ncc group

Mobile Application Security Assessment

Modern mobile devices offer far more functionality than previous generationmobile phones and Personal Digital Assisstants (PDAs). They now offer the power and functionality of traditional client computers and are therefore susceptible to many of the associated risks, as well as new risks unique to these devices. In a mobile application assessment, NCC Group's team of consultants will examine the mobile application, to identify security vulnerabilities that may be exploited to compromise user data on the device or accessed via a remote server using a web service or other network interface.

A mobile application assessment from NCC Group will give you a comprehensive audit of the security of the application, ensure that applications are secure in handling sensitive data and do not allow unauthorised access to back-end servers. It will also give you the assurance you need that your mobile application is putting neither you nor your users at unnecessary risk.

What we do

Everyassessment is different, tailored to the unique needs of the customer, but a typical assessment will include:

Recon and analysis:
We will map the application's content and functionality, analyse its behaviour, identify all possible entry points for user input and develop a clear understanding of the attack surface exposed by the application.

Assessment of access handling:
We will assess he application's core security mechanisms, including authentication, session management, and access control, to identify any defects that may enable an attacker to gain unauthorised access to functionality and data. In this stage we might find problems which could be exploited to access users' accounts, view sensitive files, or use unauthorised functions.

Assessment of input handling:
We will test the application's resilience to unexpected input throughout its functionality, looking for code injection and other vulnerabilities. Where input is not validated before being sent to a server, an attacker could use this flaw to access and attack the supporting back-end components or other users.

Assessment of device storage:
We will assess the application's interaction with local storage, looking for unprotected secrets written to local storage which can be read by malicious users, or files which can be manipulated
to subvert the application. In this stage we might find problems such as sensitive data stored in clear text - insecure local storage is a concern if the device is lost or stolen.

Transport security:
We will assess the application to ensure that appropriate transport security is used. In this stage we might find flaws which would allow an attacker to perform a man-in-the-middle attack and gain control of user data.

Flaws we look for include:

Webservice flaws:
The parameters sent to web service endpoints are analysed to identify privilege escalation opportunities, error handling problems, injection flaws, broken access controls, and other web application threats.

Sensitive information hardcoded:
A black-box assessment will be performed, in which the application is decompiled or reverse engineered to identify sensitive information such as encryption keys, hard-coded back-end credentials, server IP addresses, or default credentials within the binary.

Data interception:
Where the application makes use of networked communications, attempts will be made to intercept and tamper with the data.

For more information from NCC Group on our G-Cloud 15 service, please contact:

+44 (0)161 209 5200

bidteam@nccgroup.com