Lancashire
Cyber Foundry

The Necessity of Security Testing

READ TIME: 2 MINS

AUDIENCE: BUSINESS & TECHNOLOGY

Security testing is an essential security measure and is counted as one of the best security practices applied to applications because of its focus on application security.

Security testing is an important step to be considered in the development process of business applications as it helps to:

- Identify and mitigate potential security risks that can threaten the integrity of the application and the data it stores.

- Ensure that the application is secure from malicious attacks and intrusions, as well as from internal misuse or abuse.

- Ensure compliance with industry regulations and laws, protecting the business from legal and financial repercussions

BACKGROUND

Security requirements play a vital role in the software development process to gain a secure application. The security levels of each application can be varied depending on multiple factors, such as information processing or storing in the application, business criticality of the application, or features and functions of the system.

However, the understanding of these factors has not been done early and has little or no involvement from the business users (end-users or system owners), who have the best understanding of how the system should be used in their business and the business impacts. As a result, the system design is done without awareness about these factors.

Most of the time, security concerns in an application are addressed late in the development lifecycle, which causes extra money, effort, and time from the development team. We must understand that it is extremely difficult to retrofit the security requirements after the application is developed. This is the main reason why system owners should insist on considering the security factors from the initial stage, i.e., the design phase.

European Union
European Regional Development Fund

NORTHERN POWERHOUSE HM Government

Lancaster University

TYPES OF SECURITY TESTING

Different types of security testing methods exist, and they each have their own strengths and weaknesses. Below are some of the most popular types of application security testing.

Application Security Testing:
Application security testing describes methods that the organizations can use to find and eliminate vulnerabilities in software applications. These methods involve testing, analysing, and reporting on the security posture of a software application throughout its development lifecycle.

Web Security Testing:
Web penetration testing aims to determine whether a web application is vulnerable to attack. It gathers information about a web application, finds system vulnerabilities or flaws, investigates the success of exploiting these flaws or vulnerabilities, and evaluate the risk of web application vulnerabilities.

API Security Testing:
API security testing helps to identify vulnerabilities and attack vectors in application programming interfaces (APIs) and web services. It assists developers in remediating those vulnerabilities. APIs provide access to sensitive data, and attackers can use them as an entry point to applications.

Penetration Testing:
Penetration testing is the process of stimulating real-life cyber-attacks against an application or network under safe conditions. Most importantly, penetration testing can find unknown vulnerabilities, including technical threats and business logic vulnerabilities.

CONCLUSION

In today's cybersecurity threat landscape, more and more companies are becoming victims of attackers or intruders, often struggling to survive in the industry after data breaches and theft. However, businesses that proactively follow security measures are less likely to suffer from cyberattacks.

Application security can help your organization build a strong security posture with secure applications. This includes evaluating your existing security methods, detecting vulnerabilities, and taking proactive measures to safeguard your application from potential threats. Investing in application security yields long-term benefits in the form of reduced cost and time to identify, mitigate, and prevent security issues.

ABOUT THE AUTHOR

Anju N K

Anju has worked as a Technical Business Analyst at Tata Consultancy Services (TCS) with a record of success, breaking down and improving Business Systems. Following the exposure to security compliance and implementation activities, she developed interest in exploring cybersecurity in depth and decided to pursue a Masters in Cybersecurity.