CSW Cyber SecurityWorks

Mobile Application Penetration Testing

Introduction

CSW acts as a service company to conduct security posture assessments in various topics. A comprehensive security assessment has been performed on given target of the organization, mainly focussing on identifying the gaps and provide corrective action to mitigate the exposed risks.

Mobile application penetration testing is a form of security testing used to analyse security from inside of a mobile environment. The testing standards are built on OWASP top 10 and SANS 25 mobile application security verification standard. The mobile application penetration testing methodology concentrates on client-side safety, file system, hardware and network security.

The objective of our mobile assessments is to identify vulnerabilities/weaknesses in the given application. But our tests also focus more on critical issues which can create more business impact, tamper or loss of customer data.

Our Approach

Though there is a number of techniques and methodologies currently followed in industry. CSW finds its own way in addressing the security flaws and guiding the customers in the right direction to protect their data and enhancing their security posture.

CSW adheres to a **5 STEP** process as given below which ensures efficiency, reliability, integrity and gains the contented confidence of the customer,

- Gaining more clarity on the given scope.
- Analyse the workflow of the given application.
- Relating the scope with the given privileges after understanding the business logic of the application.
- Mapping and listing out all possible threats, vulnerabilities, flaws and attack areas.
- Perform manual and automated testing inside the given scope

Target Reconnaissance
Understand the mobile application being assessed. Gathering intelligence about the application is the most significant step in a penetration test.

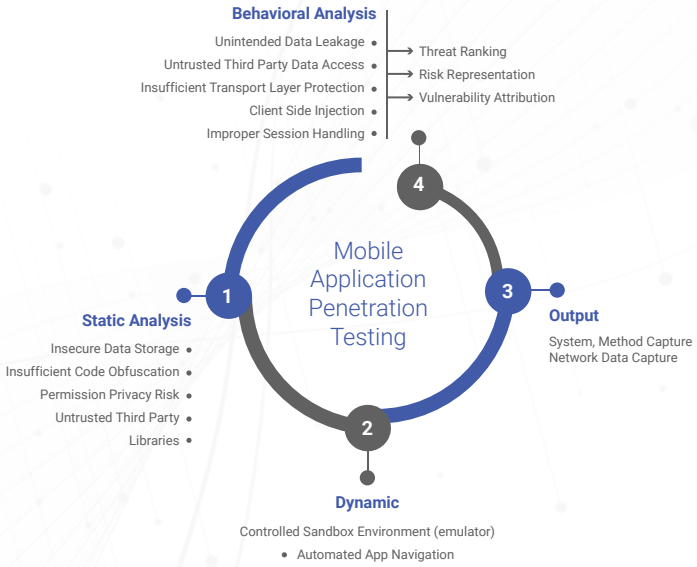
Vulnerability Enumeration
Search for exploitable vulnerabilities that may exist in services, APIs, applications or firmware.

Vulnerability Exploitation
Attempt to exploit identified vulnerabilities using a combination of publicly available exploit code, commercial penetration testing tools and internally developed exploit code and tools.

Accomplish Mission
Mission may include gaining access to the internal environment from the Internet, stealing data from segmented environments, or taking control of a device and issuing malicious commands.

Benefits

- Prevent future attacks by guessing the behaviour of attackers and anticipating their moves
- Going live with new/updated mobile application without excess worry about security risks
- Know the skill and experience of the app development agency/team that builds your mobile applications
- Test the responsiveness of your entire IT team
- Meet tough industry security standards and comply with regulations



Deliverables

- **Executive Report:**

The executive level report is written for management consumption and covers a high-level summary of assessment activities, scope, most critical vulnerabilities discovered, overall risk scoring.

- **Detailed technical report :**

Technical details with step-by-step information that allows you to recreate our findings. Fact-based risk analysis to know a critical finding is relevant to your environment. Tactical recommendations for immediate improvement and strategic recommendations for long-term improvement.

Mobile application penetration testing will assess the environment of the mobile application and determine the risks associated with the communications channels, data storage, and user interface. Undergoing regular penetration testing is key to your overall security posture. It's an important practice that gives organizations visibility into real-world threats to your security. The pros for having regular penetration tests performed far outweigh the cons.

PCI Security Standards Council
APPROVED SCANNING VENDOR

Corporate Office Address:
IITM Research Park, No.6 A-Block, 3rd Floor, Kanagam Main Road,Taramani, Chennai - 600 113.
P: +91 44 4208 9337 | E: info@cybersecurityworks.com | W: www.cybersecurityworks.com