Scripted Rest Resource Rules

By Configuration Element · https://community-staging.qualityclouds.com/qcdocs/qc/by-configuration-element/scripted-rest-resource-rules/

The below table shows the list of ServiceNow service catalog best practices that are checked by Quality Clouds.

See the Scripted REST API Best Practices for designing and implementing scripted rest APIs.

Description	Severity	Area of impact
REST API Resource modifying data without Authentication check	High	Security
REST API Resource modifying data without Authentication check - No Author	High	Security
GlideRecord API usage in Scripted REST API Resource	High	Security
Possible extra-sensitive PII usage in configuration element - Gender	High	Security
Possible extra-sensitive PII usage in configuration element - Religion	High	Security
JavaScript - Avoid use of Eval function	High	Security
JavaScript - Avoid use of debugger statements	High	Security
JavaScript - Avoid use of Function Constructors	High	Security
JavaScript - Avoid unrestricted targetOrigin on cross-domain messaging	High	Security
Possible use of private data	Warning	Security
Possible PII usage in configuration element - Email	Warning	Security
Possible PII usage in configuration element - Address	Warning	Security
Possible PII usage in configuration element - Nationality	Warning	Security
Possible PII usage in configuration element - Passport	Warning	Security
JavaScript - Avoid making connections on unsafe protocols	Warning	Security

Scripted REST API Resource with hard-coded sys_ids	Medium	Manageability
JavaScript - Use === comparison	Warning	Manageability
JavaScript - Optimize Loops	Warning	Performance
Modified Out of the Box Element	Warning	Scalability