Script Action Rules

By Configuration Element · https://community-staging.qualityclouds.com/qcdocs/qc/by-configuration-element/script-action-rules/

The below table shows the list of ServiceNow script action rules that are checked by Quality Clouds.

Description	Severity	Area of impact
Possible extra-sensitive PII usage in configuration element - Gender	High	Security
Possible extra-sensitive PII usage in configuration element - Religion	High	Security
Possible use of private data	Warning	Security
Possible PII usage in configuration element - Nationality	Warning	Security
Possible PII usage in configuration element - Address	Warning	Security
Possible PII usage in configuration element - Email	Warning	Security
Possible PII usage in configuration element - Passport	Warning	Security
JavaScript - Avoid use of Function Constructors	High	Security
JavaScript - Avoid use of WebDB	High	Security
JavaScript - Avoid use of debugger statements	High	Security
JavaScript - Avoid unrestricted targetOrigin on cross-domain messaging	High	Security
JavaScript - Avoid making connections on unsafe protocols	Warning	Security
JavaScript - Optimize Loops	Warning	Performance
JavaScript - Use === comparison	Warning	Manageability
Event Script Action with hard-coded sys_ids	Medium	Manageability
Event Script Action using GlideRecord and getRowCount	Medium	Scalability
Modified Out of the Box Element	Warning	Scalability