ITRS OP5 Monitor XSS Vulnerability

Summary

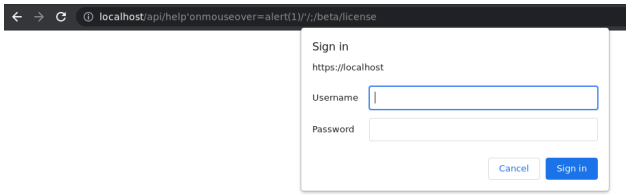
An un-authenticated user can trigger a reflected cross site scripting vulnerability on the /api/help route of the OP5 Monitor page. Versions 8.3.0 to 8.3.3 were the only versions tested and found to be vulnerable but potentially all versions from 7.5.x onwards may suffer from the same vulnerability.

Proof of Concept

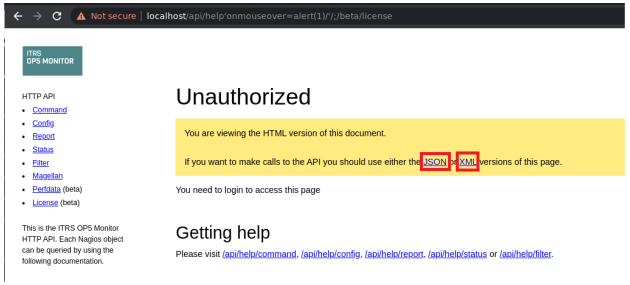
The following uses the ubiquitous "alert(1)" function to demonstrate the vulnerability:

Navigate to https://localhost/api/help'onmouseover=alert(1)/';/beta/license (the local machine is hosting the op5 monitor for demonstration purposes).

When prompted for login credentials click cancel and continue to the "Unauthorized" API help page:

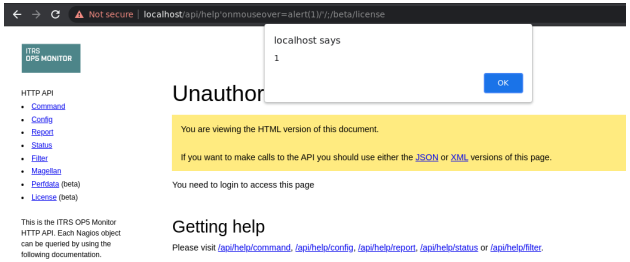


"Cancel when prompted"



"Unauthorized help page"

Mouse over on the "JSON" or "XML" links on the help page to trigger the XSS vulnerability



"alert(1)"