



# **SECURITY TESTING**



# WHAT TO EXPECT



1 Definition

2 Objectives

3 Types

4 Process

5 Benefits

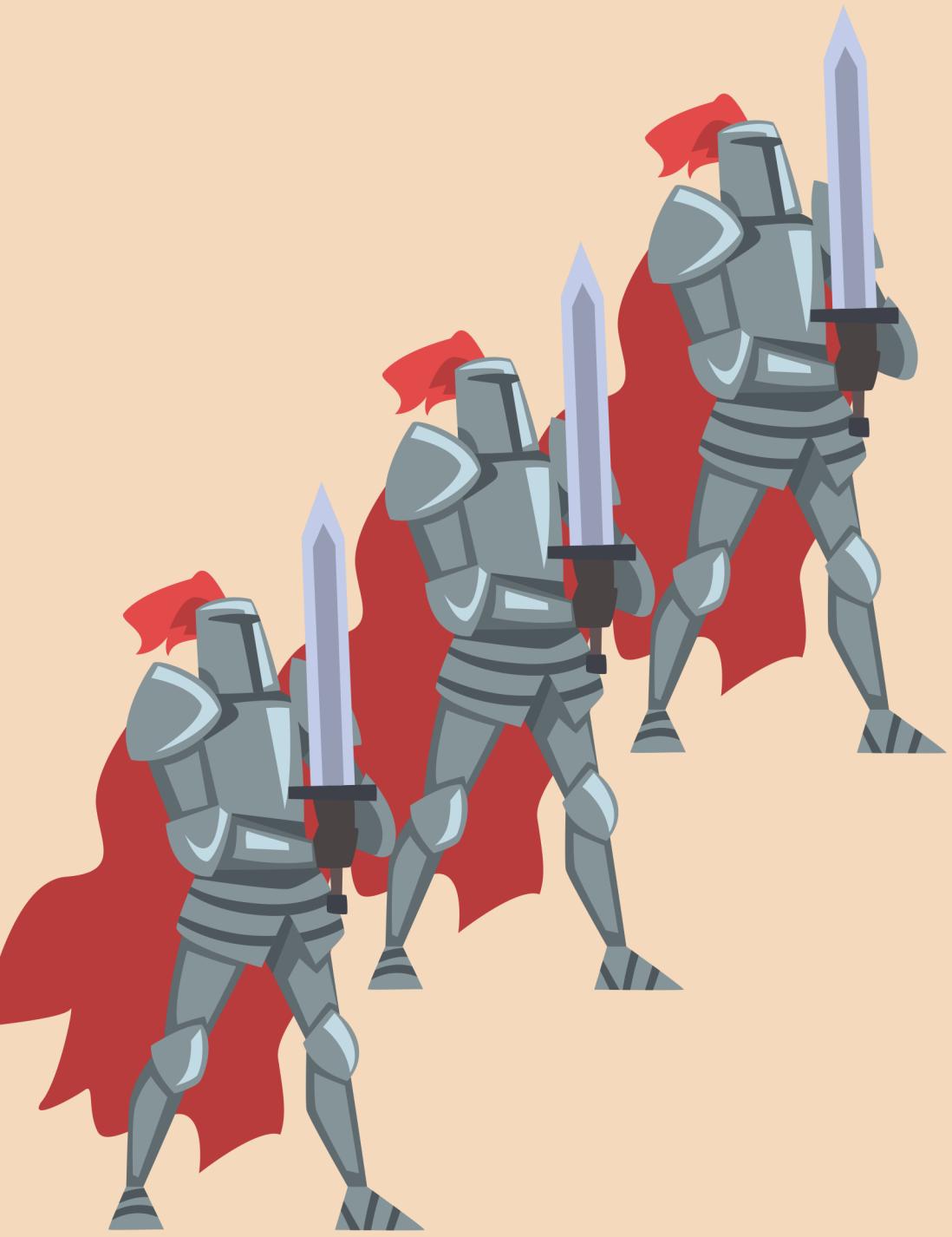
6 Techniques

7 Challenges

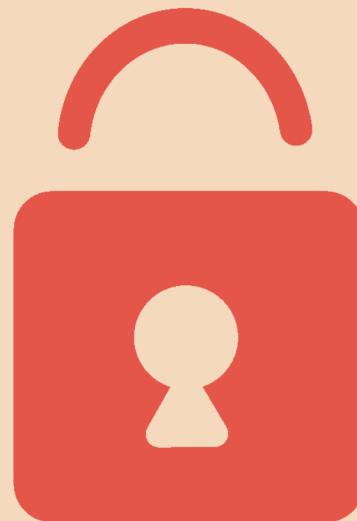
# Security Testing - Definition

Security testing is a critical software testing process that identifies vulnerabilities, weaknesses, and potential risks in a system to ensure the **confidentiality, integrity, and availability of sensitive information.**

It involves evaluating the effectiveness of security controls and measures implemented within an application or infrastructure.



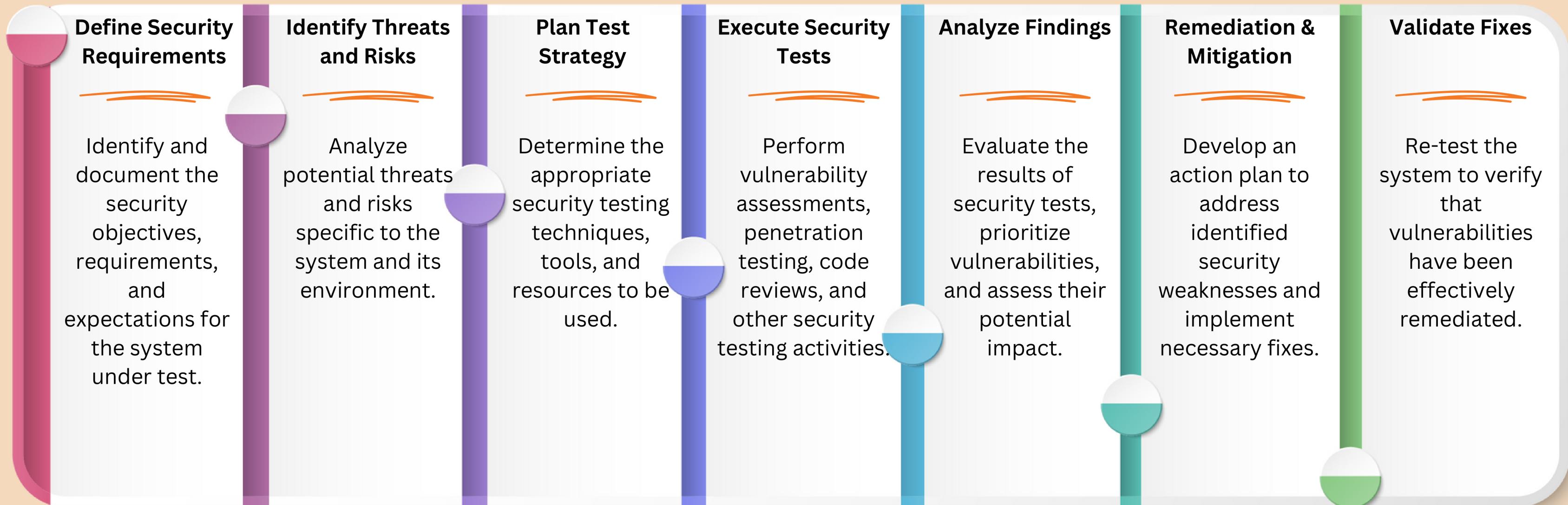
# Security Testing Objectives



# Security Testing Types



# Security Testing Process



**BENEFITS**

# of Security Testing



Proactive  
Risk  
Management

Protection  
of  
Sensitive  
Data

Regulatory  
Compliance

Safeguarding  
User  
Trust

Cost  
&  
Reputation  
Protection

# Common Security Testing Techniques

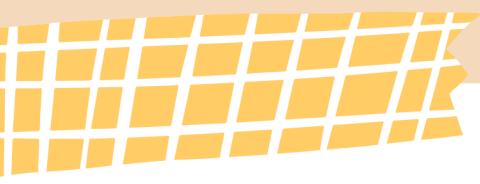
- **Authentication Testing:** Assess the strength and effectiveness of authentication mechanisms, such as username/password, multi-factor authentication, or biometrics.
- **Authorization Testing:** Verify that proper access controls are in place, ensuring that users can only access authorized resources and perform permitted actions.
- **Encryption Testing:** Validate the encryption algorithms, key management, and data transmission security to protect sensitive information.
- **Security Logging and Monitoring:** Evaluate the effectiveness of security event logging and monitoring systems for detecting and responding to potential security incidents.
- **Session Management Testing:** Test the mechanisms for managing user sessions, including session timeouts, session fixation, and session hijacking prevention.

# Challenges in Security Testing

- Evolving Threat Landscape: Security testing must adapt to rapidly evolving security threats and attack techniques.
- Application Complexity: Complex

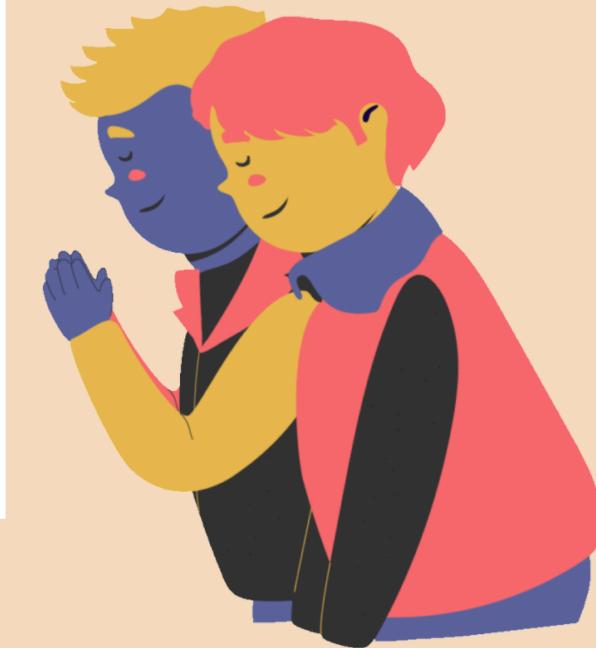
DOS  
ATTACK

BRUTEFORCE



“

**See you in Next Video**



# Xtras

# Security Testing Objectives

- Identify Vulnerabilities: Discover potential security flaws, weaknesses, and vulnerabilities that could be exploited by attackers.
- Assess Security Controls: Evaluate the effectiveness of implemented security controls, such as authentication, authorization, encryption, and intrusion detection systems.
- Test Data Protection: Verify the secure handling and storage of sensitive user data, ensuring confidentiality and privacy.
- Detect Threats and Risks: Identify potential security threats and risks that could compromise the system's security posture.
- Ensure Compliance: Validate adherence to security standards, regulations, and best practices relevant to the application or industry.

# Types of Security Testing

- Vulnerability Assessment: Systematically identify and classify vulnerabilities, focusing on weaknesses in the network, infrastructure, and applications.
- Penetration Testing: Simulate real-world attacks to uncover vulnerabilities and assess the ability of the system to withstand intrusion attempts.
- Security Code Review: Analyze application source code for potential security weaknesses, such as insecure coding practices or vulnerabilities.
- Security Configuration Review: Evaluate the security configuration settings of servers, databases, firewalls, and other components to ensure optimal security.
- Security Scanning: Automated scanning tools are used to identify potential security issues, such as open ports, misconfigurations, or outdated software.

# Security Testing Process

1. Define Security Requirements: Identify and document the security objectives, requirements, and expectations for the system under test.
2. Identify Threats and Risks: Analyze potential threats and risks specific to the system and its environment.
3. Plan Test Strategy: Determine the appropriate security testing techniques, tools, and resources to be used.
4. Execute Security Tests: Perform vulnerability assessments, penetration testing, code reviews, and other security testing activities.
5. Analyze Findings: Evaluate the results of security tests, prioritize vulnerabilities, and assess their potential impact.
6. Remediation and Mitigation: Develop an action plan to address identified security weaknesses and implement necessary fixes.
7. Validate Fixes: Re-test the system to verify that vulnerabilities have been effectively remediated.

# Benefits of Security Testing

1. Proactive Risk Management: Security testing helps identify vulnerabilities and potential risks before they can be exploited, enabling proactive risk mitigation.
2. Protection of Sensitive Data: By verifying data protection measures, security testing ensures the confidentiality and integrity of sensitive information.
3. Regulatory Compliance: Security testing assists in meeting regulatory requirements and industry-specific security standards.
4. Safeguarding User Trust: Effective security testing enhances user confidence in the application, protecting their personal information and privacy.
5. Cost and Reputation Protection: Preventing security breaches through testing minimizes financial losses, legal liabilities, and reputational damage.