A 01:2021 - Broken Access Control

Prevention

BAC Prevention

Deny by default i.e every user starts with the minimum privileged functions

BAC Prevention

Enable RBAC (Role-Based Access Control)

BAC Prevention

Disable web server directory listing and ensure file metadata and backup files are not present within web roots

BAC Prevention

Disable web server directory listing and ensure file metadata and backup files are not present within web roots

BAC Prevention

Constant Testing & Auditing of Access Controls