

Modern Approach to Security Testing

White Paper - Version 1.0

Abstract

Security is one of the prime concerns for all applications. Often it is noticed that during testing of an application, security doesn't get due focus. This document presents an approach to handling different factors that affects application security.

Security Issues in an Application

The first issue in application security is to provide data privacy to the users. This means protecting information confidentiality from the prying eyes of unauthorized internal users and external hackers before allowing the access permissions to the users to ensure the legitimacy. The process of identifying users is called authentication. Establishing the user's identity is only half the battle. The Second issue is access control/ authorization which means attaching information to various data objects denoting who can and cannot access the object and in what manner (read, write, delete, change access control permissions, and so forth). The Third issue is for audit control which means maintaining a tamper proof record of all security related events to protect it against malicious modification and maintain its integrity. The issues discussed above make security testing of applications a challenging task.

Objectives in Application Security Testing

The two main objectives of application security testing are to:

- Verify and validate that the security requirements for the application are met.
- Identify the security vulnerabilities of the application under the given environment.

The traditional Use case approach in testing has proven quite useful in general requirements engineering, both for eliciting requirements and getting a better overview of the stated requirements. However security requirements essentially need to concentrate on what should not happen in the system and this cannot be captured by the traditional Use case approach.

Modern Approach to Security Testing

The security model of all applications has undergone many changes. The traditional model for securing an application from outside elements mainly relied on access control. This model was based on creating a hard perimeter wall around the system and providing a single access gateway that can be opened only for authenticated users. This security model had worked well with most of the simple applications. The gateway here refers to a firewall that classifies all users as "trusted" or "untrusted". In this simplistic model of security, every "trusted" user who is allowed to cross the gate, gains access to every portion of one's business and no further security checks are done. As the requirements for security increases, the applications need to implement a fine-grained security.

The modern security models divide the business domain into many regions and ensure different levels of security for each region. This means creating a security perimeter for each region. The first level of security check can not be very rigorous as one would want to let in prospective customers, vendors and service providers as quickly as possible. Most of the applications today have multiple security regions with different levels of security and these regions could be nested or overlapping with other regions within a same single application. While developing an approach for testing security of these kinds of applications, a proper strategy planning is very much essential, as there are many issues, which cannot be captured later on.

Types of Security Testing and Sections

The seven main types of security testing are:

- Vulnerability Scanning
- Penetration Testing
- Security Auditing
- Posture Assessment & Security Testing
- Security Scanning
- Risk Assessment
- Ethical Hacking

The Security testing sections are:

- Information Security
- Process Security
- Internet Technology Security
- Communications Security
- Physical Security

Conclusion

Security Testing can help organizations to control and reduce security vulnerabilities. In the end, all one requires is careful thought, planning and mapping out of tasks before one actually begins testing. This document demonstrates “due diligence” and compliance with industry regulations.

About STC

STC ThirdEye Technology (India) Pvt Ltd is India’s largest Independent software testing organization providing End-to-End testing Services. We build and operate dedicated India-based testing centers for our customers with the latest computing and data communication technologies, and deliver our services, with high standards of security and confidentiality. Consistent qualities of deliverables under compressed time schedules enable us to get repeat business. We help Fortune 500 ERP, BFSI, Healthcare, Gaming and Telecom solution providers We are ISO 9001:2000 certified organization. For more details, please visit us at www.stcthirdeye.com

Disclaimer

The Whitepaper series presents reports on subjects in the sphere of activities of STC ThirdEye Technology (India) Pvt Ltd that are to be considered in the interest of wider public. These papers are part of the ongoing studies and authors will be glad to receive your comments. The views expressed in these papers are to be regarded as those of the author and should not be interpreted as reflecting the views of the management of STC ThirdEye Technology (India) Pvt Ltd. STC ThirdEye Technology (India) Pvt Ltd assumes no responsibility for any actions taken by Anybody based on the information provided in this paper.