OWASP

CHEAT SHEETS SERIES

MASTER CHEAT SHEETS

AUTHENTICATION

Ensure all entities go through an appropriate and adequate form of authentication. All the application non-public resource must be protected and shouldn't be bypassed. For more information, check Authentication Cheat Sheet

ACCESS CONTROL

Ensure that a user has access only to the resources they are entitled to. Perform access control checks on the server side on every request. All user-controlled parameters should be validated for entitlemens checks. Check if user name or role name is passed through the URL or through hidden variables. Prepare a ACL containing the Role-to-Function mapping and validate if the users are granted access as per the ACL.

OUTPUT ENCODING

Output encoding is the primary method of preventing XSS and injection attacks. Input validation helps minimize the introduction of malformed data, but it is a secondary control. For more information, check XSS (Cross Site Scripting) Prevention Cheat Sheet.

SECURE TRANSMISSION

Ensure that all the applications pages are served over cryptographically secure HTTPs protocols. Prohibit the transmission of session cookies over HTTP. For more information, check Transport Protection Cheat Sheet.

SESSION MANAGEMENT

Use secure session management practices that ensure that users authenticated users have a robust and cryptographically secure association with their session. For more information, check Session Management Cheat Sheet

INPUT VALIDATION

Input validation is performed to minimize malformed data from entering the system. Input Validation is NOT the primary method of preventing XSS, SQL Injection. These are covered in output encoding below. For more information, check Input Validation Cheat Sheet

CROSS DOMAIN

Ensure that adequate controls are present to prevent against Cross-site Request Forgery, Clickjacking and other 3rd Party Malicious scripts. For more information, check Cross Site Request Forgery.

LOGGING

Ensure that all the security related events are logged. Events include: User log-in (success/fail); view; update; create, delete, file upload/download, attempt to access through URL, URL tampering. Audit logs should be immutable and write only and must be protected from unauthorized access. For more information, check Logging Cheat Sheet

UPLOADS

Ensure that the size, type, contents and name of the uploaded files are validated. Uploaded files must not be accessible to users by direct browsing. Preferably store all the uploaded files in a different file server/drive on the server. All files must be virus scanned using a regularly updated scanner.

for more info visit:
https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series#tab=Master_Cheat_Sheet