Privia SECURITY

Mobile Application Security Service

Professional Offensive Security Services

"Strong Defense Against Mobile Threats!"

Queen Elizabeth Olympic Park, 14 East Bay Lane, Plexal, London, England, UK, E20 3BS

info@priviasecurity.co.uk

www.priviasecurity.co.uk

“We identify potential vulnerabilities in your mobile application and minimize potential risks.”

Mobile applications have become the most important communication and business tools for individuals and businesses today. This has led to an increase in cyber-attacks against mobile applications and the security of applications has become more critical than ever. As Privia Security, we offer a comprehensive penetration testing service to detect and fix the security vulnerabilities of your mobile applications.

Our penetration tests are conducted according to OWASP Mobile Security Testing Guide (MSTG) and OWASP Mobile Application Verification Standard (MASVS) methodologies. In these tests, we identify the vulnerabilities of your mobile application by addressing topics such as application analysis, user login and authentication, data security, communication security and general application security. These comprehensive tests, which are performed independently of various development languages and frameworks used on different mobile platforms (iOS android), evaluate the compliance of your mobile application with security standards and provide recommendations to developers for security improvements.

All security vulnerabilities identified as a result of Mobile Application Penetration Tests are presented in a detailed report. This report includes the importance of the vulnerabilities, their possible effects and the necessary solutions to close them. Take advantage of Privia Security's penetration testing services to secure your mobile applications and protect your users' data.

Service Components

Application Analysis

It involves examining the structure, components and functionality of the mobile application. In this process, risks are identified by identifying situations that indicate potential security vulnerabilities of the application. The findings of the analysis form the basis for improvements to be used to make the security level of the application more robust.

Authentication and Data Security

User login and authentication mechanisms are one of the most critical components of application security. In order to ensure the security of these components, comprehensive tests are performed and potential vulnerabilities are evaluated. In addition, the data security of the application is examined, especially in terms of protecting sensitive data. With the work done, it is aimed to ensure data integrity and minimize the risks of data loss.

Communication Security and Platform Compatibility

Communication security of the application is an important stage for the protection of data integrity in its connections with the outside world. Within the scope of this component, network traffic and data encryption processes are evaluated in detail. In addition, mobile application penetration tests are performed on different mobile platforms such as iOS android and in accordance with various development languages (such as Swift, Kotlin, React Native, Xamarin).

Application Vulnerabilities and Reporting

The tests performed in the process of identifying potential vulnerabilities within the application and eliminating these vulnerabilities are intended to increase the overall security level of the application. As a result of the penetration test, all security vulnerabilities identified in the application are presented in a report. This report includes the severity of the vulnerabilities, their possible effects and recommendations for their closure. These recommendations for developers provide guidance to make the application more secure.

Cryptography and Data Encryption

Cryptographic algorithms and data encryption methods used in mobile applications are of great importance to ensure the security of sensitive information. Within the scope of this component, the security of the encryption protocols and key management processes used are evaluated in detail. By ensuring that encryption methods are applied correctly and reliably, data confidentiality and integrity are guaranteed.

FAQ

What is mobile app penetration testing and why is it important?

Mobile application penetration testing is a security test conducted to identify security vulnerabilities in mobile applications and to eliminate the identified vulnerabilities. Since mobile applications today host user data and manage financial transactions, the security of these applications is of critical importance. Mobile Application Penetration tests provide protection against potential threats from attackers by detecting security vulnerabilities early.

When to perform a mobile app penetration test?

Mobile application penetration testing should be performed at different stages of the application development cycle. Testing may need to be done when the app is first being developed, before or after major updates, after integrating third-party components and for any compliance audits. For new applications that are going live, Security audits are performed during the final testing phase before release. Regular testing throughout these processes helps to keep the security level of the application high by identifying potential vulnerabilities immediately.

How to do mobile app penetration testing?

Mobile application penetration testing is performed using a combination of manual and automated tools. First, application analysis and risk assessment is performed. Then, data security, authentication, authorization and communication protocols are assessed in accordance with international methodologies such as the OWASP Mobile Security Testing Guide (MSTG) and the OWASP Mobile Application Verification Standard (MASVS). During mobile application penetration tests, the structure and functions of the application are analyzed in detail and potential security vulnerabilities are revealed through various penetration techniques.

What is included in mobile penetration test results?

As a result of the mobile application penetration test, a report is submitted that describes in detail the security vulnerabilities identified in the application and the possible effects of these vulnerabilities. The report includes an executive summary, technical steps required to eliminate the vulnerabilities, recommendations and solution methods. Thanks to the findings in the report, it offers suggestions to the developers to increase the security level of the application.

What types of vulnerabilities does mobile penetration testing detect?

Mobile application penetration testing aims to detect various security vulnerabilities. These vulnerabilities include authentication and authorization weaknesses, weak encryption algorithms, data security deficiencies, insecure network communication, misconfiguration and inappropriate storage of sensitive information on the device. Weaknesses that can be exploited by advanced threat actors are also identified, increasing the security level of the application.

How long does a mobile app penetration test take and what factors affect this time?

The duration of mobile application penetration testing varies depending on the complexity of the application, the technologies used, the size and scope of the application. A small-scale mobile app can usually be tested within 1 week, while a more complex or large app can take between 2-5 weeks. Factors such as the number of platforms on which the app needs to be tested (iOS android), third-party integrations and data encryption methods affect the testing time.

Your Trusted Partner in Cybersecurity

Founded in 2018 with a vision for the future of cybersecurity, Privia Security has been committed to delivering high-quality services to its clients from day one. With a strong and capable team, we provide the most reliable and comprehensive solutions across all areas of cybersecurity, ensuring our clients are well-protected in today's digital landscape.

As cyber threats continue to evolve rapidly and grow in complexity, combating them becomes increasingly challenging. At Privia Security, we offer both defensive and offensive cybersecurity strategies powered by cutting-edge technology to meet our clients' evolving needs. Through our innovative R&D products and strategic consultancy, we aim to enhance organizations' cybersecurity maturity and deliver proactive, tailored solutions. We are proud to be safeguarding the digital assets of more than 300 major organizations.

Global and Local Cybersecurity Solutions

Privia Security delivers cybersecurity services across a broad geographical scope, including Europe, Asia, the Middle East and the Americas. Our specialized teams in Offensive, Defensive and Forensic operations develop bespoke solutions for organizations operating in diverse sectors such as critical infrastructure, avionics systems, corporate networks and the military.

In addition, our innovative cyber warfare simulation platform, PriviaHub, offers comprehensive solutions for nations seeking to strengthen their cyber defense capabilities. PriviaHub enables the testing of cyber warfare strategies, execution of simulations and assessment of expert competencies. Designed to meet the exercise needs of private sector entities, academic institutions and military organizations, it bridges the gap between training and real-world readiness.

A Secure Future Through Advanced Technology

With R&D centers located in Istanbul, Ankara, London and at Cumhuriyet Technopark, we are continuously developing value-driven projects for our clients. From penetration tests and red team operations to cybersecurity training and custom enterprise solutions, we are redefining the standards in our industry. Through our slogan "Privacy For You," we bring a fresh, innovative perspective to security and privacy—

Privia
SECURITY