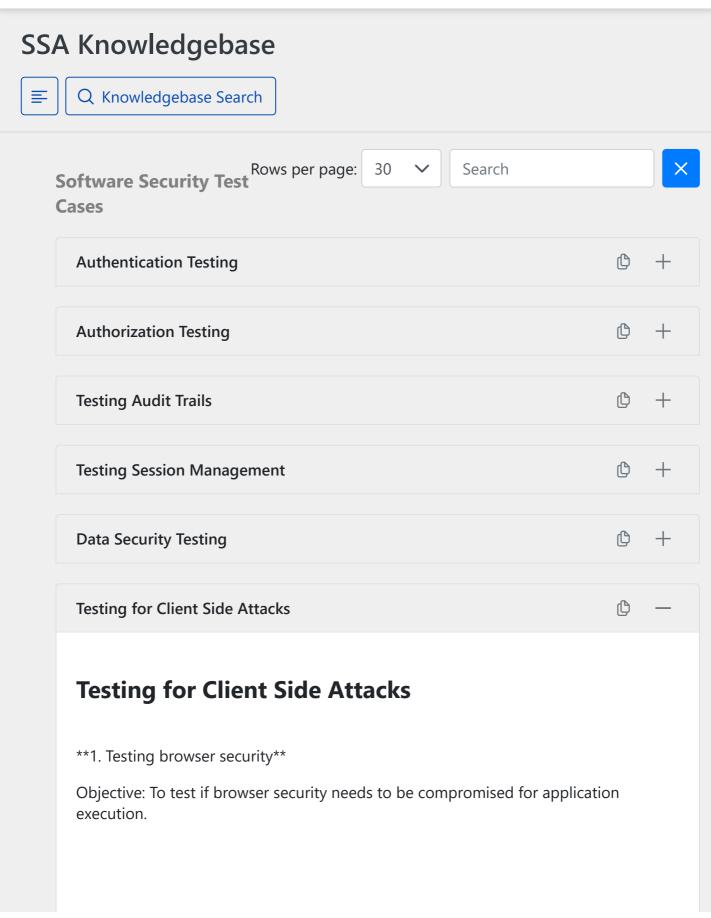
4/9/24, 5:28 PM SSA Portal







4/9/24, 5:28 PM SSA Portal

Test case ID	Description	Expected results
Client.1.1	Check if user is made aware of lowest version of browser that application can support	Installation manual contains information about browser version support
Client.1.2	Check if application has browser dependency	Application is independent of browser
Client.1.3	Check if application allows user to use browser specific features	Application is independent of browser
Client.1.4	Validate if Is application lowers browser security	Application works with highest security level of browser
Client.1.5	Check if application has dependency on third party browser add-on (i.e. flash plug-in)	Application do not have any dependency on browser extensions
Client.1.6	Check if application installs browser add-on	Application do not install any add-on

^{**2.} Testing for XSS**

Objective: To test application for XSS vulnerability.

Objective: To test application for CSRF vulnerability.

	Test case ID	Description	Expected results
	Client.2.1	Check if application takes user input and use them without validation	Application validates user input before use
	Client.2.2	Check if application stores user input at client side and displays it back without validation	Application do not store any input at client side
	Client.2.3	Check if application uses any of desktop properties (i.e. environment variables) without validation	Application do not use any of desktop properties
	Client.2.4	Check if centralized validation / sanitization library is used across application	All developers are using centralized validation / sanitization library
	Client.2.5	Check if centralized library allow end user to supply html content or scripts as input	
	Client.2.6	Check if input from any other application/service is also passed through centralized library	All inputs to application pass through centralized library that validate / sanitize inputs
	Client.2.7	Validate if application displays content from third party	Application do not display content from third party
	Client.2.8	Validate if application allow user to upload html or script file	Application do not allow html or script file upload.
3. Testing for CSRF*			

4/9/24, 5:28 PM SSA Portal

Test case ID	Description	Expected results
Client.3.1	Validate if all end user actions are performed through POST request	All end user actions are performed through POST request
Client.3.2	Validate if application generates random number to identify each action	Application generates new random number which is supplied as hidden field whenever action is requested by end user
Client.3.3	Check if application deploy CAPTCHA type mechanism to differentiate automated action vs. user action	Application uses CAPTCHA to avoid automated actions

^{**4.} Testing for Http exploits***

Objective: To test application for http response splitting and request smuggling vulnerability.

Test case ID	Description	Expected results
Client.4.1	Validate if server (or application) allow user to supply CR, LF or CRLF character as part of http request header	server / application do not allow user to supply CR (%0d) and LF (%0a) as part of header
Client.4.2	Validate if server (or application) allow user to supply data as part of http request header	server / application do not allow user to supply data as part of http request header
Client.4.3	Check if Response.Redirect(URL) type construct is used in application	Application do not blindly redirect user to given url
Client.4.4	Validate if output is encoded while displaying user supplied data	Html and Url both are encoded
Client.4.5	Validate if components between user and application (browser, cache, proxy) are not vulnerable.	•

^{**5.} Testing for content spoofing**

Objective: To test whether application is vulnerable to content spoofing.

Test case ID	Description	Expected results
Client.5.1	Is application uses Frame or iFrame based structure to display content	Application do not user insecure way of Frame/iFrame based structure
Client.5.2	Is application display content from third party site	Application do not display content/image/feed from third party site