Cross site scripting in Collabtive (CVE-2020-13655)

A cross site scripting vulnerability is present in Collabtive 3.0 and later (including the latest version, 3.1)

We contacted the developers for a disclosure on May 4th 2020, but as of August 24th 2020, we didn't receive any answer after multiple followups.

The vulnerability was found automatically by the NAVEX project, in the file managefile.php[https://github.com/philippK-de/Collabtive/blob/master/managefile.php], around line 296. Here's the relevant code snippet:

```
$action = getArrayVal($_GET, "action");

/* Not relevant code omitted... */

elseif ($action == "movefile") {
    /* Not relevant code omitted... */

    $file = $_GET["file"];
   // $file = substr($file, 4, strlen($file)-4);

    $target = $_GET["target"];
    echo "$target $file";
    echo  $fileObj->moveFile($file, $target);
```

This endpoint is meant to be called by Javascript code in the frontend, and returns some text as a feedback to the user of the status of the requested operation.

However, due to the lack of CSRF protection, and the (default) setting of the Content-Type header to text/html, an attacker can craft a malicious URL which, when visited, will reflect the file and target variables without any escaping, thus executing JavaScript code.