Web Application Security Testing Checklist

Objective	Pass / Fail	Remarks
Test by pasting internal URL directly onto the browser address bar without login. Internal pages should not open.		
If you are logged in using username and password and browsing internal pages then try changing URL options directly. I.e. If you are checking some publisher site statistics with publisher site ID= 123. Try directly changing the URL site ID parameter to different site ID which is not related to the logged in user. Access should be denied for this user to view others stats.		
Try some invalid inputs in input fields like login username, password, input text boxes etc. Check the systems reaction on all invalid inputs.		
Web directories or files should not be accessible directly unless they are given download option.		
Test the CAPTCHA for automates script logins.		
Test if SSL is used for security measures. If used proper message should get displayed when user switch from non-secure http:// pages to secure https:// pages and vice versa.		
All transactions, error messages, security breach attempts should get logged in log files somewhere on the web server.		
Check if web application is able to identify spam attacks on contact forms used in the website.		
Verify that all usernames and passwords are encrypted and transferred over secured connection like https.		
Verify information stored in website cookies. It should not be in readable format.		

Web Application Security Testing Checklist

Objective	Pass / Fail	Remarks
Password should be at least 8 character long containing at least one number and one special character.		
Username should not be like “admin” or “administrator” (if exists).		
Application login page should be locked upon few unsuccessful login attempts.		
Verify if special characters, html tags and scripts are handled properly as an input value.		
Internal system details should not be revealed in any of the error or alert messages.		
Custom error messages should be displayed to end user in case of web page crash.		
There should not be any hard coded username or password in the system.		
Verify all input fields with long input string with and without spaces.		
Verify if reset password functionality is secure.		
Verify user session ends upon log off.		
Verify that directory browsing is disabled on server.		
Verify that all applications and database versions are up to date.		
Important input validations should be done at server side instead of JavaScript checks at client side.		