NativeSPRequestMapQuery

The <Query> element is used to apply content rules to requests containing specific query string parameters.

⚠ Query string matching can be difficult, because the client totally dictates the information, and case matters. It should be used only when the case of the parameter name is significant to the application consuming it, because then the client can bypass your rule, but not actually get the application to run.

⚠ Up to version 2.4 POST data is lost in an HTTP POST requests with query strings due to a bug in the CGI parser. HTTP GET requests with a query string only or HTTP POST request without query strings should however work fine.

Attributes

Content Specifiers

- `name` (string)
  - Required, the name of the parameter that must be present to match. Parameter names are case-sensitive.
- `regex` (string)
  - Optional, specifies a regular expression that must match one of the parameter's values. If omitted, the mere presence of a value for the named parameter is sufficient for a match.

Find below a real-Ifile example for a <Query> element that is used to protect specific pages in a Dokuwiki instance. This example enforces a Shibboleth session on https://www.example.org/doku.php and only users with the given affiliation will be able to access URLs like https://www.example.org/doku.php?id=internal or https://www.example.org/doku.php?id=internal:subdirectory. Please note that the `AccessControl` rule only is enforced for a URL that starts with /doku.php

```
<RequestMap applicationId="default">
    <Host name="www.example.org">
        <Path name="doku.php" authType="shibboleth" requireSession="true"/>
            <Query name="id" regex="^internal.*">
                <AccessControl>
                        <Rule require="affiliation">faculty@osu.edu student@osu.edu</Rule>
                </AccessControl>
            </Query>
        </Path>
    </Host>
</RequestMap>
```

Content Settings

XML attributes corresponding to request mapper properties are used.

Child Elements

Access Control

One of the following elements can be used to attach an access control policy to the resource. This is a violation of the axiom that the SP doesn't do access control, but it's really just a call-out that has some predefined plugins you can use as examples to create more.

- `<htaccess>`
  - Enables Apache `.htaccess` support during the authorization phase. This is automatic and implicit for the "Native" request mapper, but can be enabled by hand if the "XML" request mapper is used. Note that this will fail for non-Apache servers.
- `<AccessControlProvider>`
  - Attaches a custom access control policy supported by a plugin.
- `<AccessControl>`
  - Attaches an access control policy using the sample XML-based plugin provided with the SP. This is just a short-hand for embedding the policy in the element above, if you want the policy inside the same file.

If no element is included (or inherited or implicitly enabled), any access control is left to the resource.

If an error occurs when processing this element, a dummy policy to deny access is installed to prevent accidental exposure.

Nested Content Specifiers

- `<Query>`
    - Matches requests containing a query string parameter satisfying the element.

Unlike paths, query strings aren't nested, but nesting the element allows for a conjunction between the parent element and the child. Sibling elements, meanwhile, form a disjunction.

For more details on how the request mapping process works, see the request mapper HOWTO.