New issue

Jump to bottom

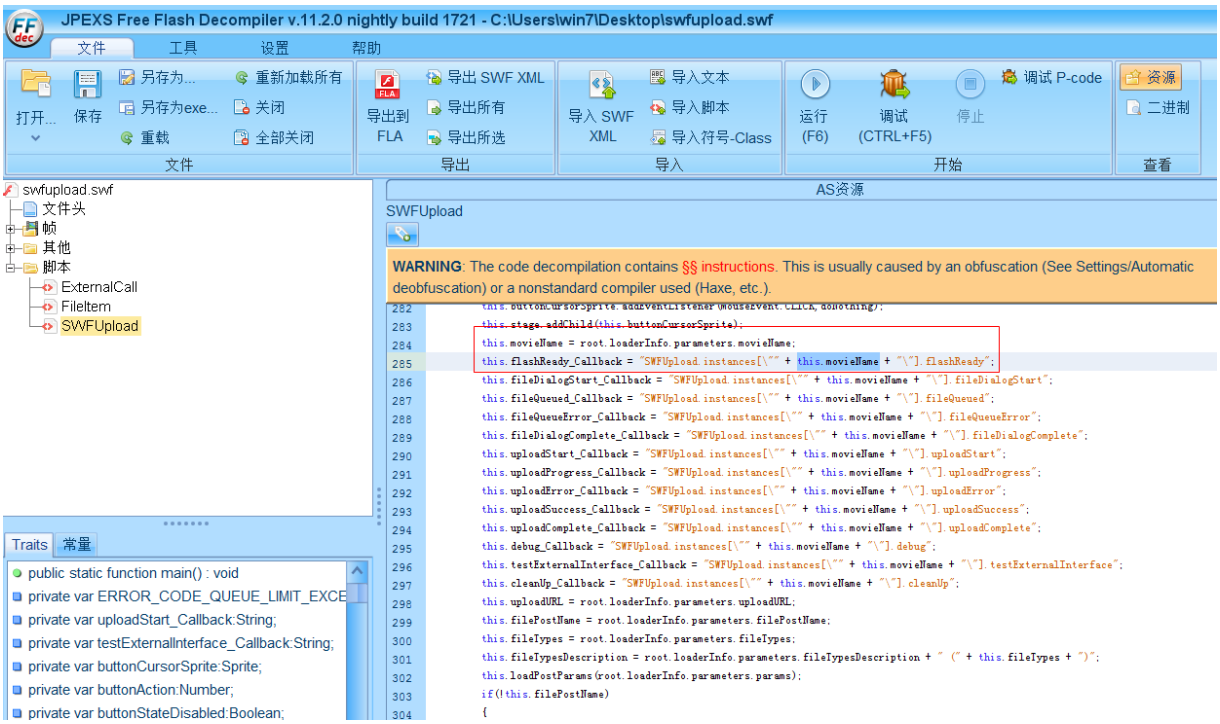
NoneCMS V1.3.0 has a XSS vulnerability in static/admin/js/kindeditor/plugins/multiimage/images/swfupload.swf #30

Open ghost opened this issue on Jun 2, 2020 · 0 comments

ghost commented on Jun 2, 2020

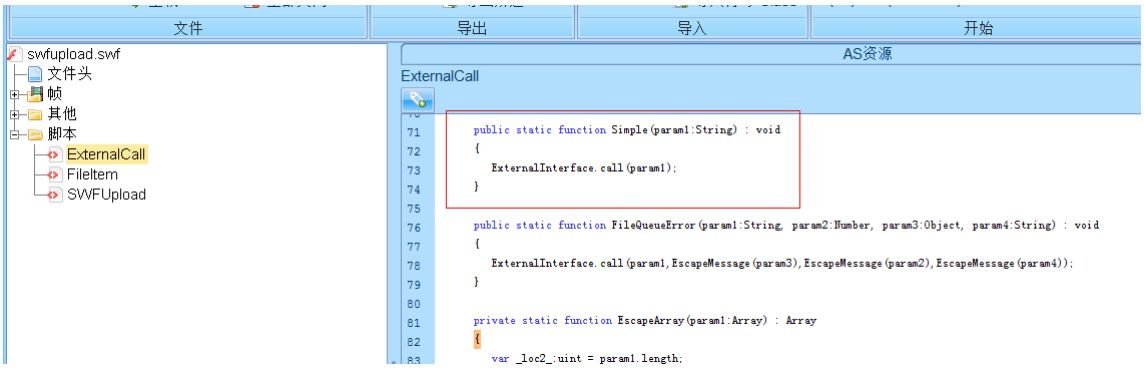
NoneCMS V1.3.0 has a XSS vulnerability in static/admin/js/kindeditor/plugins/multiimage/images/swfupload.swf.

I download the swfupload.swf file and I use FFdec to decompile the file. Then I find that user can control the movieName parameter which will concatenate as the value of flashReady_Callback:



Tracking the flashReady_Callback variable, it will call function ExternalCall.Simple() with one parameter flashReady_Callback:

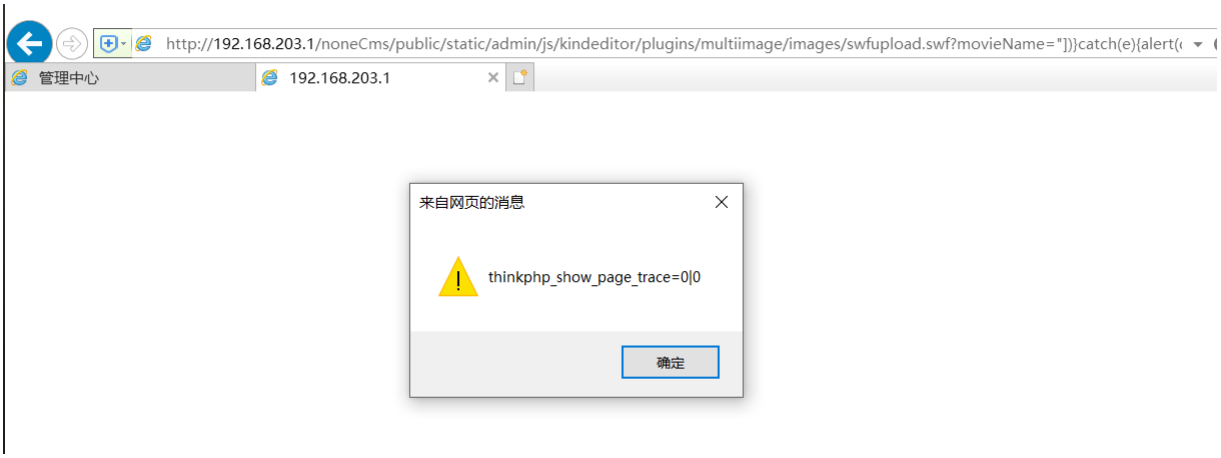
Then I check the ExternalCall.Simple() function, this is a piece of code that exists a Flash XSS vulnerability:



So PoC is as follows:

```
http://192.168.203.1/noneCms/public/static/admin/js/kindeditor/plugins/multiimage/images/swfupload.swf?movieName="])}catch(e){alert(document.cookie)};//
```

When NoneCMS administrator visits the link in IE or Microsoft Edge, it will cause xss attack:



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

0 participants