Payatu

Mobile Application Security Datasheet



OVERVIEW OF THE SERVICE

As the adoption of the mobile phone reaches its peak, mobile apps are flourishing and flooding the app stores. More and more businesses are looking at utilizing an app for launching their products on mobile devices. But this does not come without a threat. That's right, from the millions of apps available for downloads, at least thousands of them are vulnerable to malicious activities, leaving user data at stake.

The solution?

Mobile Application Security Assessment.

Payatu has been the go-to service provider for reputed organizations looking to test the security posture of their mobile apps. The service provider makes it a point to understand the client application (both, Android and iOS) thoroughly to develop a customized assessment strategy and process. The goal of these assessments is to find highly critical to low vulnerabilities, to ensure a safe delivery of offerings for the client.

KEY ATTRIBUTES

The ultimate objective of Payatu is to perform controlled attack and penetration activities, covering all possible threats and attack vectors on the mobile app. What sets Payatu apart is -

A combination of realistic and abstract approach

Having substantial experience in this arena paired with learning the application conceptually helps Payatu Bandits to define a process and roadmap specific to the client.

End-to-end defining of the scope

It is important for Payatu to address all types of potential attacks on the client's mobile apps, which is why its scope covers everything ranging from application code, client-side vulnerabilities, server-side vulnerabilities, business logic vulnerabilities, and APIs endpoints, and all other application-specific configurations, etc.

Ultramodern tech integrations

Payatu strives to widen the attack surface to ensure identification of all vulnerabilities, and it does so by integrating different internal, external, and modern third-party tools and software.

Reports that go beyond reporting

Generalized reporting is a drawback that can make any mobile application security assessment futile. With Payatu, clients get a detailed report of the test cases that worked, a granular breakdown of the vulnerabilities, failed test cases, mitigation strategies, and recommendations.

The Payatu Extra Mile

Payatu goes an extra mile to retest and revalidate the apps, offer guidance to the in-house security team of the client on the mitigation plan, get the compliance of the application with the mandated standards, and a lot more.

Payatu

KEY BENEFITS

For a client, the top priority is to know the current security posture of its application, in order to better formulate a plan to strengthen it. Payatu ensures via its assessment approach that all hidden cues are discovered by offering -

01 Identification of Security Gaps with Integrity Check

Clients can identify security gaps which is highly important to protect the organization's assets by bypassing integrity checks. Integrity checks like anti-tampering, anti-debug, root prevention, SSL pinning, are given prime importance to ensure that the client's application can be secured efficiently. This is done so by trying out all the possible test cases for bypassing these protections.

02 Finding Hidden Vulnerabilities with Reverse Engineering

Clients need to have a complete overview of all the vulnerabilities in their systems. Payatu Bandits excel at identifying hidden vulnerabilities to help the client strengthen its security posture. For this, the compiled applications are converted into human-readable source code. This code is then reviewed in order to understand the internal application functionality making it easy to spot vulnerabilities.

03 360-degree Overview with Comprehensive Analysis

For the clients to make better and informed decisions, a comprehensive analysis consisting of – static analysis, dynamic analysis, and inter-process communication endpoint analysis is carried out with each mobile app assessment. Vulnerabilities are checked for several categories such as – code signing, authentication, password policy, authorization bypass, business logic flaw, input data validation, remember me feature, XML external entity attacks, SSL-related vulnerabilities, miscellaneous attacks, etc

04 Presentable Outcome

A detailed yet comprehensive report is a must for clients to understand the assessment optimally. All exploitable security vulnerabilities in the target system are recorded with associated CVSSV3.1-based scores and are reported to the client.

05 Build Brand Confidence for Users

Clients can make security their value proposition in the competitive digital market by establishing trust within their users/clients by offering security as their brands' proposition.

06 High Quality Testing

9 out of 10 industry leaders have made it a point to recommend Payatu's services to other pioneers because of the experiences they had while getting their applications tested. This has been made possible because of the best-in-class hires who have proved their mettle by going beyond their scope of work, even before they're hired.

Top Customers

stryker

Johnson Controls

TATA DIGITAL

BCG

navi

one card

Payatu

ENGAGEMENT MODELS

You choose what works best for you!

Payatu offers different engagement models to let the client decide what floats their boat when they avail themselves of the mobile application security assessment service. They can choose from

01

Time-boxed Approach,

where the client shares the details of the scope of assessment with Payatu and the service provider evaluates the time and investment required to execute the project. This evaluation is done with the help of complexity models

Complexity	Android or iOS	Android + iOS
Low	4 mandays	6 mandays
Medium	11 mandays	15 mandays
High	28 mandays	36 mandays

The complexity of the application is decided based on the number of screens, number of APIs, and the number of user roles in the app.

02

Staff Augmentation,

where the client leverages the skillset of Payatu's security consultants and has them work with their in-house security team for an agreed-upon period of time.

03

Master Services Agreement

Minimum duration & projects commitment,

where Payatu conducts a T-shirt sizing of the client-proposed minimum scope and classifies each project as per complexity.

Minimum T&M effort commitment,

where Payatu proposes investment mapped with resource skill, resource experience, duration of T&M engagement, based on the client-proposed minimum commitment.