Static Resource Rules

By Configuration Elements · https://community-staging.qualityclouds.com/qcdocs/qc/configuration-elements/static-resource-rules/

The following table shows the list of Salesforce Static resource rules that are checked by Quality Clouds.

Best Practice	Issue Severity	Impact Area
Use of Open Source Javascript framework	Warning	Manageability
XSS vulnerability in Ext JS Action Column getTip	Warning	Security
AngularJS - Prototype Pollution Vulnerability under 1.7.9	High	Security
AngularJS - XSS vulnerability using AngularJS under 1.6.9 with Firefox	High	Security
AngularJS - XSS vulnerability through the attribute "usemap" from 1.3.0 to 1.5.0-rc2	High	Security
AngularJS - XSS vulnerability through the attribute "usemap" from 1.0.0 to 1.2.30	High	Security
AngularJS - XSS vulnerability using AngularJS under 1.6.5 in Firefox and Safari - sanitize on inert Documents	High	Security
AngularJS - XSS vulnerability under 1.8.0 - input HTML	High	Security
AngularJS - Denial of Service attack through DOM clobbering on versions under 1.6.3	High	Security
jQuery - XSS vulnerability under 3.5.0, when using htmlPrefilter	High	Security
XSS vulnerability in Ext JS Action Column getTip	High	Security
jQuery - Prototype Pollution Vulnerability under 3.4.0	High	Security
jQuery - XSS vulnerability under 1.6.3, when using location.hash	High	Security

jQuery - XSS vulnerability under 1.9.0, when using jQuery(strInput)	High	Security
jQuery - XSS vulnerability under 3.0.0, when making cross-domain calls without the dataType option	High	Security
jQuery-ui-tooltip - XSS vulnerability under 1.10.0, title attribute	High	Security
jQuery-ui-dialog - XSS vulnerability under 1.10.0, title attribute	High	Security
jQuery-ui-dialog - XSS vulnerability under 1.10.0, closeText parameter	High	Security
moment.js - Regular Expression Denial of Service Vulnerability	High	Security