Broken authentication and session management

Broken authentication and session management is a web application vulnerability that allows attacker to gain unauthorized access to web site by stealing the user credentials or by forging the sessions data .commonly the application will implement the login functionality to provide functionalities based on users role and will track the users based on session id .if this functionality is not implemented correctly then attacker will tries to gain unauthorized access.

If the authentication mechanism is not implemented then the attacker can brute force with a list of usernames and passwords and can get the credentials or if the application is using the default usernames and password the attacker can easily guess, the attacker can also bypass using Boolean based using injection. If the session is not managed correctly then the attacker can guess the session id or session hijack or session reuse.By successfully attack using broken authentication and session management the attacker can gain access to victim user accounts sometimes attackers can also get access to the admin account.

The best methods for avoiding broken authentication-related issues is to implement strong password policy, account lockout policy after invalid attempts, implementing strong captcha for avoiding brute-forcing, and implementing a strong authenticating system by hashing password rather then sending in plain text if possible implementing the two-factor authentication. for avoiding the session management related issues is to not expose the session id in URLs, the session-id generating should be unpredictable, properly validating the sessions id with every request, session should be terminated after user logged out, the new session should be generated with every new login and user session should be terminated after a certain amount of inactive time(maximum 5 to 10 minutes).