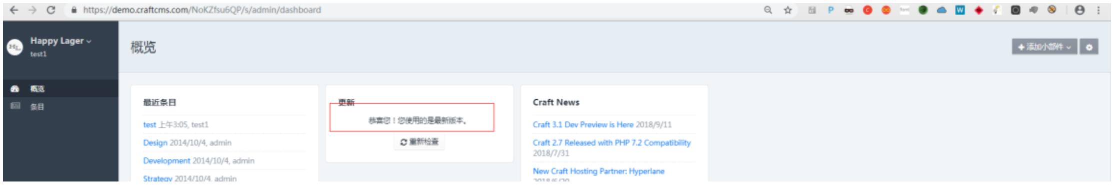
Prepare

First get your own craft demo site(https://demo.craftcms.com/NoKZfsu6QP/s/),then add a test account, he just can only edit related items.



https://demo.craftcms.com/NoKZfsu6QP/s/admin/dashboard

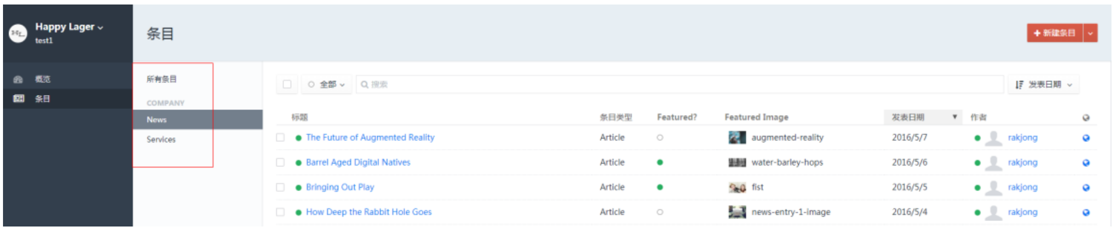
Happy Lager
test1

概览

最近条目
test 上午3:05, test1
Design 2014/10/4, admin
Development 2014/10/4, admin
Strategy 2014/10/4, admin

更新
恭喜您！您使用的是最新版本。

Craft News
Craft 3.1 Dev Preview is Here 2018/9/11
Craft 2.7 Released with PHP 7.2 Compatibility 2018/7/31
New Craft Hosting Partner: Hyperlane



Happy Lager
test1

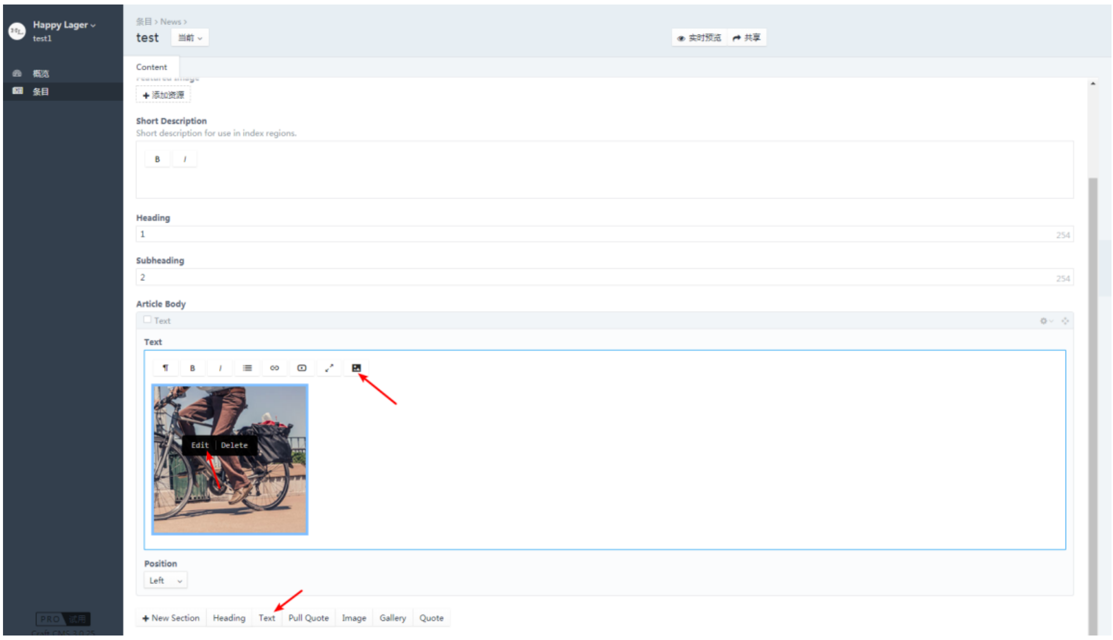
条目

所有条目
COMPANY
News
Services

标题	条目类型	Featured?	Featured Image	发表日期	作者
The Future of Augmented Reality	Article	○	augmented-reality	2016/5/7	rakjong
Barrel Aged Digital Natives	Article	●	water-barley-hops	2016/5/6	rakjong
Bringing Out Play	Article	●	fist	2016/5/5	rakjong
How Deep the Rabbit Hole Goes	Article	○	news-entry-1-image	2016/5/4	rakjong

PoC

1, Log in with an account that only has editing Permission.
2, Edit a news, add a text edit box, then choose to add a picture, just select one from the system.



条目 > News >
test

Content

Short Description
Short description for use in index regions.

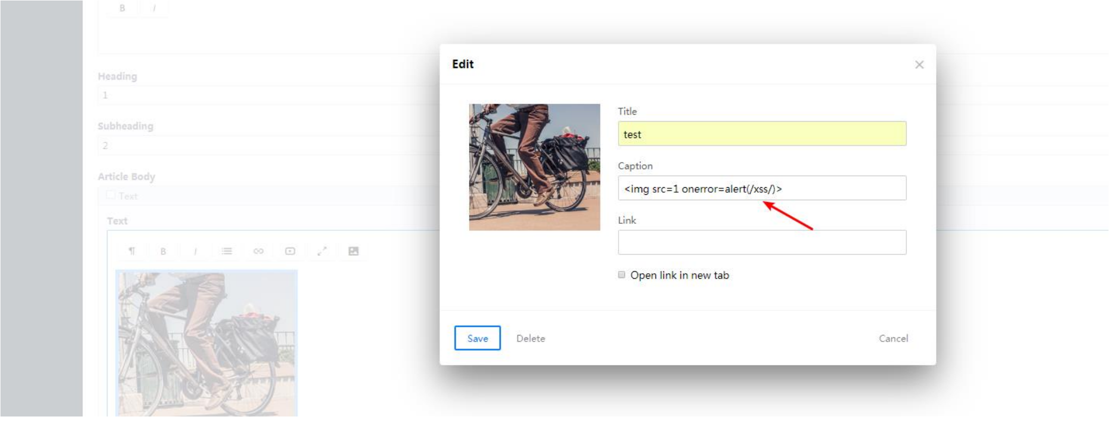
Heading
1

Subheading
2

Article Body
Text

Position
Left

3, Click edit to edit the image, insert the xss code in Caption and click save.
code:<img src=1 onerror=alert(/xss/)>



Edit

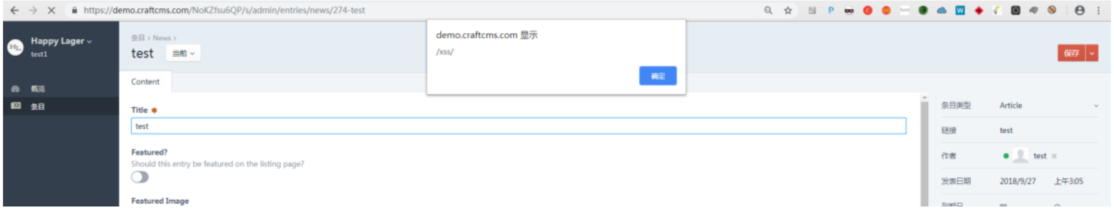
Title: test

Caption: <img src=1 onerror=alert(/xss/)>

Link:

□ Open link in new tab

4, We can see that the xss code is executed. Any users accessing this news after saving news will be attacked by xss (including system administrator).



https://demo.craftcms.com/NoKZfsu6QP/s/admin/entries/news/274-test

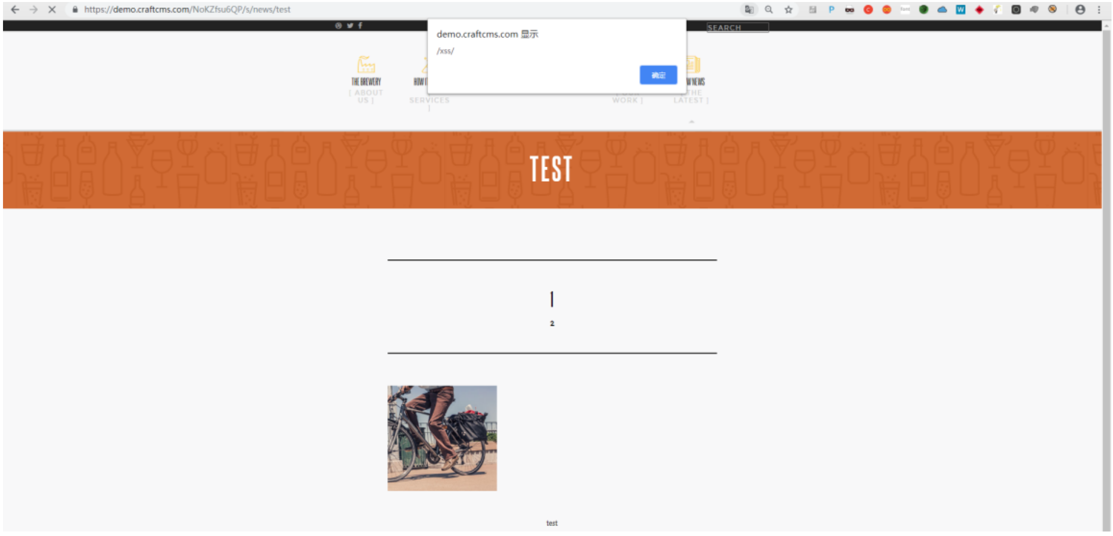
demo.craftcms.com 显示
/xss/

Title: test

Featured?
Should this entry be featured on the listing page?

Featured Image

条目类型	Article
链接	test
作者	test
发表日期	2018/9/27 上午3:05



https://demo.craftcms.com/NoKZfsu6QP/s/news/test

demo.craftcms.com 显示
/xss/