To make the Pega Platform applications more secure, you can run the Rule Security Analyzer. This tool searches through non-auto generated rules to find specific javascript or SQL coding patterns that might indicate a security vulnerability.

To use the analyzer, you must have the pxSecurityVA privilege in your access group’s role. Standard developer rules such as SysAdmn4 includes this privilege

We also have to note that

Rule Security Analyzer tool examines only custom code, not autogenerated rules

Blocked rules are ignored. These rules are identified by the property .pyRuleAvailable = ‘Blocked’

The tool scans rules in your own applications, not rules in standard Pega 7 rulesets.

The rule security analyzer searches for vulnearbilities in code by searching for matches to regular expressions rules. The system provides the following standard regular expressions

pyCrossSiteScripting

pyCrossSiteScriptingFromParam

pyCssInLink

pyScriptJS

pyUnsafeURL

All these are available in the wizard can navigate as shown below

A screenshot of a computer

Description automatically generated

Now after using it Click on ‘Run Analyzer’ on the right side we can see the search statistics where it will show the total vulnerable rules per total rules searched

If anything vulnerable it will show as 1/4 as in the above example so one harness rule is unsafe.

A screenshot of a computer

Description automatically generated



A screenshot of a computer

Description automatically generated

That is the rule security analyzer. It will basically show the vulnerabilities of the rules on the application.