Web Service / API Security Assessment

In a web service assessment, NCC Group's team of consultants will identify security vulnerabilities that may be exploited to compromise either the server-side application or ordinary users of the application.

The primary areas of concern in web service security are code execution, authentication bypass, injection, privilege escalation and data extraction. A web service assessment from NCC Group will give you a comprehensive audit of the security of the service, finding common vulnerabilities such as message replay attacks, XML complexity attacks and transport security weaknesses. This gives you the assurance you need that your web services are not providing attackers with easy access to your data and systems.

What we do

Analysis:
We will use the API documentation to 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 the service'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. When access control restrictions are not properly enforced, an attacker can exploit these flaws to access other users' accounts, view sensitive files, or use unauthorised functions.

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

Assessment of application logic:
We will probe for defects within the service's logic, including inappropriate reliance on client-side controls, and logic flaws within server-side functionality. In this stage we might find flaws such as buffer overflows, in which a remote attacker may be able to provide specially-crafted malicious input which causes the components to crash and, in some cases, can lead to remote code execution.

Other flaws we look for include:

Injection flaws:
Web services pass data between the user and server using a protocol called SOAP (Simple Object Access Protocol). If an attacker can embed malicious commands in the SOAP parameters, the external system may execute those commands on behalf of the web service.

Improper error handling:
There are instances where error conditions occur during normal operations and are not handled properly. If an attacker can identify the errors that the web service fails to handle correctly, they can systematically force those errors, revealing system information.

Insecure storage:
Storing information such as credentials usually involves cryptography. Integrating cryptography into a web application can be complex, and as a result, there are often deficiencies in its execution. When the cryptographic function is not coded properly, or is not integrated appropriately, information is not protected.

Denial of service:
An attacker can survey a service to determine what processes use the most resources. With this knowledge it is possible to consume web service resources to a point where legitimate users can no longer access or use the service. In extreme cases the service can be knocked over and cease functioning completely.

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