***Secure Code Review***

***SQLI***

To check whether a web application is vulnerable to SQL Injection or not , we can following the steps

1. Enter single quote or double quotes into the input fields, if we receive error message this indicates the vulnerability.
2. Enter the various payloads in the input field.

* 1' OR '1'='1
* ' UNION SELECT NULL --
* 1' AND 1=1
* 1' OR 'x'='x

If the application is vulnerable SQLi it gives us error messages or unexpected data.

1. Boolean conditions such as ***OR 1=1*** and ***OR 1=2***, and look for differences in the application's responses.
2. We can use tools like Burp Suite to scan for SQL Injection vulnerabilities

***Preventing SQLi***

1. We can prevent SQLi using parametrized queries instead of string concatenation within the query
2. Validate the user input and URL parameters before the processing.
3. Escape the special characters such as single quote,double quote.
4. Limit the data base privileges to the application user.
5. Use Web application firewalls.
6. Use CSP (Content Security Policy)

***XSS***

To check whether the application is vulnerable for XSS (Cross-Site-Scripting) we can follow the steps below:

1. Test the input fields by injecting some common payloads .If the payload executes , the application is vulnerable.

* <script>alert9123)</script>
* "><img src=x onerror=alert(1)>
* <svg onload=alert('XSS')>
* javascript:alert('XSS')

1. Look for specific error message , some applications return error messages that reveals information about input handling.
2. Use tools like Burp Suite’s web vulnerability scanner, which combines static and dynamic analysis to identify XSS vulnerabilities.

***Preventing XSS***

1. Convert special characters in output to their corresponding HTML entities.

* < becomes &lt;
* becomes &gt;
* & becomes &amp;

1. Validate user input.
2. Set the ***HttpOnly*** flag on cookies to prevent access to cookie data via JavaScript. This helps mitigate XSS-related session hijacking.
3. Avoid inline javascript to reduce the risk of XSS,

* Onclick
* Onreset

1. Use CSP and WAF .