Phases		
Analysis	• Historical goals e.g. allow people to access historical information from anywhere in the world. • Privileges can be given to administrator and program manager only so that anyone else can not misuse those privileges.	
Design	Input Validation	During designing of online form do proper validation of name, birth date, email, contact number, address, username etc. Otherwise this section can be used by attacker for input validation.
	Authentication	Only authorised user should get access to website otherwise hacker can perform any of the following activity Network eavesdropping, brute force attacks, dictionary attacks, cookies reply, credential theft.
	Authorization	Identify all roles (admin, program manager, account manager, registered user, new user) properly then give privileges according to the roles.
	Sensitive management	Access to sensitive data like user details, shopping details and account details should be given to registered users only, otherwise there is possibility of network eavesdropping, data tampering.

Aim: To implement a security framework (secure software lifecycle) for Museum management System.

	Session management	Once the user login till that user is going to logout his session should get maintain properly.

	Cryptography	we need encrypted password so keys for encryption and decryption should be strong so that password will not get reveal.
	Parameter manipulation	Parameters passed by clients like UserId, username, password, contact number, email should be manipulated properly by removing suspicious special characters.
	Exception mgmt	Error should get handled properly, it should not reveal any program information
Implem e-ntation	Input Validation	Validate all text boxes, remove special characters like < , >, from otherwise SQLIA,XSS and BOF is possible
	Authentication	Instead of using only registration and password use biometric registration otherwise hacker can get access to your database
	Authorization	Identify all roles (admin, program manager, account manager, registered user, new user) properly then give privileges according to the roles. Make proper use of grant command.
	Sensitive management	Access to sensitive data user details, shopping details and account details should be given to administrator only , otherwise there is possibility of network eavesdropping, data tampering.
	Session management	Once the user login till that user is going to logout his session should get maintain properly using Http Session Objects or any other session tracking technique. Otherwise attacker hijack any session.
	Cryptography	For sorting password, barcode and fingerprints in database we need encrypted data so keys for encryption and decryption should be strong so that data will not get reveal. Use proper DES or AES systems or Quantum Key Protocol.

	Parameter manipulation	Parameters passed by clients like registration number, finger prints, password, email should be manipulated properly by removing suspicious special characters and spaces should get replace with hexadecimal symbols.
	Exception management	Error should get handled properly, it should not reveal any program information
Testing	Improper test data: Most published literatures introduce techniques for generating test cases from UML models, such as sequence diagrams or activity diagrams, and so on. Any diagram-based test method is based on path traversing. A run driven by one test case may not detect the modelled threats, so various runs taking different paths may be necessary to find a path which can activate the threat behaviour. Killing criteria should get defined properly. Design test data such a way that it will cover paths.	
Deployment	Network Threats: All network guards like firewall, application firewall, honey-pot and IDS should be updated otherwise following threats are present Information gathering, Sniffing or eavesdropping , spoofing, Session hijacking, Denial of service Server Threats : Server on which I am going to deploy “museum mangmt System” should be secure otherwise following threats are possible Viruses , Trojan horse and worms Foot printing Password cracking Denial of service Arbitrary code execution Unauthorized access.	
Maintenance	All tables used in “Museum management System” should be updated properly.	