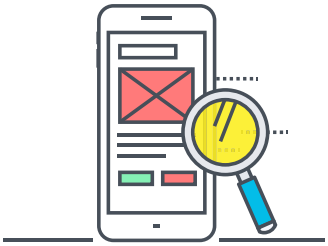
Mobile Application Scanning

A Dynamic Mobile Application Security Penetration Testing Solution from Indusface



Enterprises are now more open to the idea of Bring Your Own Device (BYOD) into corporate ecosystems as it boosts business efficiency, increases productivity and provides flexibility to users. However, enterprises are also faced with an alarming trend of increase in security breaches due to applications within these devices being compromised by vulnerabilities and malware, and hacking exploits leading to sensitive data leaks, privacy and commercial losses.

Disabled or circumvented security, unlocked or modified features, free pirated copies, ad-removed versions, source code/IP theft, and illegal malware-infested versions are some examples of the diverse hacks/attacks mobile applications are subjected to. More than 90% of the top mobile applications have been hacked in recent times. Hacking is prevalent in all types of mobile apps, and it is becoming a major economic issue with mobile application revenues growing to over $60 billion and mobile payments volume likely to exceed $1 trillion by 2016.

Studies have shown that with the prevalence of BYOD, 72% of organizations are extremely concerned over the state of application security and 66% over compliance requirements. Indusface has powered its technology combined with years of application security intelligence expertise to help address these concerns with Indusface MAS.

> We appreciate the quality of Indusface WAF and related services delivered to us and would recommend that Indusface can be entrusted with similar job for any prospective customer without hesitation
>
> Kinshuk De,
> Business Operations, Enterprise Security Risk Management,
> TCS

PRODUCT OVERVIEW

Indusface MAS is a comprehensive, next generation, on demand, dynamic application security penetration testing solution for mobile applications. It detects vulnerabilities and malware across multiple operating systems and devices. It gives a complete security posture, risk profile and readiness of enterprise apps to be used safely on mobile devices.

It uses a broad combination of mobile application security assessment techniques specific to mobile computing environments.

Adheres to industry standards which include the Open Web Application Security Project (OWASP) Top 10 for Mobile Applications.

Indusface MAS can be leveraged by Enterprises and App Stores to conduct in-depth security tests of their mobile applications before permitting them into their business ecosystem. Enterprises also get to maximize on existing investments in Mobile Device Management (MDM) or Mobile Application Management (MAM) products, since Indusface MAS adeptly complements these control point technologies with.

On Demand Comprehensive Mobile Application Security

Most Comprehensive Platform Coverage: Indusface MAS supports applications across all mobile computing platforms, such as iOS, Google Play, Windows, Symbian and RIM. It also supports all types of applications be it native, mobile web or HTML5.

Hybrid Mobile Application Security: is a powerful, high tech combination of automated application scanning and manual penetration testing, giving a complete and in-depth security assessment for all types of mobile applications.

Gain Risk Visibility: Detailed insightful reports with remediation guidelines of application vulnerabilities are shared, giving you a complete view of the risks the application is exposed to.

Improve and Increase Business Efficiency: Secure mobile applications help in minimizing productivity losses, enabling organizations to host their most productive applications onto mobile devices, gives users flexibility and enhancing business efficiency.

Strengthen Brand Reputation: Safe and secure apps help strengthen brand reputation immensely, as users know that they can always rely on a secure mobile computing environment to conduct business through these applications.

Mobile Application Security Threats Addressed

Each of these threats can be exploited by rogue applications and malicious users, which is extremely harmful for the enterprise, leading to dangerous exposure to sensitive corporate data.

Sensitive information written on mobile device

Mobile applications can access sensitive information such as financial details, passwords or private information stored on device memory.

Unencrypted traffic:

Mobile applications exchange information with the server such as login credentials, transaction details which can be sniffed out from the clear text traffic on the network by an attacker.

Injection attacks:

Injection flaws occur when an application sends untrustworthy data to an interpreter, thus causing loss of data and can even lead to hostile takeover, ruining clients' reputation.

Parameter manipulation attacks:

Malicious user may get access to the data or active session by manipulating parameters going in to HTTP requests and in the same way make fraudulent transactions.

Insecure coding:

By doing reverse engineering on the application installer file, an attacker can look into the code for hard coded sensitive and useful information like password, database credentials, log information etc.

Malware infected application:

Malware is designed to infiltrate and damage smartphones without the users consent. A mobile application needs to be assessed for any possible malicious activity on a mobile device to avoid any brand abuse or data breach.

Exception and error handling:

If error messages are not customized then they can reveal information about the application or server which might be a useful breach of security.

Weak server side controls:

If server side controls are not in place, this can lead to bypass validation implemented on the client and business logic, leading to security breach resulting in business loss.

Authorization and Authentication related checks:

An attacker can get unauthorized access of the application and will be able to perform malicious action leading to high security risks for the application.

Cryptographic storage:

In most of the implementations, mobile applications store some sensitive data on the mobile device. If this data is not encrypted and stored, then the stored clear text data or weakly encrypted data can be stolen and used against the legitimate user.

Session related threats:

Improper session management may lead to a compromised user session.

Unwanted Permissions:

Any unwanted permissions allowed by the application on a mobile device can lead to misuse of the application and can also lead to brand abuse / loss of sensitive data of the application owner.

FEATURES

On Demand, Hybrid Mobile Application Penetration Testing

Indusface MAS provides a complete security assessment of threats that can be potentially exploited in mobile applications using a combination of software tools and manual security intelligence.

Memory Analysis

Intensive memory analysis is undertaken by extracting data stored on the device by any application, this includes SQLite database analysis as well as cryptanalysis attacks.

Log Analysis

Analyze logs for sensitive information stored by any application like login credentials, personal information etc.

Static Code Analysis

Identify the main reasons of security vulnerabilities within source code by performing static analysis, receive severity of risk results in order of priority and get remediation guidance on how to fix these issues.

Malware Detection

Indusface MAS's unique malware detection engine ensures that applications do not have malware like signatures, which if exposed and exploited can significantly damage brand reputation and can result in huge commercial losses to a business.

Layer 7 Attacks Assessment

Business logic checks and session related attacks

Privilege escalation and authentication related checks

Intercept and manipulate Layer 7 traffic to bypass implemented controls.

Logical Vulnerabilities Detection

In-depth testing of the mobile application's business logic is conducted by security experts to check for complex vulnerabilities.

Remediation Guidance

Detailed remediation recommendation guidance is provided, which includes step by step instructions on how to address the threats captured.

Insecure permissions detection

All permissions are checked and verified to ensure that unwanted permissions do not exist in the application, which could result in unauthorized access and misuse of sensitive data.

Flexible and Comprehensive Reporting

Indusface MAS's executive dashboard provides a comprehensive synopsis of the threat profile of enterprise mobile applications along with business impact.

SUPPORT

Support is available to all Indusface MAS customers, covering:

24X7 unlimited e-mail support.

Dedicated on call support during business hours.

Prompt response and resolution turnaround time on support query requests.

Review of all threats found which helps assess how Indusface MAS has improved the application's security posture.

Dedicated technical account manager to address mobile application security requirements.

Unlimited proof of concepts to be conducted if required for proof of vulnerability remediation.

INDUSFACE™

Indusface is an award-winning SaaS-based total application security company with more than 900 enterprise customers spread across 18 countries who trust us with their web and mobile application security.

www.indusface.com | sales@indusface.com | support@indusface.com

SAN FRANCISCO VADODARA BENGALURU MUMBAI DELHI