matthieu-hackwitharts Update calendar_xss.md History

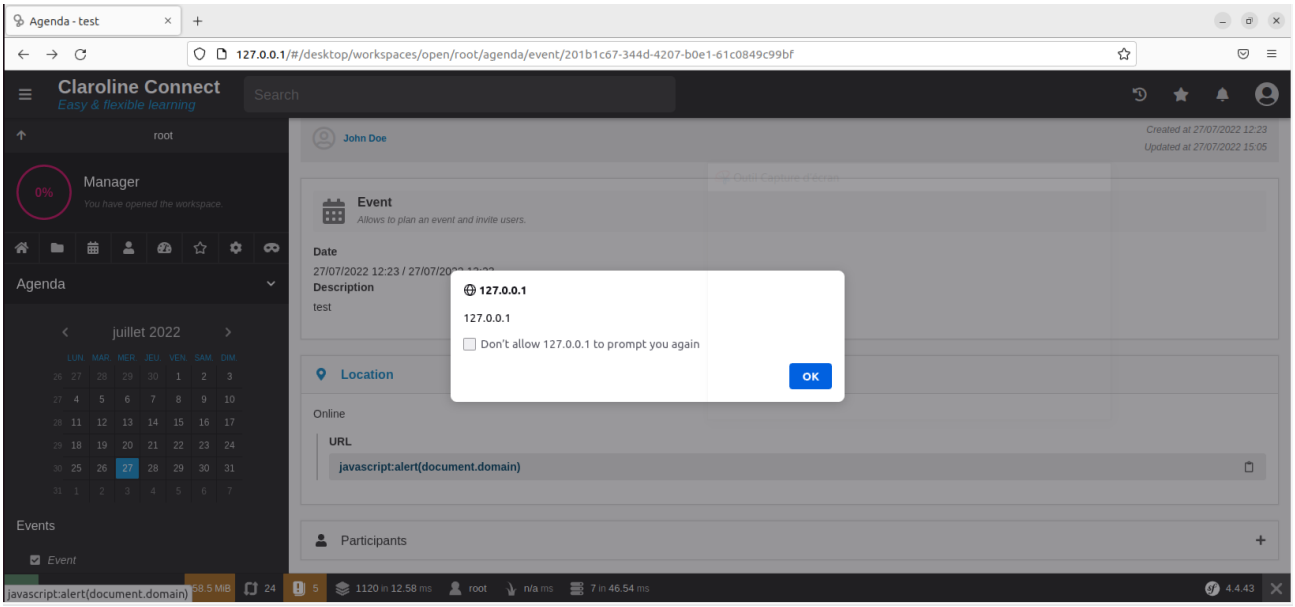
1 contributor

13 lines (8 sloc) | 665 Bytes

'Location' stored XSS (CVE-2022-37162)

Claroline Connect suffers from a stored xss vulnerability in 'Calendar' functionality. By adding a specific payload in the `Location` of an event, an attacker can trigger an xss.

User input is reflected as an href attribute in the `Location` parameter. Therefore it is possible to enter a payload like `javascript:alert(document.domain)` to execute some javascript code.



Fix suggestion : apply XSS filters on user input, and check if the entered content is a real URL.