# Becoming a Pro

## IN Mobile Applications Testing

# Mobile Test Industry Standards :

## Testing Strategies for Mobile Apps

### Security Test EXTRA

## Mobile Device Risks at Every Layer

- NETWORK
- HARDWARE
- OS
- APPLICATION

Example :

Your device isn't rooted but all your email and pictures are stolen, your location is tracked, and your phone bill is much higher than usual.

# Mobile Test Industry Standards :

## Testing Strategies for Mobile Apps


### Security Test EXTRA

## What is OWASP ?

- The Open Web Application Security project is an online community which creates freely-available articles, methodologies, documentation, tools, and technologies in the field of Web App Security

## OWASP Top Ten:

- The Top Ten was first published in 2003 and is regularly updated.
- Its goal is to raise awareness about application security by identifying some of the most critical risks facing organizations.
- The Top 10 project is referenced by many standards, books, tools, and organizations, including MITRE, PCI DSS, Defense Information Systems Agency, FTC, and many more.

CWE – COMMON WEAKNESS ENUMERATION :
https://cwe.mitre.org/about/

# Mobile Test Industry Standards :

## Testing Strategies for Mobile Apps

### Security Test EXTRA- OWASP TOP TEN

**There are two main categories of mobile code security risks:**

**MALICIOUS FUNCTIONALITY**

- The category of malicious functionality is a list of unwanted and dangerous mobile code behaviors that are stealthily placed in a Trojan app that the user is tricked into installing.
- Users think they are installing a game or utility and instead get hidden spyware, phishing UI or unauthorized premium dialing.

**VULNERABILITIES.**

- The category of Mobily Security vulnerabilities are errors in design or implementation that expose the mobile device data to interception and retrieval by attackers.
- Mobile code security vulnerabilities can also expose the mobile device or the cloud applications used from the device to unauthorized access.

# Mobile Test Industry Standards :

## Testing Strategies for Mobile Apps

### Security Test EXTRA- OWASP TOP TEN 2017

- A1-Injection
- A2-Broken Authentication and Session Management
- A3-Cross-Site Scripting (XSS)
- A4-Broken Access Control
- A5-Security Misconfiguration
- A6-Sensitive Data Exposure
- A7-Insufficient Attack Protection
- A8-Cross-Site Request Forgery (CSRF)
- A9-Using Components with Known Vulnerabilities
- A10-Underprotected APIs

# Mobile Test Industry Standards :

## Testing Strategies for Mobile Apps

### Security Test EXTRA- OWASP TOP TEN

## A1-Injection

Injection flaws, such as SQL, OS, XXE, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query.

**Example:**

- The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

# Mobile Test Industry Standards :

## Testing Strategies for Mobile Apps

### Security Test EXTRA- OWASP TOP TEN

### 2. A2-Broken Authentication and Session Management

Application functions related to authentication and session management are often implemented incorrectly,

Attackers can compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities (temporarily or permanently).

# Mobile Test Industry Standards :

## Testing Strategies for Mobile Apps

### Security Test EXTRA- OWASP TOP TEN

### 3. A3-Cross-Site Scripting (XSS)

XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user supplied data using a browser API that can create JavaScript

**Example:**

XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

# Mobile Test Industry Standards :

## Testing Strategies for Mobile Apps

### Security Test EXTRA- OWASP TOP TEN

## 4. A4-Broken Access Control

Restrictions on what authenticated users are allowed to do are not properly enforced

Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

# Mobile Test Industry Standards :

## Testing Strategies for Mobile Apps

### Security Test EXTRA- OWASP TOP TEN

## A5-Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, platform, etc.

Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

# Mobile Test Industry Standards :

## Testing Strategies for Mobile Apps

### Security Test EXTRA- OWASP TOP TEN

## 6. A6-Sensitive Data Exposure

Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

# Mobile Test Industry Standards :

## Testing Strategies for Mobile Apps

### Security Test EXTRA- OWASP TOP TEN

## 7. A7-Insufficient Attack Protection

The majority of applications and APIs lack the basic ability to detect, prevent, and respond to both manual and automated attacks.

Attack protection goes far beyond basic input validation and involves automatically detecting, logging, responding, and even blocking exploit attempts

Application owners also need to be able to deploy patches quickly to protect against attacks.

# Mobile Test Industry Standards :

## Testing Strategies for Mobile Apps

### Security Test EXTRA- OWASP TOP TEN

## 8. A8-Cross-Site Request Forgery (CSRF)

A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application.

Such an attack allows the attacker to force a victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

# Mobile Test Industry Standards :

## Testing Strategies for Mobile Apps

### Security Test EXTRA- OWASP TOP TEN

### 9. A9-Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover.

Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts

# Mobile Test Industry Standards :

## Testing Strategies for Mobile Apps

### Security Test EXTRA- OWASP TOP TEN

## 10. A10-Underprotected APIs

Modern applications often involve rich client applications and APIs, such as JavaScript in the browser and mobile apps, that connect to an API of some kind (SOAP/XML, REST/JSON, RPC, GWT, etc.).

These APIs are often unprotected and contain numerous vulnerabilities.

# Mobile Test Industry Standards :

## Testing Strategies for Mobile Apps

## Security Test

### 2016 OWASP Release Candidate (not yet official)

- M1 - Improper Platform Usage
- M2 - Insecure Data Storage
- M3 - Insecure Communication
- M4 - Insecure Authentication
- M5 - Insufficient Cryptography
- M6 - Insecure Authorization
- M7 - Client Code Quality
- M8 - Code Tampering
- M9 - Reverse Engineering
- M10 - Extraneous Functionality

# Mobile Test Industry Standards :

## Testing Strategies for Mobile Apps

## Security Test

## CREATE CHECK LIST BEFORE

- Phone identifiers such as (IMSI or IMEI)
- Address Book
- Account Details
- E-maiL
- Stock application data
- Banking Data
- GPS Location(s)
- Web History
- User's Dictionary
- Images
- Notes
- Calendar Appointments
- Call Logs
- Encryption Keys

# Mobile Test Industry Standards :

## Testing Strategies for Mobile Apps EXTRA

## SUMMARY

### Functional
- Validation of Functionality
- Smoke / Regressions Testing
- Offline access testing
- Negative Testing

### Non Functional
- Network Strength / Outage / Recovery
- Different NW Types
- Peripheral Testing

### Interoperability (IOP)
- Voice / SMS interrupts
- Notifications
- Battery /Cable Removal

### Memory Leak
- Memory Usage
- Memory Leaks
- Garbage Collection

### Performance Testing
- CPU Usage testing
- Network Usage
- Page Render time or activity Render time

### Usability Testing
- User Experience
- Competitive Analysis
- Expert Review

### Installation Testing
- New App Install
- Uninstall and **Reinstall**
- Upgrade testing

### Security Testing
- OWASP Vulnerabilities
- Dynamic Testing
- Static Code Analysis
- Data Encryption

### Language Testing
- Validation for Locales
- Images and Text
- Currencies, time zones etc.
- Context

# Mobile Test Industry Standards

## Testing Strategies for Mobile Apps : LETS PRACTICE

# Mobile Test Industry Standards

## Testing Strategies for Mobile Apps : LETS PRACTICE

## How to Start Testing a Mobile Page

Find and divide page into components/modules

Create a list/table of modules/testing types/ testing

Create a variety of variables and conditions within each module

Specify the Expected and leave place for Actual Results

FOR TROUBLESHOUTING Create a list/table to view ANY problem from different angels

Create a Check List for Testing Categories:

Functionality Testing

Usability testing

Interruption testing

Connectivity testing

Compatibility testing

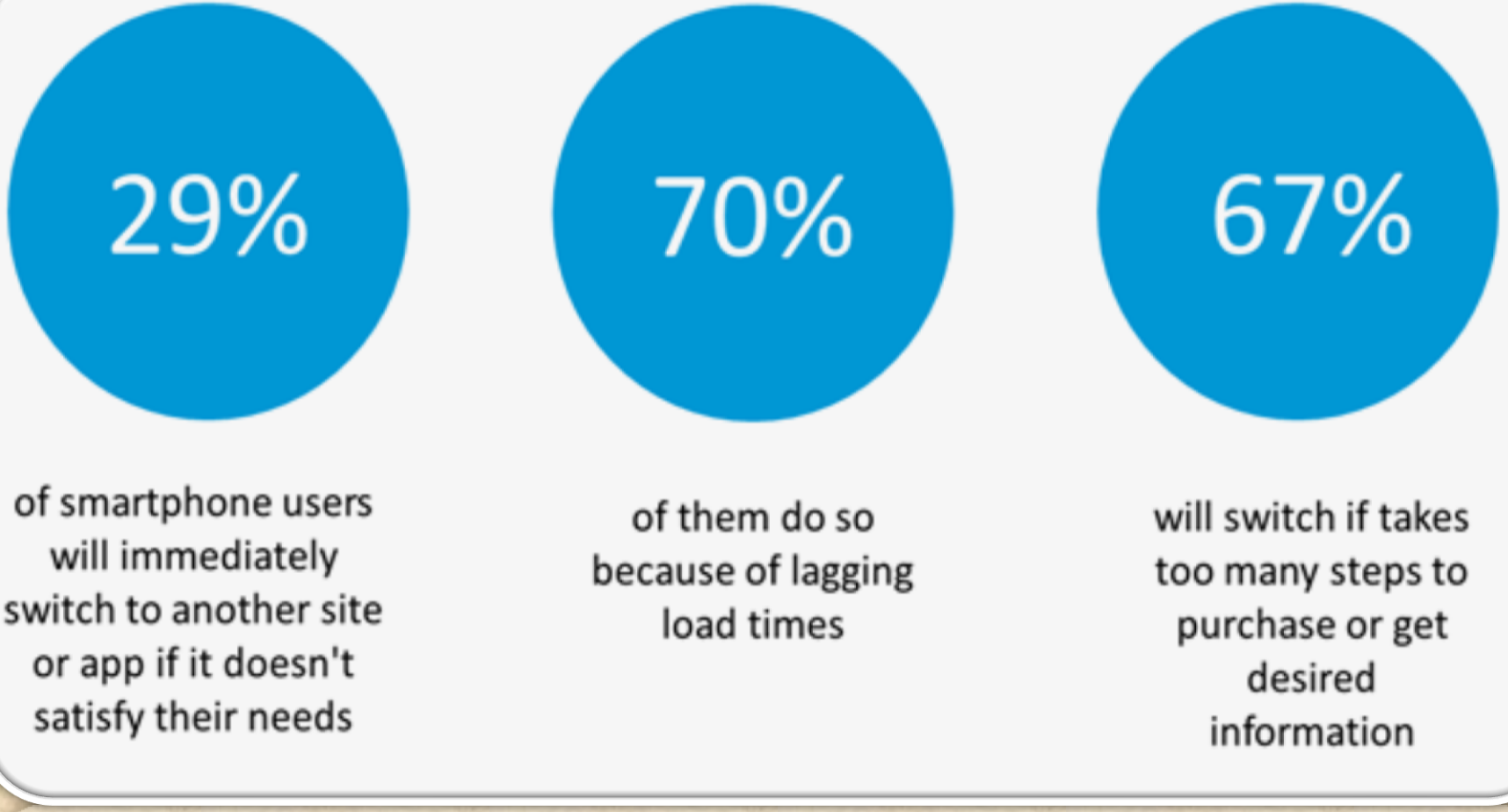
Performance testing

Security testing

# Mobile Test Industry Standards

## Testing Strategies for Mobile Apps : LETS PRACTICE

**Consumers behaviour only on the basis of experience delivered by app**



# Mobile Test Industry Standards :

## Testing Strategies for Mobile Apps

## GUI TEST Checklist

- Navigation
- Formatting
- Color and fonts
- Scrolls
- Controls and alignments
- Spelling and grammar
- Justification
- Look and feel
- Default and shortcut keys
- Tab
- Opening input
- Alternatives
- Behavior
- Modality and multiple windows
- Contrast
- Images

# Mobile Test Industry Standards

## Testing Strategies for Mobile Apps : LETS PRACTICE

**top considerations for creating a release CHECK LIST for mobile app testing**

- Application Installation/Update
- Application Sign Up & Log in
- Subscription scenarios
- Application Sanity Suit
- APP works in different Mobile modes
- User Friendly
- Network connectivity
- Data save conditions
- Mobile interruptions
- Battery Consumption
- Mobile memory utilization
- Mobile data utilization
- Screen scrolling application screen
- New OS release support
- correct implementation of AdMob or other mobile ad platform