

Case Study – A Large Corporation

Brief

To test corporate extranet and advise as necessary.

Approach

No information was provided about the extranet, other than the web URL through which it was accessed.

Outcome

Multiple vulnerabilities were found in RSS feeds linked to the extranet's news areas. These XML exploits enabled us to gain administrative access to the network server providing the news feeds. From here we were able to enumerate the entire anonymous head office network structure and escalate privileges to administrator. SQL union vulnerabilities were found in extranet logins and inter extranet functions such as bulletin postings etc.

Solutions

Complete code review of this extranet was largely irrelevant due to the extent of the vulnerabilities found and the extranet was redesigned and rebuilt by ourselves to provide higher levels of functionality in a secure environment.