White **PAPER**

TEST TRIANGLE
Trusted Partner in IT Consulting

System Security Testing: Scanning your Vulnerabilities

This white paper is Test Triangle's attempt to shed light on various security testing methodologies. Based on the insight and experiences of the Test Triangle's testing team, this white paper offers detailed information about the IT security challenges and their testing approaches. This document will be beneficial for both small and large organizations in creating an exhaustive security system for their organization.

Introduction

Today, internet has opened countless new opportunities for business organizations, which cannot be accessed earlier. Internet is ubiquitous with no geographical boundaries; however, it has also opened possibilities for the malicious intent to exploit vulnerabilities. In cyberspace, several sensitive documents such as financial reports, employee salary, passwords, and trade secrets are duplicated, distributed and destroyed. According to Akamai (2018), the total number of web application attacks has increased by 69% in the year 2017.

These issues can be mitigated with the help of proper security approaches. The current status of the security system can be evaluated with the help of security testing. It protects the system or software application from unforeseen events. Unlike other testing methods, security testing requires working in a nebulous environment. There are infinite conditions, which are difficult to predict and constantly shifting, which makes security testing challenging than other types of testing. More than enough times, security testing is less conclusive[1].

Security testing is based on three elementary attributes, namely, confidentiality, integrity, and availability (CIA).

Confidentiality:

The security testing must examine whether an unauthorized or less privileged user is able to access the organization's private data. For this, the organization must store the information in an encrypted format.

1 https://techbeacon.com/security-testing-unlike-other-qa-what-your-team-needs-know?utm_source=newsletter&utm_medium=email&utm_campaign=tb_welcome

Integrity:

The system integrity means that the system information remains intact and correct information is presented to the users.

Availability:

The availability means that the system must be available every single time, an authorized user accesses it. The system downtime can attack due to cyber attack or other uncontrollable external events such as hardware failure or natural disasters.

Types of security threats

There are several types of security threats, which can exploit the system vulnerability

- **Cross-Site Scripting (XSS)**

  In cross-site scripting, the attackers inject malicious scripts in the web pages and trick users to click or move on to other web pages. This code can manipulate the website response or steal sensitive information from the organization.

- **Data Manipulation**

  In data manipulation, the hackers change the data published on the website to embarrass the publishers or gain some personal advantage

- **Identity Spoofing**

  In this method, the hackers use the credentials of a legitimate user to enter the system and steal sensitive system information.

- **SQL Injection**

  It is a common application layer attack in which the hackers enter malicious SQL statements. These statements can be used to obtain sensitive information from the web application or hack the entire system.

IT Security Testing Approaches

The IT security assurance is the process of identifying and managing security flaws so that the organizations can manage the existing security threats while competing for the industrial security standards. The IT security assurance is imperative for business organizations to prevent legal issues, establish customer trust and maintain the organization's reputation. In technical security assessment, the companies need to conduct the vulnerability assessment of different system components such as IT network infrastructure, mobility, and virtualized cloud database and security applications.

System security testing

The security testing is fundamental in identifying the network security issues, which an organization might expose to, in case of a cyber attack. The main phases of security testing are discussed below:

- **System Profiling:** In this phase, different scanning tools are used to identify the active sessions and live hosts on the system. There are several tools, used for system profiling.

- **Security Assessment:** At this stage, an automated assessment of system vulnerabilities is conducted. This audit is conducted for network services and information system. Manual intervention is used to eliminate the possibility of false positives. OWASP, WASC and SANS references are used to cover all the security vulnerabilities.

- **Vulnerability Exploitation:** In this stage, the information collected from the above phases is used to conduct controlled attacks on the system. These attacks are strictly conducted in accordance with the agreed terms of testers and the client organization.

- **Reporting:** In this phase, all the identified security vulnerabilities are documented and submitted to the client. The report also contains appropriate security measures and mitigation strategies.

- **Solution:** In this phase, appropriate remedies and enterprise-level solutions are provided for the vulnerabilities. After recommendations, a reassessment is conducted to validate the effectiveness of the IT control counter-measures in reporting the security vulnerabilities.

Security in SDLC

In the present times, it is important to introduce system security at the initial software development stage for building robust and secure applications. It can reduce time and cost associated with system security. The security measures embedded at every stage of software development will assure anomaly detection at an early stage.

Security configuration: At this stage, the security requirements are gathered and a gap analysis is conducted to identify the differences in security requirements and current security measures. With this phase, security is designed and implemented at the software development lifecycle.

Security configuration review: In the security configuration review, it is evaluated that the current security procedures are capable of handling security issues such as access control, unapproved applications, cryptography and other security settings for the network or system devices.
Threat modeling: In threat modeling, all the identified threats are analyzed so that the most hazardous threats can be identified. It covers all the possible scenarios and security threats and creates a roadmap for highest priority risks.

Security audit: In this phase, a code crawling activity is conducted to identify the post-deployment security threats. It includes issues regarding data flow, control flow, business logic flaws, security design flaws, and code level flaws.

Types of security testing

Network Infrastructure security testing

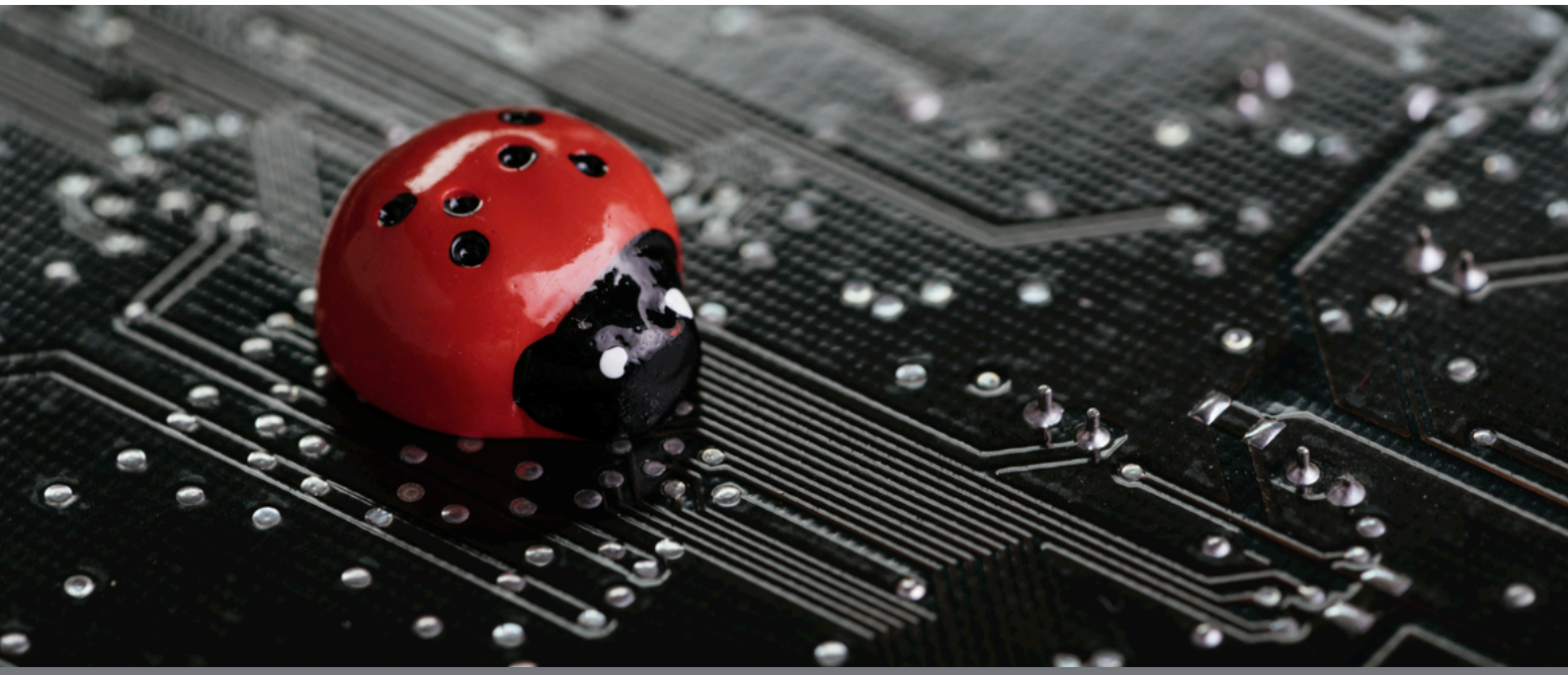
The network infrastructure security testing reveals a lot of information about system security such as source code, HTTP method, and authentication and system configurations. The network penetration test evaluates the security approaches and deployment method of the networking infrastructure. Even if appropriate security measures are taken, a small part of network configuration can be at the installation stage which can create a probability of external attack.

Following are the major phases in network infrastructure security implementation:

- Use of strong cipher algorithm
- Security measures for DB listener port, database servers, and authentication servers
- Security configuration of file handling extensions
- Configuring HTTP methods for eliminating system vulnerability

There are several tools, which can be used to identify the system vulnerabilities as follows:

Various scanning tools used for Vulnerability in the application configuration are W3AF, iScan, N-Stalker, WebInspect, Jsky, Acunetix. Scanning tools used for HTTP methods are Nessus, ZAP,skipfish, IBM appScan, Grendel Scan and Unreferenced files are W3AF, Paros Proxy, Wapiti, WEbInspect, Acunetix



Digital Authentication Security Testing

Authentication refers to process of validating or verifying the digital identity of the user. Testing user identity requires an understanding of the authentication process and identifying vulnerabilities, which can lead to bypassing the authentication procedure. Following procedure is used for system identification:

- Examining the data encryption, while it is traveling from web browser to the server
- Using brute force testing with the help of valid usernames
- Security examination of the user account retrieval process
- Using different penetration testing methods and tampering methods which can change the application
- Evaluating the "Remember password" and "Password Reset" options
- Testing the log out and cache functions of the webpage
- Evaluating the strength of different authentication systems such as passwords and OTPs (One time Password)

Various Scanning tools used for Bypassing security system WebScatab, WebGoat NTOSpider, IBM AppScan

Session and Cookies Management Security Testing

Session and cookies management testing is responsible for handling the user active sessions. The session time refers to the time duration in which the user remains active for a session. The session time is regulated for less-privileged users. In session management testing, the testers evaluate the session time and the amount of permission given to each user. In cookie testing, the test application examines whether the cookies are working properly.

The session and cookies management application have the following features:

- Evaluating the existing session management approach
- Security measures for the cookie system
- Scanning the system for Session Fixation and Cross-Site Request Forgery

The security scanning tools used in session identifier analysis are W3AF, Webscarab, NTO Spider, Burpsuite

User authorization Testing

The user access authorization refers to a process, which controls the user access for an application. Different users are granted different levels of user access. In this security testing, it is examined whether a user has the permission to access or invoke an action in the system.

The user authorization testing has the following features:

- Conducting path traversal attack and access confidential user information
- Examining the privileges given to a different set of users

Various Scanning tools used for privilege escalation are Webscarab, IBM AppScan, NTOSpider

Denial of Service Security Testing

The denial-of-service refers to an attack in which the users cannot access the machines or network resources. It makes the whole system or a part of the system not usable for legitimate users. This attack is based on the fundamental that every system has operational limits and if the system is overloaded, it will halt.

The Denial of Service (DoS) testing has the following features:

- Using wildcards to carry out CPU intensive queries
- Evaluating the system capacity by repeatedly entering the wrong password and trying to l ock the valid users out
- Using overflowing data structure technique to cause DoS attack
- Using different techniques to exhaust server resources
- Using large data in a user session object

Various Scanning tools for denial of service attack W3AF, WebSecurity, WebInspect

Data Validation Security testing

One of the most significant and common security issues is malicious data entry from external means. It leads to some common vulnerability such as XSS and SQL injection. The erroneous data can be mistakenly input into the system or maliciously entered by an external entity. Therefore, web applications must validate all the input data before it is processed. The data validation testing analyzes whether the digital application evaluates all type of data beforehand before processing it.

Various elements of data validation testing are:

- Implementing Reflected cross-site scripting in which offending URI is loaded on the site
- Implementing stored cross-site scripting which means that malicious code is entered on the webpage
- Testing for DOM-based Cross site scripting
- Injecting OS command with HTTP request

Some of the common tools used for code injection are Sandcat, Uber Web SEcurty Scanner and IBM AppScan. Tools used for DOM based Cross Site scripting are W3AF, Cenzic Hailstorm and NTO Spider.

About Test Triangle

Originally founded in 2012, Test Triangle has become a leader in IT consultancy services providing services in application testing, DevOps, RPA, Custom software development, mobile app development, Atlassian consultancy, niche IT staff augmentation and training in advanced technologies. Test Triangle is headquartered in Ireland; but it also has branch offices in London, United Kingdom, and Hyderabad, India. We have exponentially grown to become a team of 200+ members providing services in different verticals such as Banking & Finance, Utilities, Pharma, Retail, IT & Education etc.

Test Triangle's R&D department has created a propriety platform, Test Outsourcing Dashboard [TOD] which can be used to manage software testing lifecycle using collaboration tools like email, live chat, video conferencing. We have also launched a self- service testing platform (the premium version will be released as SaaS solution), which can provide a project overview and real-time updates of the software development lifecycle.

Over the years, we have established the reputation of being a 'trusted partner in IT consulting'. Test triangle is an agile software company, which constantly strives to exceed the expectations of its clients. We adopt the software testing and software application lifecycle to meet the customer's demand in an efficient and reliable manner. With a global workforce, we have proved ourselves in delivering tight-deadline projects.

We are proud to declare ourselves a client of Enterprise Ireland and European commission.

ENTERPRISE IRELAND
where innovation means business

European Commission

For inquiry please contact: inquiry@testtriangle.com

Ireland - HQ
Suite 12, Plaza 212 Blanchardstown Corporate Park,
Ballycoolen, Dublin, D15 W535

UK
4th floor, 86-90 Paul Street, London, EC2A 4NE

India
1-98/9/3, Plot No.3, Flat No.102, Jaihind Enclave,
Madhapur, Hyderabad 500 081

Sales Phone Number

ROI Hotline
+353 1 9685077

UK Hotline
+44 (0) 2071933020

India Hotline
+44 (0) 2071933020
+91 40 49510533

facebook.com/TestTriangle
linkedin.com/company/test-triangle
twitter.com/testtriangle
youtube.com/user/TestTriangle