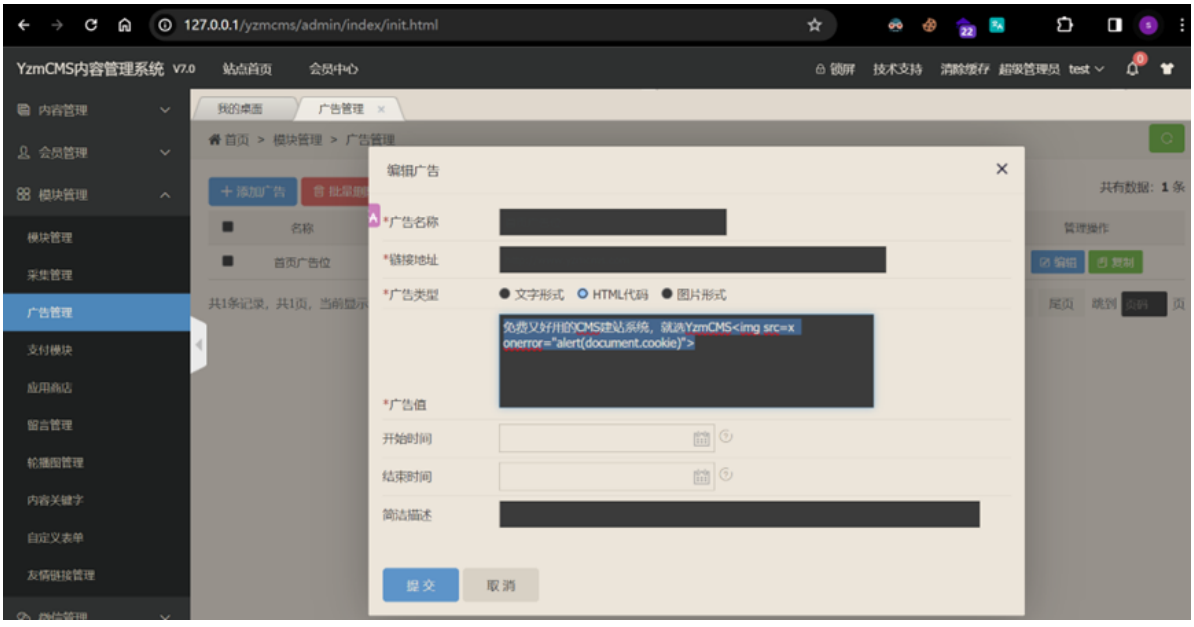
YZMCMS(v7.0) has multiple vulnerabilities， Cross Site Scripting(XSS)

The YzmCMS v7.0 content management system has multiple storage-optimized XSS vulnerabilities.
The vulnerability detection process is as follows:

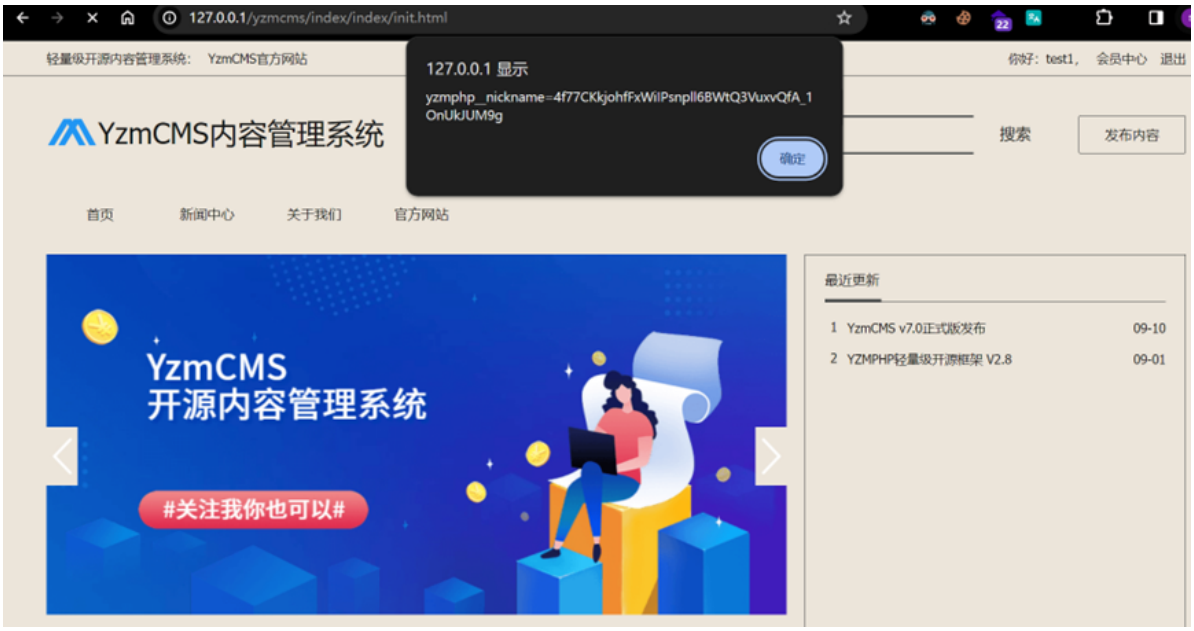
Location of the vulnerability: Module Management -> Ads Management

1、Click Edit and select HTML as the ad type.

```
payload1:<img src=x onerror="(‘asen-xss’)">
payload2:<img src=x onerror="alert(document.cookie)">
```

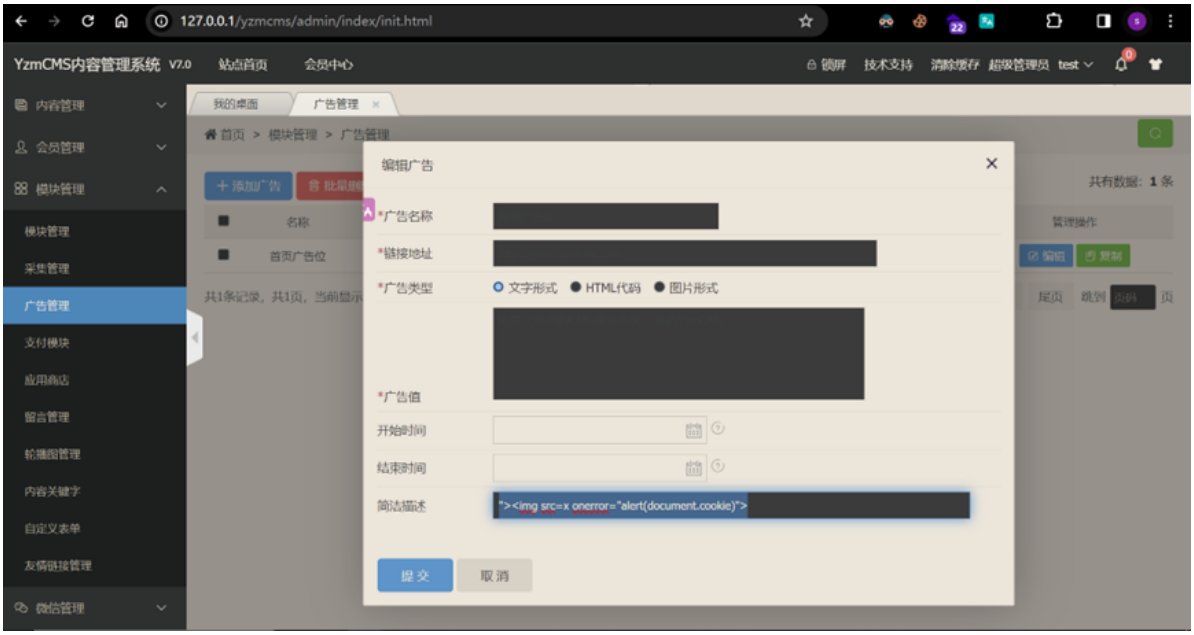


Registered members test1, triggered after visiting the homepage.



2、In the edit ad, select any ad type, and there is a stored XSS in the concise description.

```
payload:"><img src=x onerror="alert(document.cookie)">
```

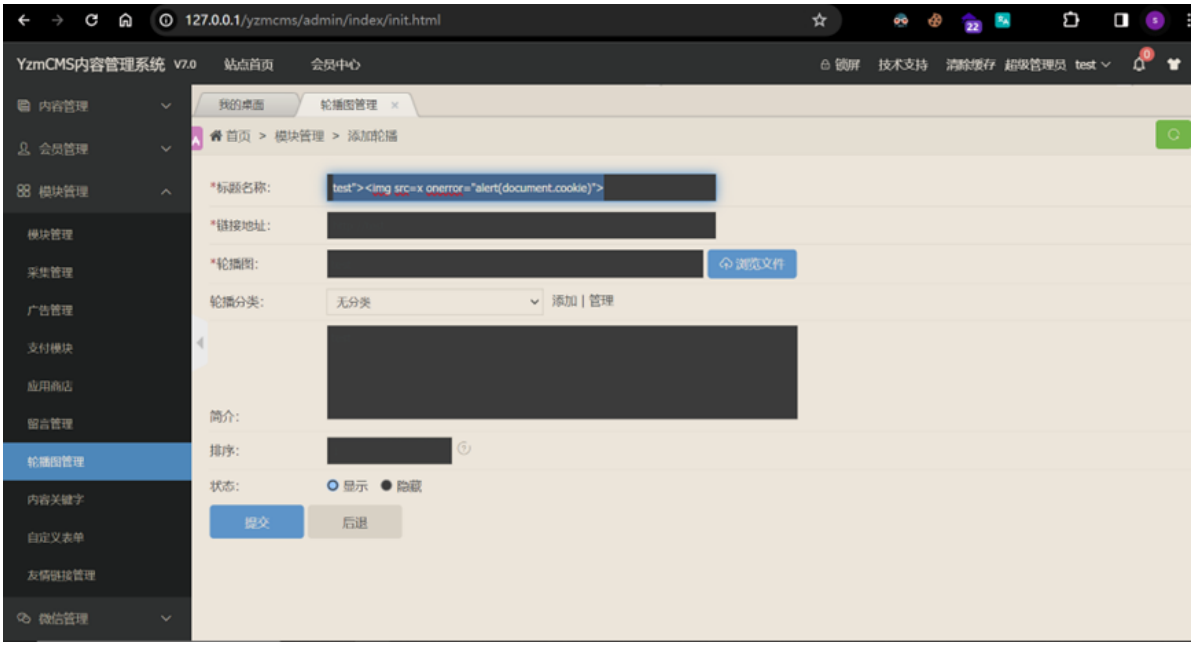


Triggered when this ad is edited.

Location of the vulnerability: Module Management - > Carousel Management - > Add Carousel - > Edit

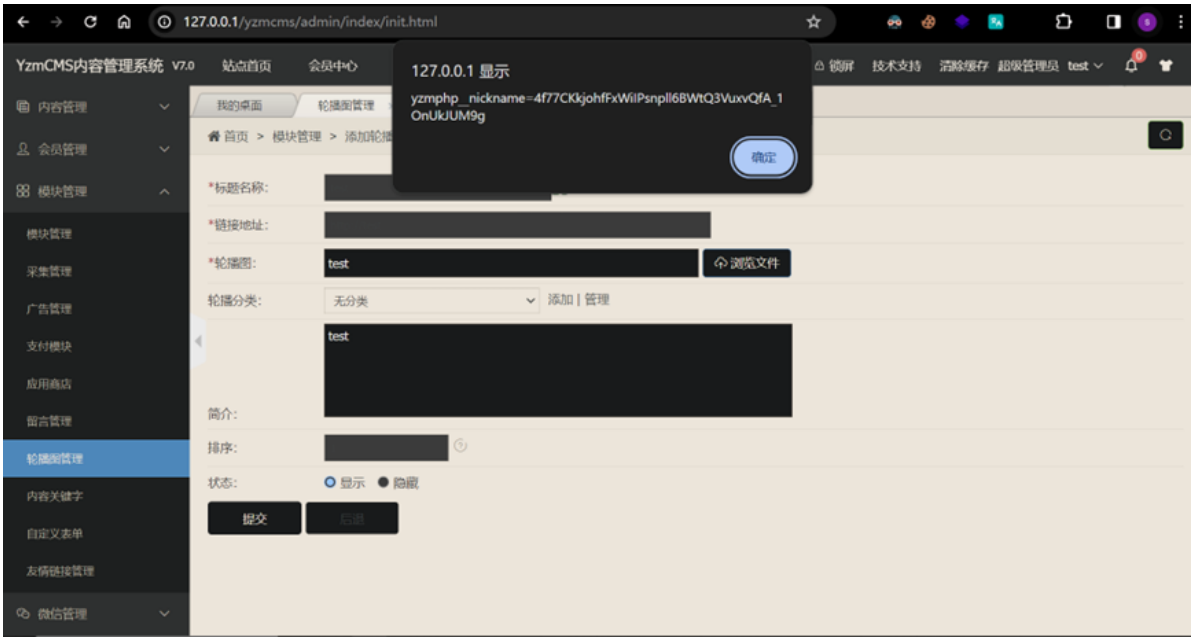
1、Stored XSS instances exist in the title name.

```
payload: test"><img src=x onerror="alert(document.cookie)">
```



After saving, it is triggered by accessing the carousel management interface.

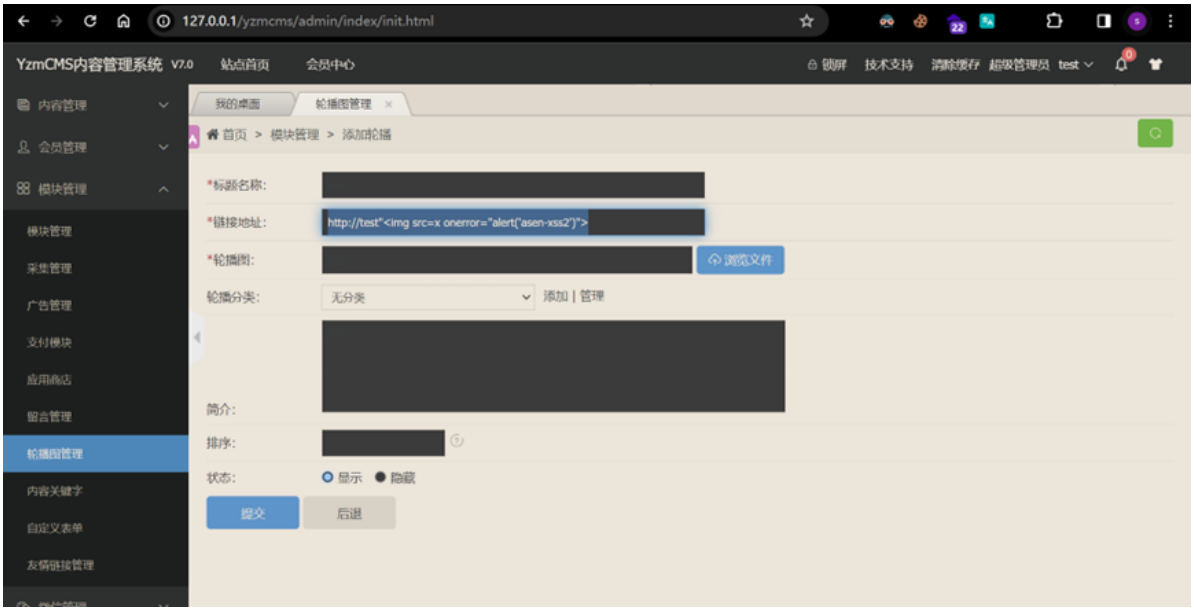
Editing the corresponding carousel is also triggered.

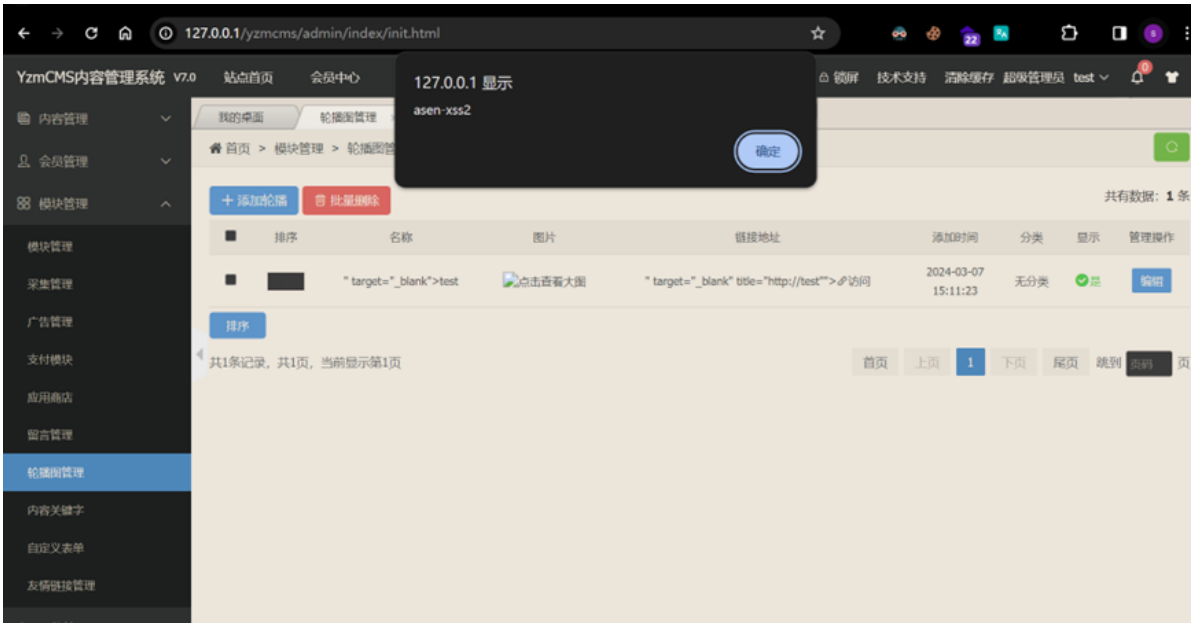


2、XSS is stored at the link address, which cannot be changed after being written, and the malicious code can only be eliminated by deleting the carousel.

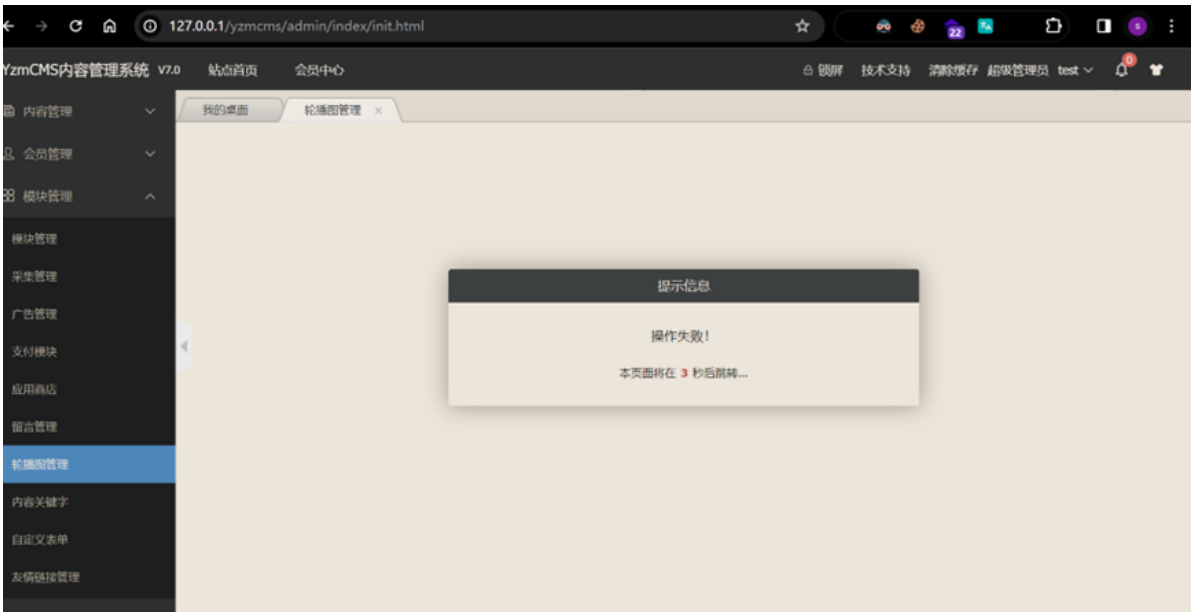
(1) XSS is triggered only once.

```
payload: http://test"<img src=x onerror="alert('asen-xss2')">
```





At this point, we went to modify the link address again, and found that the change failed anyway.

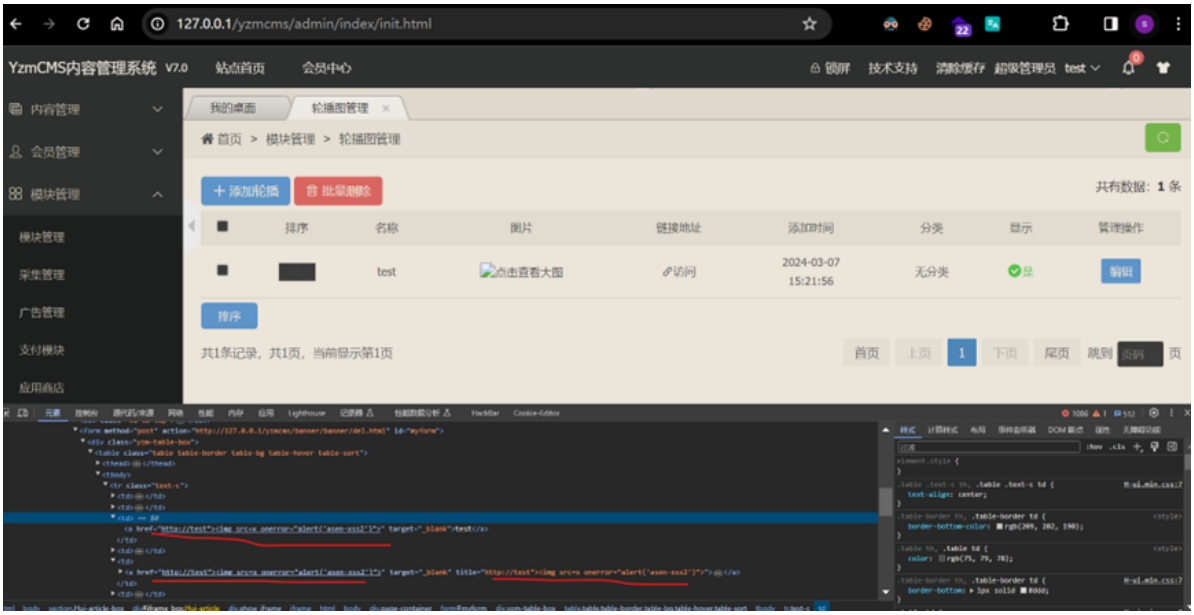


(2) XSS is triggered multiple times.

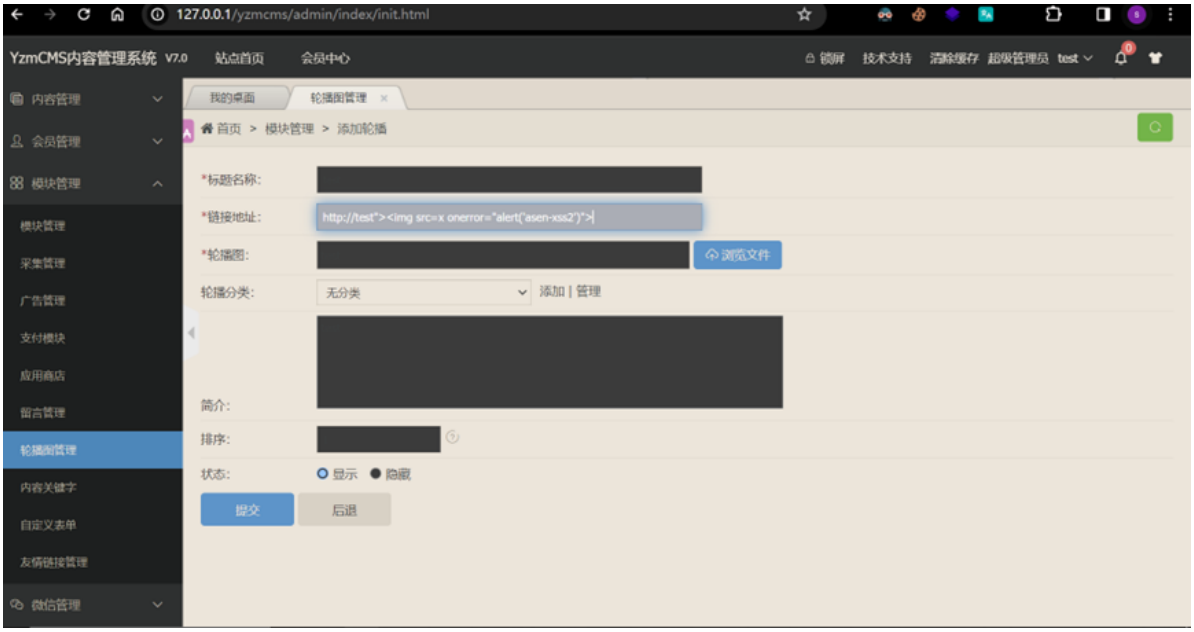
```
payload: test"><img src=x onerror="alert(document.cookie)">
```

If you enter payload twice at the link address, the first XSS will not be triggered, and after the second entry is saved, the carousel management will trigger multiple XSS, and the editing will also trigger multiple XSS.

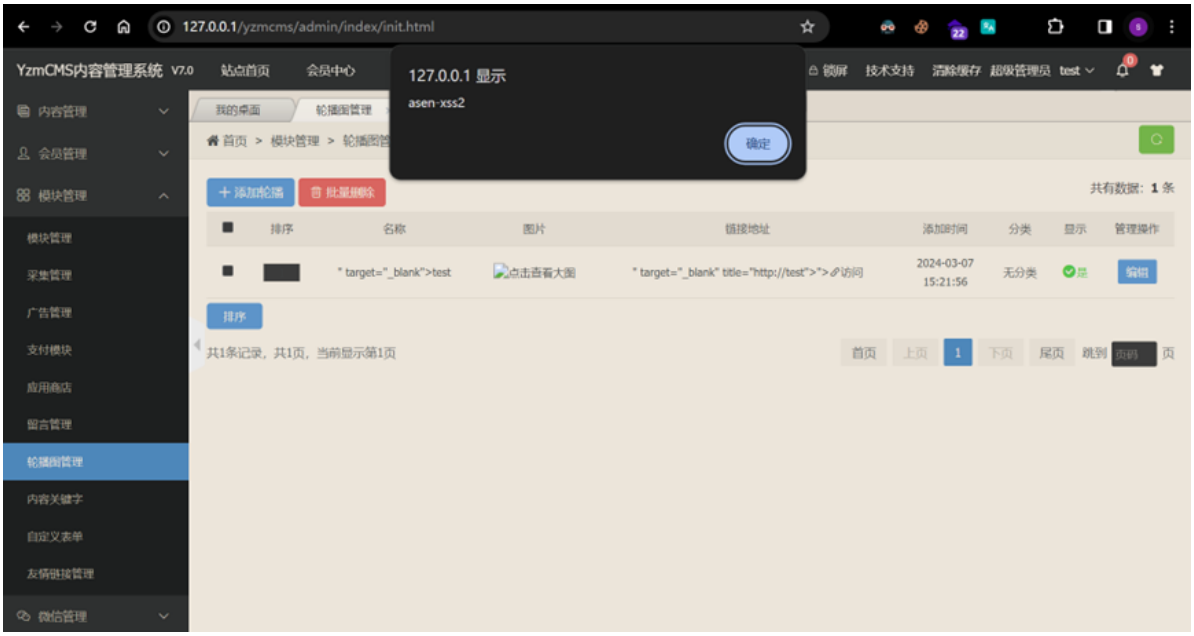
After the first entry, the result:

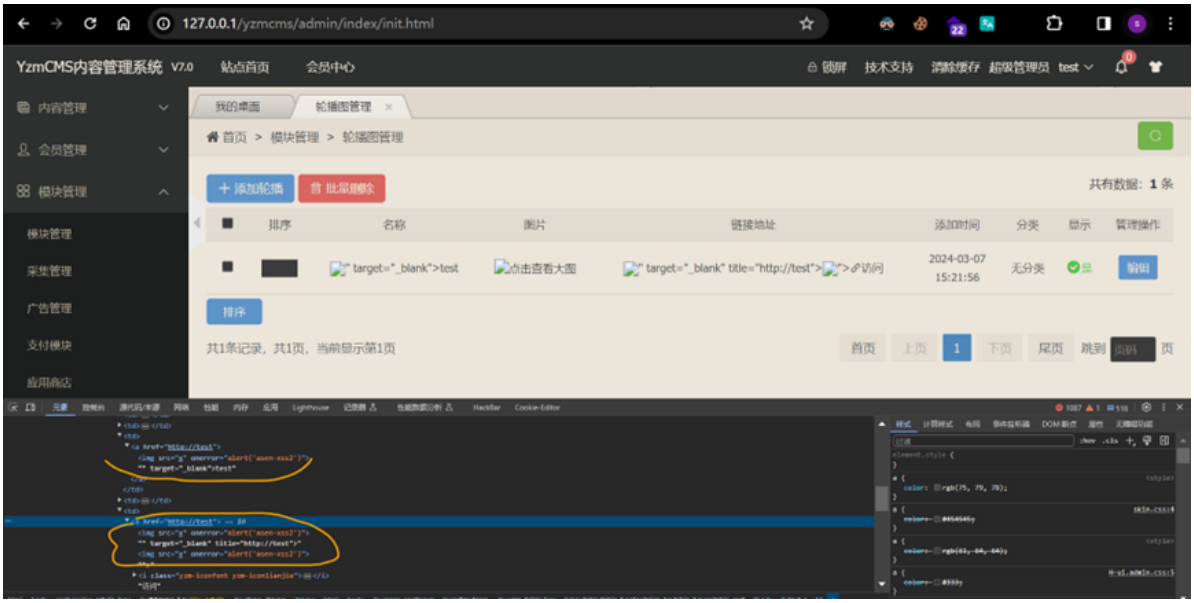


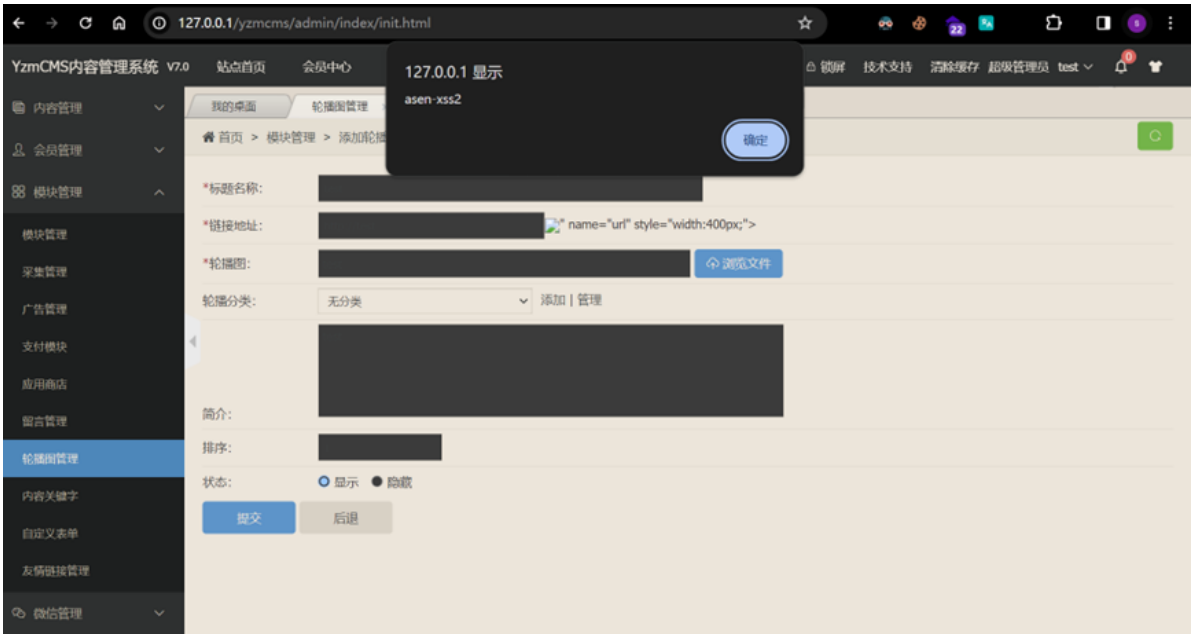
Second Input:



The result of the second input after saving:

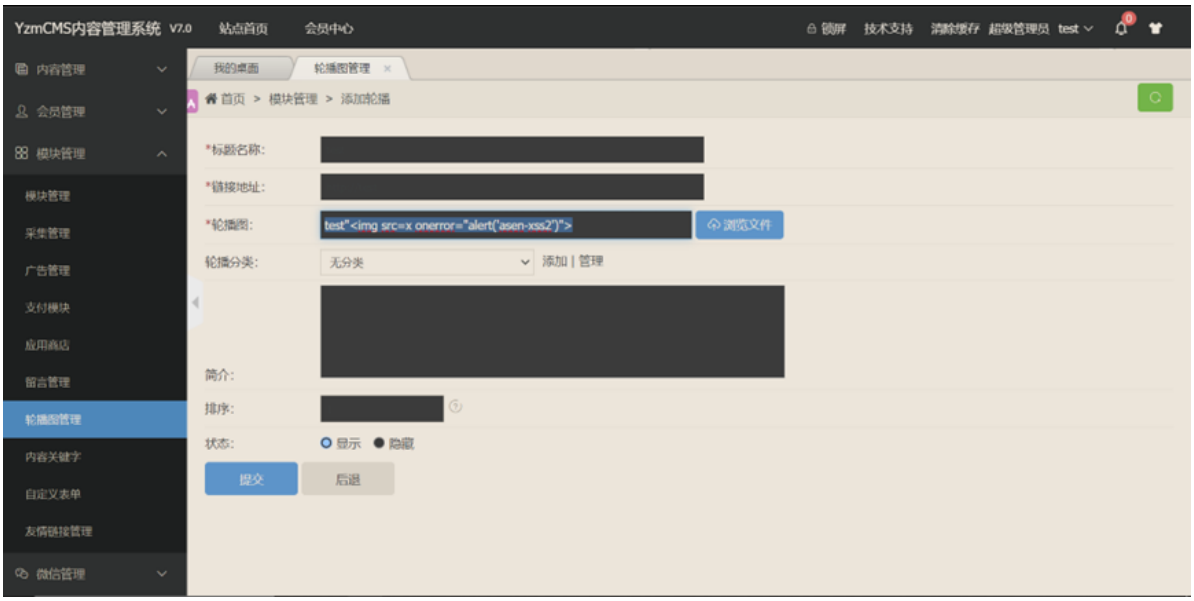


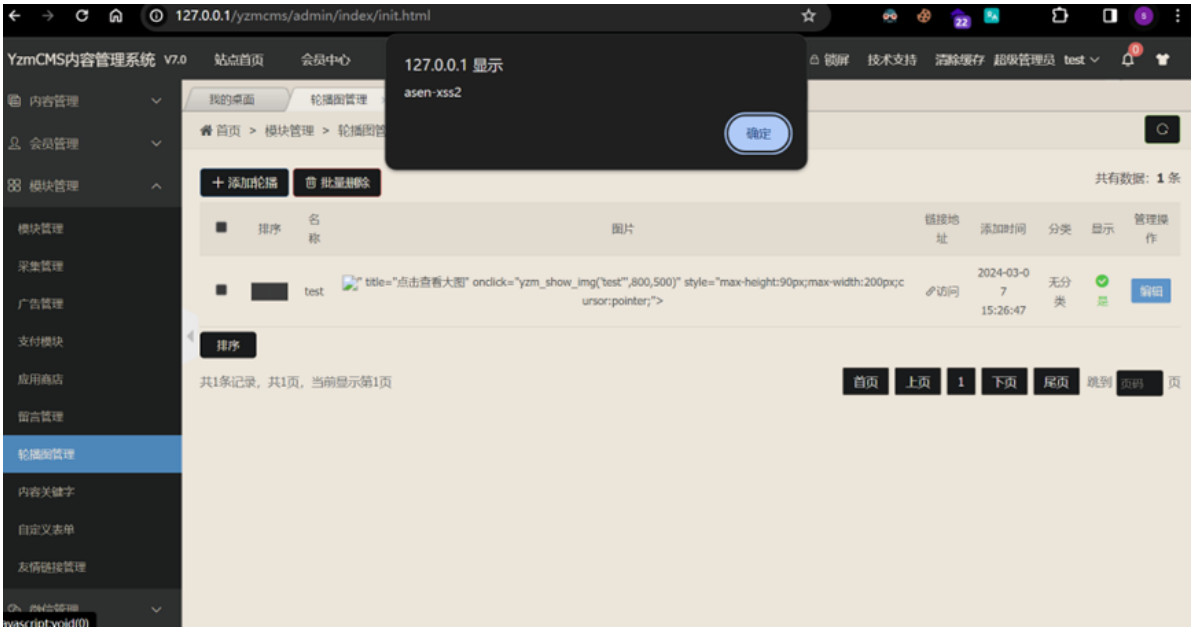




3、The carousel in the edit has xss stored in it.

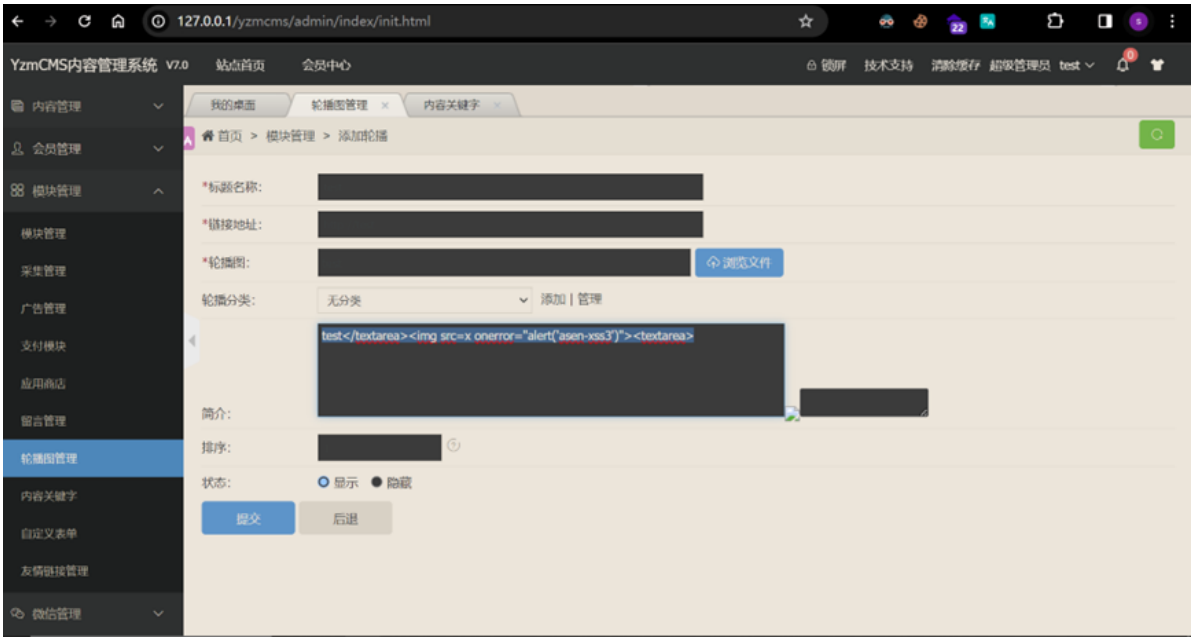
```
payload: test"<img src=x onerror="alert('asen-xss2')">
```



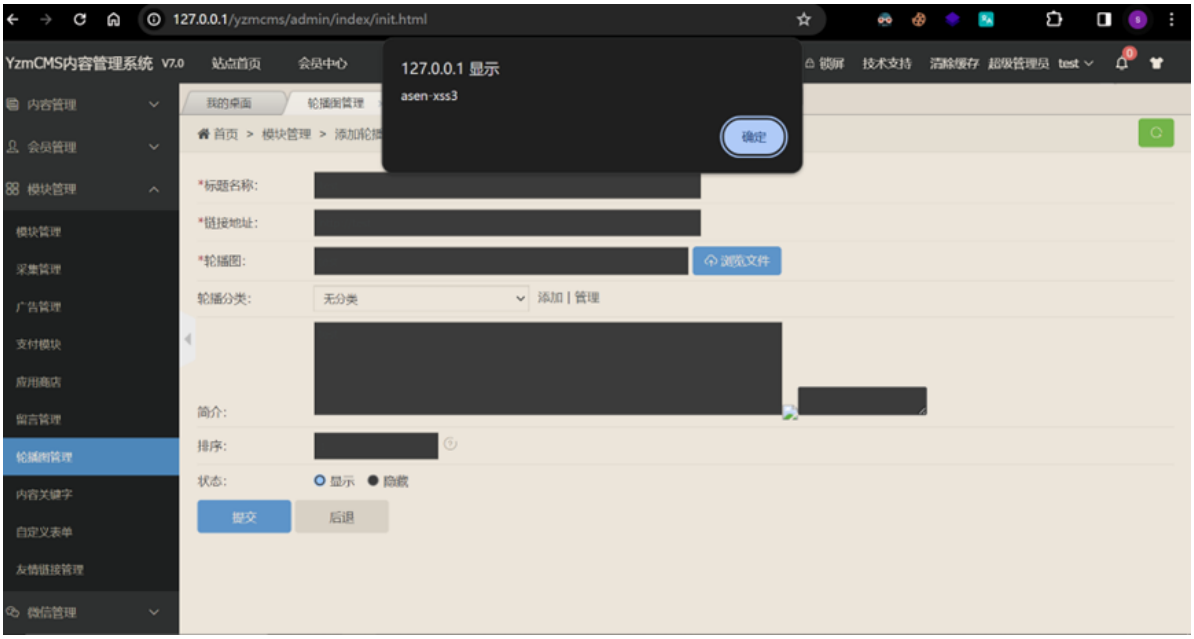


4、Edit - > briefly states that there is a storage XSS

```
payload: test</textarea><img src=x onerror="alert('asen-xss3')"><textarea>
```



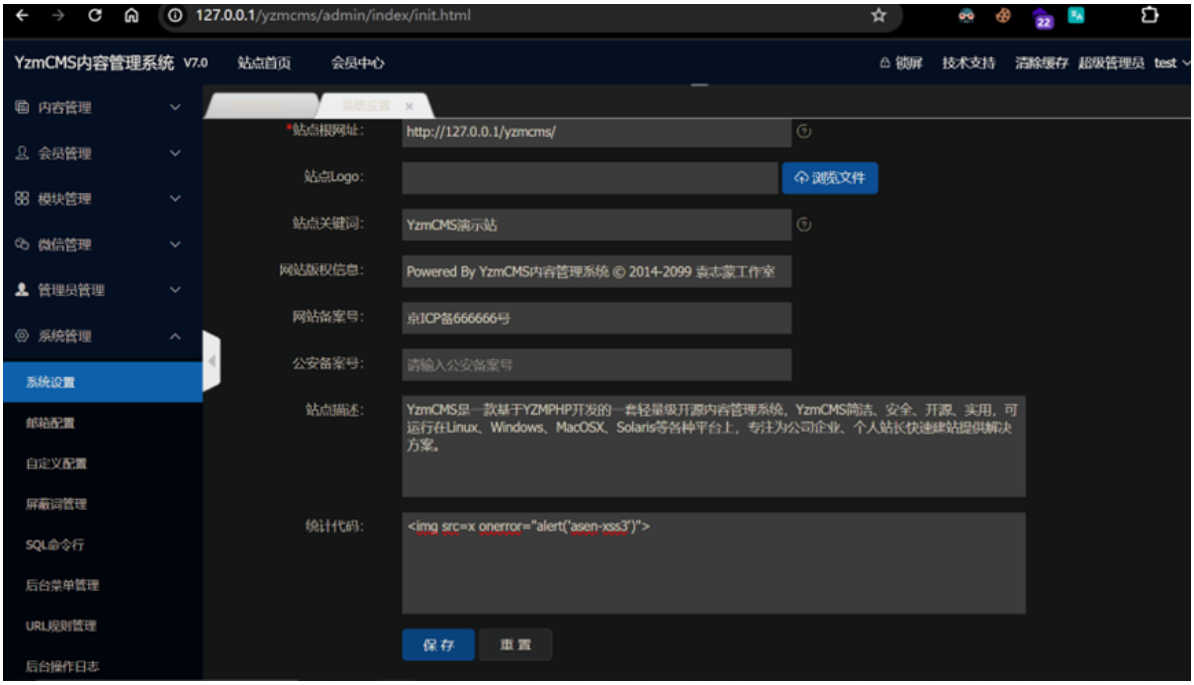
Once submitted, click Edit in this carousel again to trigger it.



Location of the vulnerability: Background Management - > System Management - > System Settings

1、Basic Settings - > at the statistics code

```
payload:<img src=x onerror="alert('asen-xss3')">
```



Triggered when you visit the homepage.

Suggestion: The vendor changed the code to filter the input parameters.