Security Best Practices For ServiceNow

By Impact Area · https://community-staging.qualityclouds.com/qcdocs/qc/by-impact-area/security-best-practices-for-servicenow/

The following table shows the list of best practices for ServiceNow security.

Click the button below to open the table in a popup.

Open Table

Description	Severity	Configuration Element Type
JavaScript – Avoid use of Function Constructors	High	Access control Business rules Client script Catalog client scripts Email script Inbound email action Record producer Script action Script include Scripted rest resource Table transform map Transform script UI Action UI Script Widget Widget Angular Provider

JavaScript – Avoid use of WebDB	High	Access control Business rules Client script Catalog client scripts Email script Inbound email action Record producer Script action Script include UI Action UI Script Widget Widget Angular Provider
JavaScript – Avoid use of debugger statements	High	Access control Business rules Client script Catalog client scripts Email script Inbound email action Record producer Script action Script include Scripted rest resource UI Action UI Script Widget Widget Angular Provider

JavaScript – Avoid unrestricted targetOrigin on cross-domain messaging	High	Access control Business rules Client script Catalog client scripts Email script Inbound email action Record producer Script action Script include Scripted rest resource UI Action UI Script Widget Widget Angular Provider
Possible use of private data	Warning	Access control Client script Catalog client scripts Email script Inbound email action Record producer Script action Script include Scripted rest resource Table transform map Transform script UI Action UI Script Widget Widget Angular Provider

JavaScript – Avoid making connections on unsafe protocols	Warning	Access control Business rules Client script Catalog client scripts Email script Inbound email action Record producer Script action Script include Scripted rest resource Table transform map Transform script UI Action UI Script Widget Widget Angular Provider
Business Rules using eval function	High	Business rules
Possible extra-sensitive PII usage in configuration element – Gender	High	Business rules Client script Catalog client script Dictionary Script include Script action Scripted rest resource
Possible extra-sensitive PII usage in configuration element – Religion	High	Business rules Client script Catalog client script Dictionary Script include Script action Scripted rest resource

Possible PII usage in configuration element – Email	Warning	Business rules Client script Catalog client script Dictionary Inbound email action Script action Script include Scripted rest resource
Possible PII usage in configuration element – Address	Warning	Business rules Client script Catalog client script Dictionary Inbound email action Script action Script include Scripted rest resource
Possible PII usage in configuration element – Nationality	Warning	Business rules Client script Catalog client script Dictionary Inbound email action Script action Script include Scripted rest resource
Possible PII usage in configuration element – Passport	Warning	Business rules Client script Catalog client script Dictionary Inbound email action Script action Script include Scripted rest resource

JavaScript – Avoid use of Eval function	High	Client script Catalog client scripts Record producer Scripted rest resource UI Script Widget Widget Angular Provider
Javascript – Avoid use of local storage on Client Scripts	High	Client script Catalog client scripts UI Action UI Script Widget Widget Angular Provider
Possible use of private data – Catalog UI Policy scriptFalse	Warning	Catalog UI policy
Possible use of private data – Catalog UI Policy scriptTrue	Warning	Catalog UI policy
JavaScript – Avoid use of Function Constructors – Catalog UI Policy scriptFalse	High	Catalog UI policy
JavaScript – Avoid use of Function Constructors – Catalog UI Policy scriptTrue	High	Catalog UI policy
JavaScript – Avoid making connections on unsafe protocols – Catalog UI Policy scriptFalse	Warning	Catalog UI policy
JavaScript – Avoid making connections on unsafe protocols – Catalog UI Policy scriptTrue	Warning	Catalog UI policy
JavaScript – Avoid unrestricted targetOrigin on cross-domain messaging – Catalog UI Policy scriptFalse	High	Catalog UI policy
JavaScript – Avoid unrestricted targetOrigin on cross-domain messaging – Catalog UI Policy scriptTrue	High	Catalog UI policy

JavaScript – Avoid use of debugger statements – Catalog UI Policy scriptFalse	High	Catalog UI policy
JavaScript – Avoid use of debugger statements – Catalog UI Policy scriptTrue	High	Catalog UI policy
JavaScript – Avoid use of WebDB – Catalog UI Policy scriptFalse	High	Catalog UI policy
JavaScript – Avoid use of WebDB – Catalog UI Policy scriptTrue	High	Catalog UI policy
Possible use of private data – UI Policy scriptFalse	Warning	UI Policy
Possible use of private data – UI Policy scriptTrue	Warning	UI Policy
JavaScript – Avoid use of Function Constructors – UI Policy scriptFalse	High	UI Policy
JavaScript – Avoid use of Function Constructors – UI Policy scriptTrue	High	UI Policy
JavaScript – Avoid making connections on unsafe protocols – UI Policy scriptFalse	Warning	UI Policy
JavaScript – Avoid making connections on unsafe protocols – UI Policy scriptTrue	Warning	UI Policy
JavaScript – Avoid unrestricted targetOrigin on cross-domain messaging – UI Policy scriptFalse	High	UI Policy
JavaScript – Avoid unrestricted targetOrigin on cross-domain messaging – UI Policy scriptTrue	High	UI Policy
JavaScript – Avoid use of debugger statements – UI Policy scriptFalse	High	UI Policy
JavaScript – Avoid use of debugger statements – UI Policy scriptTrue	High	UI Policy
JavaScript – Avoid use of WebDB – UI Policy scriptFalse	High	UI Policy
JavaScript – Avoid use of WebDB – UI Policy scriptTrue	High	UI Policy
JavaScript – Avoid use of WebDB	High	Script include
AngularJS – Denial of Service attack through DOM clobbering on versions under 1.6.3	High	UI Script
AngularJS – Prototype Pollution Vulnerability under 1.7.9	High	UI Script

AngularJS – XSS vulnerability through the attribute “usemap” from 1.0.0 to 1.2.30	High	UI Script
AngularJS – XSS vulnerability through the attribute “usemap” from 1.3.0 to 1.5.0-rc2	High	UI Script
AngularJS – XSS vulnerability under 1.8.0 – input HTML	High	UI Script
AngularJS – XSS vulnerability using AngularJS under 1.6.5 in Firefox and Safari – sanitize on inert Documents	High	UI Script
AngularJS – XSS vulnerability using AngularJS under 1.6.9 with Firefox	High	UI Script
jQuery – Prototype Pollution Vulnerability under 3.4.0	High	UI Script
jQuery – XSS vulnerability under 1.6.3, when using location.hash	High	UI Script
jQuery – XSS vulnerability under 1.9.0, when using jQuery(strInput)	High	UI Script
jQuery – XSS vulnerability under 3.0.0, when making cross-domain calls without the dataType option	High	UI Script
jQuery – XSS vulnerability under 3.5.0, when using htmlPrefilter	High	UI Script
jQuery-ui-dialog – XSS vulnerability under 1.10.0, closeText parameter	High	UI Script
jQuery-ui-dialog – XSS vulnerability under 1.10.0, title attribute	High	UI Script
moment.js – Regular Expression Denial of Service Vulnerability	High	UI Script
XSS vulnerability in Ext JS Action Column getTip	High	UI Script
The “Security Manager” System Property is set to “Allow Access”	High	System property
SOAP Request Strict Security should be enabled	High	System property
SSLv2/SSLv3 should be disabled	High	System property
Escape Jelly should be enabled	High	System property
Escape HTML should be enabled	High	System property
Enable AJAXEvaluate should be disabled	High	System property
AJAXGlideRecord ACL Checking should be enabled	High	System property

“Check UI Action Conditions check before Execution” should be enabled	High	System property
Escape XML should be enabled	High	System property
Client Generated Scripts Sandbox should be enabled	High	System property
HTML Sanitizer property should be enabled	High	System property
Java Package Collection mode and Collection mode override properties should be disabled	High	System property
Cookies – HTTP Only should be enabled	High	System property
CSV Request Authorization should be enabled	High	System property
Basic Auth SOAP Requests setting should be enabled	High	System property
Old UI enabled or being used	High	System property
Script Request Authorization should be enabled	High	System property
“Allow Javascript tags in Embedded HTML” property should be disabled	High	System property
The sn_hr_core.impersonateCheck System Property is false	High	System property
Anti-CSRF Token setting should be enabled	High	System property
High Security Settings plugin disabled	High	Inactive security plugins
Contextual Security Plugin disabled	High	Inactive security plugins
GlideRecord API usage in Scripted REST API Resource	High	Scripted rest resource
REST API Resource modifying data without Authentication check	High	Scripted rest resource
REST API Resource modifying data without Authentication check – No Author	High	Scripted rest resource