New issue

Jump to bottom

A Stored XSS exists in YzmCMS V5.6 #45

Closed ghost opened this issue on May 22, 2020 · 1 comment

ghost commented on May 22, 2020

Description

In YzmCMS 5.6, Stored XSS exists via the common/static/plugin/ueditor/1.4.3.3/php/controller.php action parameter, which allows remote attackers to upload a swf file. The swf file can be injected arbitrary web script or HTML.

PoC

In yzmcms\common\static\plugin\ueditor\1.4.3.3\php\config.json, when the value of action parameter is 'uploadvideo' or 'uploadfile', it allows remote user to upload a swf file:

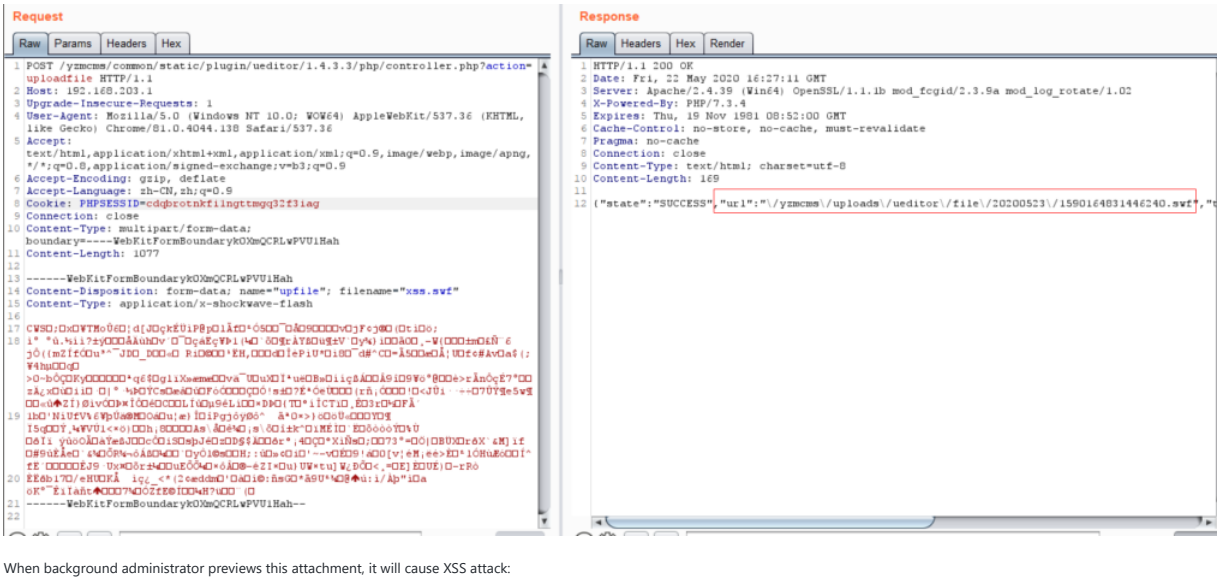
```
    /* 上传视频配置 */
    "videoActionName": "uploadvideo", /* 执行上传视频的action名称 */
    "videoFieldName": "upfile", /* 提交的视频表单名称 */
    "videoPathFormat": "/ueditor/video/{yyyy}{mm}{dd}/{time}{rand:6}", /* 上传保存路径,可以自定义保存路径和文件名格式 */
    "videoUrlPrefix": "", /* 视频访问路径前缀 */
    "videoMaxSize": 102400000, /* 上传大小限制，单位B，默认100MB */
    "videoAllowFiles": [
        ".flv", ".swf", ".mkv", ".avi", ".rm", ".rmvb", ".mpeg", ".mpg",
        ".ogg", ".ogv", ".mov", ".wmv", ".mp4", ".webm", ".mp3", ".wav", ".mid"], /* 上传视频格式显示 */

    /* 上传文件配置 */
    "fileActionName": "uploadfile", /* controller里,执行上传视频的action名称 */
    "fileFieldName": "upfile", /* 提交的文件表单名称 */
    "filePathFormat": "/ueditor/file/{yyyy}{mm}{dd}/{time}{rand:6}", /* 上传保存路径,可以自定义保存路径和文件名格式 */
    "fileUrlPrefix": "", /* 文件访问路径前缀 */
    "fileMaxSize": 51200000, /* 上传大小限制，单位B，默认50MB */
    "fileAllowFiles": [
        ".png", ".jpg", ".jpeg", ".gif", ".bmp",
        ".flv", ".swf", ".mkv", ".avi", ".rm", ".rmvb", ".mpeg", ".mpg",
        ".ogg", ".ogv", ".mov", ".wmv", ".mp4", ".webm", ".mp3", ".wav", ".mid",
        ".rar", ".zip", ".tar", ".gz", ".7z", ".bz2", ".cab", ".iso",
        ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".pptx", ".pdf", ".txt", ".md", ".xml"
    ], /* 上传文件格式显示 */
```

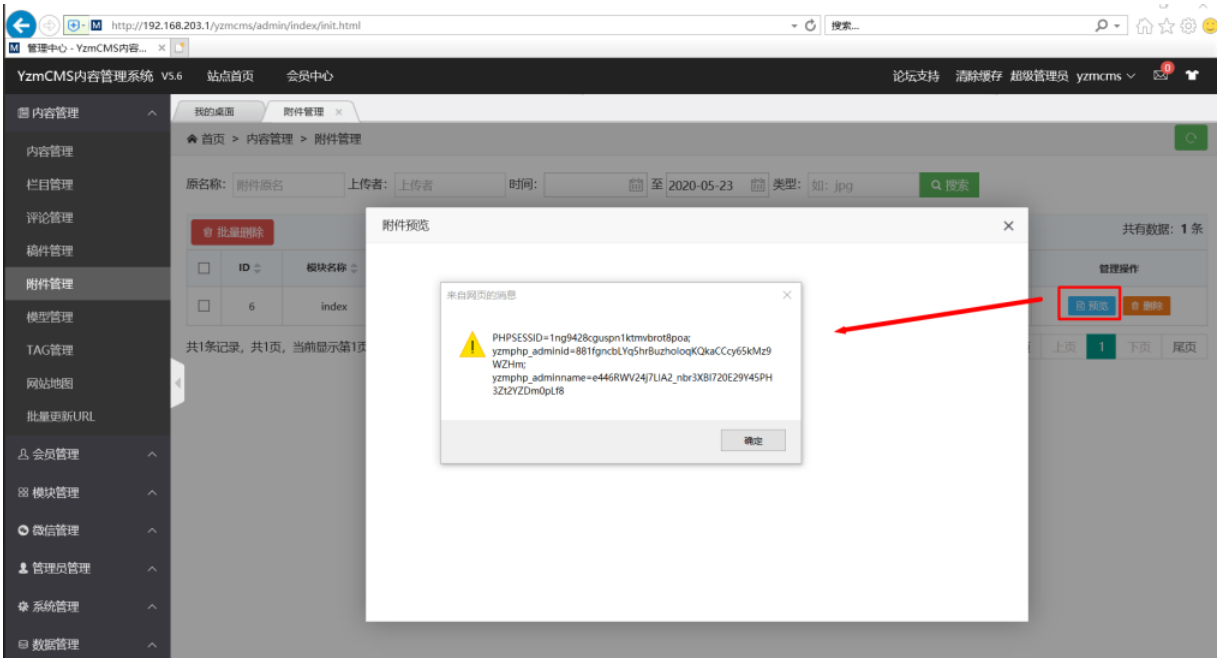
So I write and compile an evil swf file whose source code is as follows:

```
import flash.external.ExternalInterface;
ExternalInterface.call('alert(document.cookie)');
```

Then I upload the swf file through common/static/plugin/ueditor/1.4.3.3/php/controller.php without login:



When background administrator previews this attachment, it will cause XSS attack:



ghost changed the title ~~A Stored XSS exists in YzmCMS 5.6~~ A Stored XSS exists in YzmCMS V5.6 on May 22, 2020

yzmcms commented on May 22, 2020 — Owner

谢谢你的反馈，下一个版本修复。

yzmcms closed this as completed on May 22, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant