Cyber Security & Security Testing

SE3010

Software Engineering Process and Quality Management

Agenda

- What we covered Last Week…
- Security Testing
  - What is Security Testing?
  - Principles of Security Testing
  - Key Areas in Security Testing
  - Types of Security Testing
  - Methodologies/ Approach / Techniques for Security Testing
  - Security Testing along with SDLC
  - Example Test Scenarios for Security Testing
  - Security Testing Tool
  - Myths and Facts of Security Testing
  - Advantages of Security Testing
  - Disadvantages of Security Testing
  - Key Roles Associated with Security Testing
- Cyber Security
  - What is Cyber Security?
  - Types of Cyber Threats
  - What is the impact of a Cyberattack?
  - Common Cyber Threats
  - Malware
  - What are Cyber Security best practices?
- Recap
- Next Week…

What we covered Last Week…

- Cloud Computing
  - Cloud Computing Architecture
  - Types of Cloud Computing
  - Public Cloud Providers
  - Cloud Computing Service Models
  - On-Premise Vs IaaS Vs PaaS Vs SaaS
  - SaaS Tools
  - PaaS Examples in Cloud Computing
  - IaaS Services
  - Public Cloud Market Share
  - Key Benefits Cloud Offers
  - Biggest Challenges of Cloud Computing
- Cloud Testing
  - Types of Cloud Testing
  - Testing Performed within the Cloud
  - Benefits of Cloud Testing
  - Key Cloud Testing Challenges

What is Security Testing?

Security Testing

data and resource protect karanna system eke thyna weaknes hoyana eka thamai security testing kiynne.

- **Security Testing** is a type of Software Testing that uncovers vulnerabilities in the system and determines that the data and resources of the system are protected from possible intruders.

- It ensures that the software system and application are free from any threats or risks that can cause a loss.
- Security testing of any system is focused on finding all possible loopholes and weaknesses of the system that might result in the loss of information or repute of the organization.

Principles of Security Testing

- **Confidentiality**
  - Confidentiality is one of the cornerstones of information security. Confidentiality is the obligation of an organization or individual to keep the information confidential. Confidential information is any information that is not meant to be shared with third parties. The primary purpose of confidentiality is to protect the stakeholders' interests by preventing the unauthorized disclosure of information.
- **Integrity**
  - Integrity is one of the core security concepts. It is about system and data integrity. The need for integrity stems from the fact that we often want to ensure that a file or data record has not been modified or has not been modified by an unauthorized party. Integrity is a fundamental security concept and is often confused with the related concepts of confidentiality and non-repudiation.
- **Availability**
  - The definition of availability in information security is relatively straightforward. It's the ability to access your information when you need it. A data breach might cause downtime, productivity, loss of reputation, fines, regulatory action, and many other problems. For all of these reasons, it's crucial to have a data availability plan in case a data breach happens.

Principles of Security Testing (Contd…)

- **Authentication**
  - Authentication is the act of confirming or denying the truth of an attribute of a single piece of data claimed valid by an entity. Authentication can be perceived as a set of security procedures intended to verify the identity of an object or person.

- **Authorization**
  - Authorization is a security mechanism to determine access levels or user/client privileges related to system resources, including files, services, computer programs, data, and application features.

- **Non-repudiation** Accountability
  - In the context of information security, non-repudiation is the capability to prove the identity of a user or process that sent a particular message or performed a specific action. Proof of non-repudiation is a critical component of electronic commerce. It protects businesses from fraud and ensures that a company can trust a message or transaction from a specific user or computer system.

Key Areas in Security Testing

- **Network Security:** Data transfer between UI and API is ensured to be encrypted and secured.
- **System Software Security:** The entire application, UI, server, and database must be secured.
- **Client-side Application Security:** The data sent by the user to server under HTTPS must be secured.
- **Server-side Application Security:** The interaction between the database and receiving data from the database and the client has to be secured.

Areas in Security Testing (Contd…)

- **Authentication and Authorization:** Testing the system's ability to properly authenticate and authorize users and devices. This includes testing the strength and effectiveness of passwords, usernames, and other forms of authentication, as well as testing the system's access controls and permission mechanisms.
- **Network and Infrastructure Security:** Testing the security of the system's network and infrastructure, including firewalls, routers, and other network devices. This includes testing the system's ability to defend against common network attacks such as denial of service (DoS) and man-in-the-middle (MitM) attacks.
- **Database Security:** Testing the security of the system's databases, including testing for SQL injection, cross-site scripting, and other types of attacks.
- **Application Security:** Testing the security of the system's applications, including testing for cross-site scripting, injection attacks, and other types of vulnerabilities.
- **Data Security:** Testing the security of the system's data, including testing for data encryption, data integrity, and data leakage.
- **Compliance:** Testing the system's compliance with relevant security standards and regulations, such as HIPAA, PCI DSS, and SOC2.
- **Cloud Security:** Testing the security of cloud.

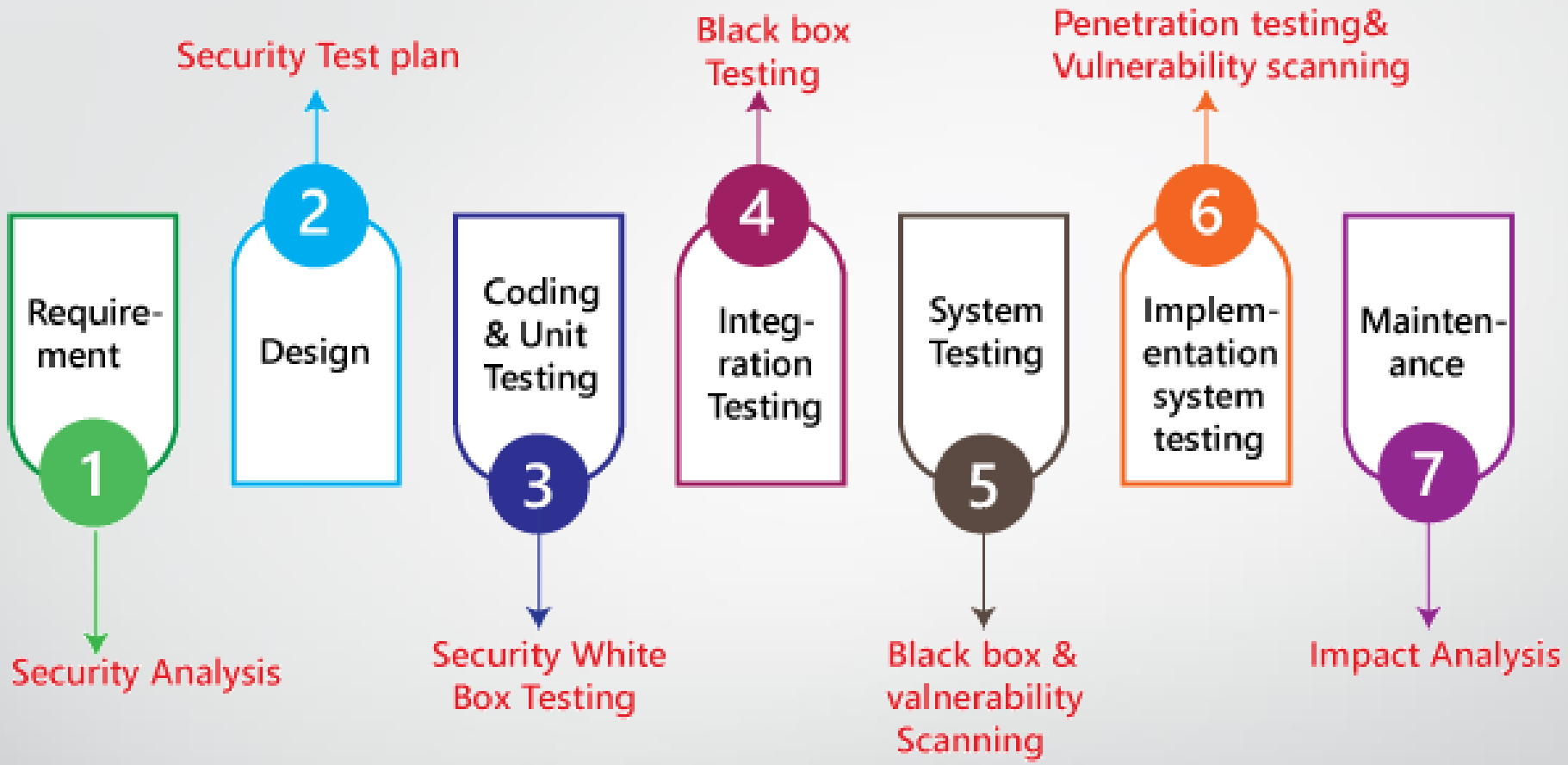
Types of Security Testing

- **Vulnerability Scanning** involves using automated software to examine a system and identify known patterns of vulnerabilities.
- **Security Scanning** involves identifying weaknesses in network and system security, followed by proposing solutions to mitigate these risks.
- **Security Auditing** is an internal inspection of applications and operating systems to identify security flaws. It may involve a line-by-line examination of code.
- **Penetration Testing** mimics a malicious hacker's attack on a specific system to uncover potential vulnerabilities. It involves analyzing the system for vulnerabilities while attempting to breach it.
- **Risk Assessment** involves analyzing security risks within an organization and categorizing them as low, medium, or high. This testing helps establish controls and measures to minimize these risks.
- **Network Security Testing** focuses on identifying vulnerabilities within the network infrastructure, such as firewalls, routers, and other network devices.
- **Ethical Hacking** differs from malicious hacking as its purpose is to expose security flaws in an organization's system.
- **Application Security Testing** focuses on identifying vulnerabilities within the application itself, including its code, configuration, and dependencies.
- **Social Engineering Testing** simulates social engineering attacks, such as phishing or baiting, to identify vulnerabilities in the system's human element.
- **Posture Assessment** combines security scanning, ethical hacking, and risk assessments to provide an overall evaluation of the system's security posture.
- Tools like ***Nessus, OpenVAS, and Metasploit*** can **automate** and **streamline** the security testing process.

Methodologies/ Approach / Techniques for Security Testing

- **Tiger Box Testing:** This hacking is usually done on a laptop that has a collection of OSs and hacking tools. This testing helps penetration and security testers conduct vulnerability assessments and attacks.
- **Black Box Testing:** Testers are authorized to perform testing on everything about the network topology and the technology.
- **Grey Box Testing:** Partial information about the system is given to the testers, and it is a hybrid of white and black box models.

Security Testing along with SDLC



- **Test Plan should include,**
  - Security-related test cases or scenarios
  - Test Data related to security testing
  - Test Tools required for security testing
  - Analysis of various tests outputs from different security tools

Example Test Scenarios for Security Testing

- Password stored must be encrypted in the database.
- Application or System should not allow invalid users.
- Penetration testing like SQL injection must be tested.
- Data transfer from UI to API must also be encrypted.
- Sessions and Cookies must be tested for security.
- For financial sites, the Browser back button should not work.

Security Testing Tool

- **Intruder:** Intruder is a penetration testing tool that is used in cloud resources and API integration with CI/CD resources. It tests the vulnerabilities of the system.
- **Teramind:** Teramind delivers a comprehensive suite for insider threat prevention and employee monitoring. It enhances security through behavior analytics and data loss prevention, ensuring compliance and optimizing business processes
- **Acunetix:** Acunetix is a web-only vulnerability testing software for websites that is integrable with GIT, Gitlab, Azure, and Jira.
- **Owasp:** The Open Web Application Security Project (OWASP) is a non-profit organization for security testing. The organization has multiple tools and documentation for various system security resources.
- **WireShark:** WireShark is a network protocol analyzer that checks for errors at the network level. It checks for packets, protocols, three-pane packet browsers, and VoIP analysis.
- **W3af:** W3af stands for web application attack and audit framework. This tool checks for SQL Injection in the code and vulnerabilities identified by plugins written in python, where one sends HTTP requests to find errors.

Myths and Facts of Security Testing

Myths	Facts
Security testing is needed where payment gateway integration is there.	Security testing is needed for system and network security
Security testing should be done in the end	Security testing is needed at every stage of product development
After Security testing application is 100% secure	There is never 100% security. The product is improved daily.
Security testing is needed only in large scaled products	Security Testing is needed from small to big products

Advantages of Security Testing

- **Identifying Vulnerabilities:** Security testing helps identify vulnerabilities in the system that could be exploited by attackers, such as weak passwords, unpatched software, and misconfigured systems.
- **Improving System Security:** Security testing helps improve the overall security of the system by identifying and fixing vulnerabilities and potential threats.
- **Ensuring Compliance:** Security testing helps ensure that the system meets relevant security standards and regulations, such as HIPAA, PCI DSS, and SOC2.
- **Reducing Risk:** By identifying and fixing vulnerabilities and potential threats before the system is deployed to production, security testing helps reduce the risk of a security incident occurring in a production environment.
- **Improving Incident Response:** Security testing helps organizations understand the potential risks and vulnerabilities that they face, enabling them to prepare for and respond to potential security incidents.

Disadvantages of Security Testing

- **Resource-Intensive:** Security testing can be resource-intensive, requiring significant hardware and software resources to simulate different types of attacks.
- **Complexity:** Security testing can be complex, requiring specialized knowledge and expertise to set up and execute effectively.
- **Limited Testing Scope:** Security testing may not be able to identify all types of vulnerabilities and threats.
- **False Positives and Negatives:** Security testing may produce false positives or false negatives, which can lead to confusion and wasted effort.
- **Time-Consuming:** Security testing can be time-consuming, especially if the system is large and complex.
- **Difficulty in Simulating Real-World Attacks:** It's difficult to simulate real-world attacks, and it's hard to predict how attackers will interact with the system.

Disadvantages of Security Testing

- **Resource-Intensive:** Security testing can be resource-intensive, requiring significant hardware and software resources to simulate different types of attacks.
- **Complexity:** Security testing can be complex, requiring specialized knowledge and expertise to set up and execute effectively.
- **Limited Testing Scope:** Security testing may not be able to identify all types of vulnerabilities and threats.
- **False Positives and Negatives:** Security testing may produce false positives or false negatives, which can lead to confusion and wasted effort.
- **Time-Consuming:** Security testing can be time-consuming, especially if the system is large and complex.
- **Difficulty in Simulating Real-World Attacks:** It's difficult to simulate real-world attacks, and it's hard to predict how attackers will interact with the system.

Key Roles Associated with Security Testing

- **Hackers –** Access computer system or network without authorization…
- **Crackers –** Break into the systems to steal or destroy data…
- **Ethical Hacker –** Performs most of the breaking activities but with permission from the owner…
- **Script Kiddies or Packet Monkeys –** Inexperienced Hackers with programming language skill…

What is Cyber Security?

Cyber Security

- **Cyber security** is the practice of protecting networks, applications, confidential or sensitive data, and users from cyber attacks.
- Cyber attacks are malicious attempts by individuals or groups to gain unauthorized access to computer systems, networks, and devices in order to steal information, disrupt operations, or launch larger attacks.
- It's also known as **Information Technology Security** or **Electronic Information Security.**

Types of Cyber Threats

- **The threats countered by cyber-security are three-fold:**

1. **Cybercrime** includes single actors or groups targeting systems for financial gain or to cause disruption.

2. **Cyber-attack** often involves politically motivated information gathering.

3. **Cyberterrorism** is intended to undermine electronic systems to cause panic or fear.

What is the impact of a Cyberattack?

- **The impact of a cyberattack can be far-reaching and devastating for businesses.** One of the most significant impacts is economic costs, as cyberattacks can result in the loss of revenue, increased expenses for remediation and recovery, and supply chain disruption.

- **Cyber attacks can also impact brand reputation.** When organizations suffer a data breach or a temporary outage, their brand image may be affected — resulting in poor media coverage and the potential loss of current and future customers to competitors.

- **Additionally,** cyberattacks can result in regulatory costs, as companies may face fines for failing to protect user data in accordance with data protection laws such as the GDPR or HIPAA.

Common Cyber Threats

- **Malware** is software designed to disrupt normal operations of a device, and can refer to a wide range of attacks like worms, Trojans, adware, or spyware.
- **Social Engineering** attacks manipulate victims into handing over sensitive information used for malicious purposes like fraud or account takeover.
- **Phishing** attacks trick victims into sharing usernames, passwords, card numbers, bank account information, or other sensitive data.
- **DDoS** attacks are malicious attempts to disrupt the flow of traffic to a server or network by overwhelming the targeted infrastructure with a flood of traffic, which renders them non-operational.
- **SQL (structured language query) Injection** is a type of cyber-attack used to take control of and steal data from a database.

Malware

Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer. D

Different types of malware,

- **Virus:** A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.
- **Trojans:** A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.
- **Spyware:** A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.
- **Ransomware:** Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.
- **Adware:** Advertising software which can be used to spread malware.
- **Botnets:** Networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.

What are Cyber Security best practices?

For Individuals:

- Use strong passwords,
- Do not reuse the same passwords for different websites or apps,
- Use multi-factor authentication or 2FA whenever possible,
- Avoid unsecure websites (many browsers will warn you if you are about to visit an unsecured website, or look for a padlock in the URL bar at the top to make sure the website uses TLS for encryption and authentication),
- Do not download or open unfamiliar files or links,
- Know the signs of a phishing email,

What are Cyber Security best practices?

For Business:

- Enforce the above for all of your users,
- Have visibility into all infrastructure used in your organization, including shadow IT,
- Use DDoS protection to remain online,
- Use firewalls and WAFs to protect internal networks and external-facing websites,
- Encrypt and back up data,
- Find a third-party risk management solution to implement a Zero Trust approach,

Next Week…

- AI / ML → Quality Management,
- Recap of all sessions [Summary…],
- Discussions related to the exam,

Thank You !!!

Tutorial – 05/05/2024

Q1: What is Security Testing?

Q2: Explain the 6 Principles of Security Testing…

Q3: What are the 4 Key Areas in Security Testing?

Q4: What are the types of Security Testing?

Q5: What are the methodologies of Security Testing?

Q6: Name few example Test Scenarios for Security Testing…

Q7: Name few Security Testing Tools…

Q8: What are the advantages of Security Testing?

Q9: Name key roles related to Security Testing…

Tutorial – 05/05/2024 [Answers - I]

Q1: What is Security Testing?

- **Security Testing** is a type of Software Testing that uncovers vulnerabilities in the system and determines that the data and resources of the system are protected from possible intruders.

Q2: Explain the 6 Principles of Security Testing

- Confidentiality / Integrity / Authentication / Authorization / Availability / Non-repudiation.

Q3: What are the 4 Key Areas in Security Testing?

- Network Security
- System Software Security
- Client-side Application Security
- Server-side Application Security

Tutorial – 05/05/2024 [Answers - II]

Q4: **What are the types of Security Testing?**

- ***Refer the slide…***

Q5: **What are the methodologies of Security Testing?**

- Tiger Box Testing
- Black Box Testing
- Grey Box Testing

Q6: **Name few example Test Scenarios for Security Testing…**

- Password stored must be encrypted in the database.
- Application or System should not allow invalid users.
- Penetration testing like SQL injection must be tested.
- Data transfer from UI to API must also be encrypted.
- Sessions and Cookies must be tested for security.
- For financial sites, the Browser back button should not work.

Tutorial – 05/05/2024 [Answers - III]

Q7: Name few Security Testing Tools…

- Intruder / Teramind / Acunetix / Owasp / WireShark / W3af

Q8: What are the advantages of Security Testing?

- Identifying Vulnerabilities
- Improving System Security
- Ensuring Compliance
- Reducing Risk
- Improving Incident Response

Q9: Name key roles related to Security Testing…

- Hackers
- Crackers
- Ethical Hacker
- Script Kiddies or Packet Monkeys

Guide / Help for Assignment II

- Assignment consists of 3 main parts,
  - Creating a business case as the entrepreneur [business owner],
  - Gathering the requirements as the QA Manager,
  - Creating the Test Plan as the QA Manager & Testing Lead,

Thank You Again!!!