considered. Looking at the delicacy of web security measures a firm is taking, independent testing firms came into the picture. This shift leaves firms vulnerable to unexpected security threats. It is also collective effort of the service providers, cloud service providers to ensure security and integrity of an enterprise is maintained.

Need of INDEPENDENT Testing Firms

The product or service in its inception is developed keeping in view the expected the results or criteria which it is intended to be put to use. The user is also expected to use the application in a particular fashion but the case is always not the same. Today with the advancement and availability of technology the end user is quite versatile and sometimes mischievous in a manner of speaking.

The breach in security of web-site or as a matter of fact any application/service can be intentional as well as non-intentional. As a provider of service/product we can pray for the user to use it in the desired manner but one has to be prepared for the unexpected use also. While taking security measures one has to think from intentional perspectives as well. A person who has written a code himself can be at loss in testing/verifying the code from the view point of finding “loop holes”. One has to think from intentional perspective or popularly ethical Hacker’s perspective.

The independent testing firms with expertise in niche skill domain can come in very handy in making a service or product robust. With the varied pool of talent and the right mix of approach the testing firms can provide the essential or fix the points where an application can be toyed with.

Software Testing in Various development methodologies

Waterfall model has been in quite usage from some time. Normally the flow in the model is as follows:

• System feasibility -> Requirement analysis -> System design -> Coding and unit testing. In this phase, the actual coding is done for the various modules. Generally the coder himself reviews the code and individually test the functionality of each module -> Integration and system testing. In this phase, integration of all the modules in the system is done and testing is done of the entire system, making sure that the modules meet the requirements. -> Deployment and maintenance. In this phase, the software is deployed in the production environment. One can rectify any errors that are identified in this phase, and tweak the functionality based on the updated requirements.

Manual vs Automated testing

Manual testing though very useful for checking the nuts and bolts of the code written but may lack in scanning the entire module on a comprehensive note.

Automated testing owing to its comprehensive nature is quite good in identifying the threats and when coupled with manual testing it can prove to be very beneficial.
A code may be tested by various techniques like SQL injection, code injection, remote code inclusion and cross-site scripting, an automated tool can come in handy to automate testing of these techniques but an experienced tester can prove more valuable who along with his “out of the box thinking” can test the application by subjecting it to unexpected attacks.

The best practices would facilitate tweaking the script of Automation tool (IBM Ad Scan, Peros, QA inspect etc) depending upon the technical requirement of the code to be tested and then taking the manual approach to rectify the end results. In this scenario the manual tester is preferred who has the expertise over the required domain.

Conclusion

With the advancement of more and more people shifting to web based applications, which definitely makes life and work easy one has to take care of threats which comes with the package.

Threats are not just for the consumer but for the enterprises as well. Common threats can be like Web-based attacks, Social phishing, Malicious data loss etc. One has to take care of prevention mechanism rather responsive mechanism.