matthieu-hackwitharts Update csrf.md History

1 contributor

13 lines (6 sloc) | 636 Bytes

Admin account takeover (CSRF) via XSS because of arbitrary file upload (CVE-2022-37160)

Claroline Connect is affected by a CSRF vulnerability, because of missing CSRF tokens or other protection means. This CSRF can be triggered via the Claroline's API, by combining an XSS vulnerability (like svg maybe ?) with a fetch request to the API. An arbitrary user with admin rights can be created by triggering the XSS from an admin user.

Example of POC :

Fix suggest : adding CSRF tokens or other protection way.