Introduction Mobile Application Security Testing

Mobile Application Security is one of the most important components in the application development life cycle as hackers are increasingly targeting applications with their sophisticated attacks. It is making sure that the security of an application is more secure by identifying, rectifying and taking preventive action.

Our comprehensive test methodologies include frameworks for detecting and highlighting security flaws in mobile applications using the SAST, DAST, and IAST methods for static and behavioral analysis. Our methods eliminate the possibility of false positives, and they identify risks and develop a plan to close any gaps.

Every new iteration of our mobile device security testing solution is thoroughly tested against a 12-point specific certification criteria that maps to OWASP Mobile Top 10, SANS Top 25, and other regulatory requirements like PCI-DSS.

Service Benefits

- Risks in iOS, Android, and Windows Phone applications are identified and remedied.
- Evaluate and report on the security of mobile applications to senior management and other stakeholders.
- Identify critical information exposures in your environment due to mobile apps.
- Assess the security posture of newly developed mobile technologies.

Assessment Details and Methodology

At Infopercept, we begin by intercepting traffic, analyzing HTTP transactions, manipulating commands and related responses, and finally submitting a final report that includes a clear and measurable remediation plan and workflow.

Information gathering on the target environment

1.Reconnaissance
As with malicious hackers, any penetration test starts with the collection of information. To detect vulnerabilities, collecting, parsing, and correlating information on the target is essential.

Identify and map vulnerabilities

2.Vulnerability Detection
If the goal has been thoroughly listed, Infopercept uses both vulnerability scanning software and manual inspection to find security vulnerabilities. With decades of experience and custom-built equipment, our security engineers have found several unique and innovative ways of finding and fixing vulnerabilities.

Although code scanning tools may be helpful in detecting low-hanging threats, they are no substitute for professional engineers. By using the previous mapping and scanning techniques, we concentrate on the most vulnerable areas of the code – and discover weaknesses that automated services have overlooked.

Safe and controlled exploitation of vulnerabilities

3.Attack and Post-Exploitation
At this point of the evaluation, our experts will analyse all prior data to detect and securely exploit known bugs in the program. Once critical access has been achieved, the emphasis will be on escalation and movement to determine technological risks and the overall market effect. During each step of the compromise, we keep client stakeholders updated about progress testing, maintaining asset protection and stability.

Detailed, risk- prioritized report with remediation steps

4.Assessment Reporting

If the engagement has been completed, Infopercept will include a concise review and vulnerability report, including remedial action. Our advisors set industry standards for transparent and succinct reviews, prioritizing the highest risk vulnerabilities.

The appraisal shall contain the following:

> Executive Summary.
> Strategic strengths and weaknesses.
> Identified vulnerability and risk rating.
> Detailed risk remediation.
> Assets and Data Committed during the assessment

About Infopercept - Infopercept is one of the fastest-growing comprehensive cybersecurity companies in India, serving global clients. It provides platform led managed security services that covers all areas of cybersecurity, including defensive, offensive, detection and response, and security compliance. Infopercept has its own cybersecurity platform, 'Invinsense,' which integrates tools such as SIEM, SOAR, EDR, deception, offensive security, and compliance tools. Its cybersecurity and MDR services include dedicated teams of experts, ensuring that organizations have 24x7 cybersecurity operations support.

Infopercept | **INVINSENSE**