ncc group

Web Application Assessment

In a web application assessment, NCC Group's team of consultants will examine your web application to identify vulnerabilities which a malicious user could exploit to attack your systems or users or to extract sensitive data.

Working remotely from NCC Group's offices, our consultants will use their expertise, combined with state-of-the-art automated tools, to identify vulnerabilities in your application and to provide advice on how to rectify them.

During the assessment the consultants use proven non- invasive testing techniques to quickly identify any weaknesses. The application is viewed and manipulated from several perspectives, including with no credentials, user credentials, and privileged user credentials.

What we do

Recon and analysis:
We will map the application's content and functionality, analyse its behaviour and develop a clear understanding of the attack surface exposed by the application. In this stage we might find problems such as the possibility of a denial of service attack. If an attacker can determine what processes use the most resources, it is possible to consume web application resources to a point where legitimate users can no longer access or use the application.

Assessment of input handling:
We test how the application responds to unexpected input, looking for code injection and other vulnerabilities. In this stage we might find problems such as injection flaws or buffer overflow susceptibility. When information from web requests is not validated before being used by a web application, a malicious user could use this to attack the back-end components or other users.

Assessment of access handling:
We test the application's core security mechanisms to identify any defects that may enable an attacker to gain unauthorised access to functionality and data. In this stage we might find problems such as improperly enforced access ontrols, which an attacker can exploit to access other users' accounts, view sensitive files or use unauthorised functions.

Assessment of application logic:
We will probe for defects within the application's logic, including inappropriate reliance on client-side controls and logic flaws within server-side functionality. In this stage we might find problems such as improper error handling. If an attacker can identify errors that the web application fails to handle correctly, they can systematically force those errors, revealing system information.

Other flaws we look for include:

Broken authentication and session management:
When account credentials and session tokens are not properly protected, an attacker can exploit these weaknesses in order to defeat authentication restrictions and assume other users' identities.

Cross-site scripting (XSS) flaws:
A successful XSS attack could allow a malicious user to create a malicious link or write malicious code into a web application.

Insecure storage:
Storing information such as credentials usually involves cryptography. When the cryptographic function is not coded properly, or is not integrated appropriately, information is not protected.

Insecure configuration management:
Build testing usually results in improvements to standard builds. We can supply build standard documents customised to your requirements, based on the results of the assessment.

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

+44 (0)161 209 5200

bidteam@nccgroup.com