

 gh-pages ▾

...

UCMS-v1.6 / UCMS\_v1.6.0 XSS.md



Zoe0427 Update UCMS\_v1.6.0 XSS.md ✓

 History

 1 contributor

 31 lines (17 sloc) | 1.33 KB

...

# UCMS\_v1.6.0 has a vulnerability, stored cross-site scripting (XSS)

vendor: <http://uuu.la/>

Download link for UCMS-1.6 installation package:

[http://uuu.la/uploadfile/file/ucms\\_1.6.zip](http://uuu.la/uploadfile/file/ucms_1.6.zip)

1. Enter the background and click site management, Next, click Import column.
2. Configure parameters according to the picture. Click Submit after configuration

127.0.0.1:9876/ucms/index.php?do=sadmin\_cadd

站点设置 新增 后台管理 > 栏目配置

### 增加栏目

返回

上级栏目 --顶级栏目--

栏目名 666

栏目类型 ☐ 单页栏目 ☒ 文章栏目 ☐ 过渡栏目 ☐ 前台链接 ☐ 后台链接

☐ 不导入  
☒ 默认配置  
☐ 复制其他栏目配置 上级栏目  
☐ 导入配置文件 浏览... 未选择文件。

提交

1

2

### 3.Continue, click OK to import

127.0.0.1:9876/ucms/index.php?do=sadmin\_cinedit&cid=1&key=default\_2

站点设置 666 新增 后台管理 > 栏目配置

### 导入向导

返回

栏目名	666			
栏目配置信息	<input checked="" type="checkbox"/> 导入栏目配置 导入后将覆盖原有配置			
栏目字段[全选] [反选]	<input checked="" type="checkbox"/> 标题[title]	<input checked="" type="checkbox"/> 关键词[keywords]	<input checked="" type="checkbox"/> 描述[description]	<input checked="" type="checkbox"/> 内容[content]
	已存在的字段不会被导入			
栏目变量[全选] [反选]	<input checked="" type="checkbox"/> 将字段创建到数据库 如您还需修改表名或调整字段,请不必勾选,请保持默认文章表字段一致			
	<input checked="" type="checkbox"/> 栏目标题	<input checked="" type="checkbox"/> 栏目关键词	<input checked="" type="checkbox"/> 栏目描述	<input checked="" type="checkbox"/> 内容
已存在的变量不会被导入				
确认导入				

### 4.Next. Add after the column name:

```
666<script>alert(document.cookie)</script>
```

127.0.0.1:9876/ucms/index.php?do=sadmin\_cedit&cid=1

666 栏目配置

666 栏目配置

上级栏目: --顶级栏目--

1 栏目名: 666<script>alert(document.cookie)</script>

栏目域名:

栏目备注: 默认文章栏目配置

栏目类型: ☐ 单页栏目 ☒ 文章栏目 ☐ 过渡栏目 ☐ 前台链接 ☐ 后台链接

后台显示设置: ☒ 后台显示该栏目 ☒ 后台左侧显示

栏目数据库表: ucms\_article

编辑设置[帮助]: ☐ 禁止添加 ☐ 禁止编辑 ☐ 禁止删除 ☐ 文章转移 ☒ 文章限制 ☐ 显示复制按钮 ☐ 显示文章作者 ☐ 默认显示父分类

前台设置: ☐ 禁用该栏目 ☒ 导航栏显示 ☐ 新窗口中打开

文章列表显示: 默认显示数量: 15 默认排序方式: id desc

栏目页面[帮助]:

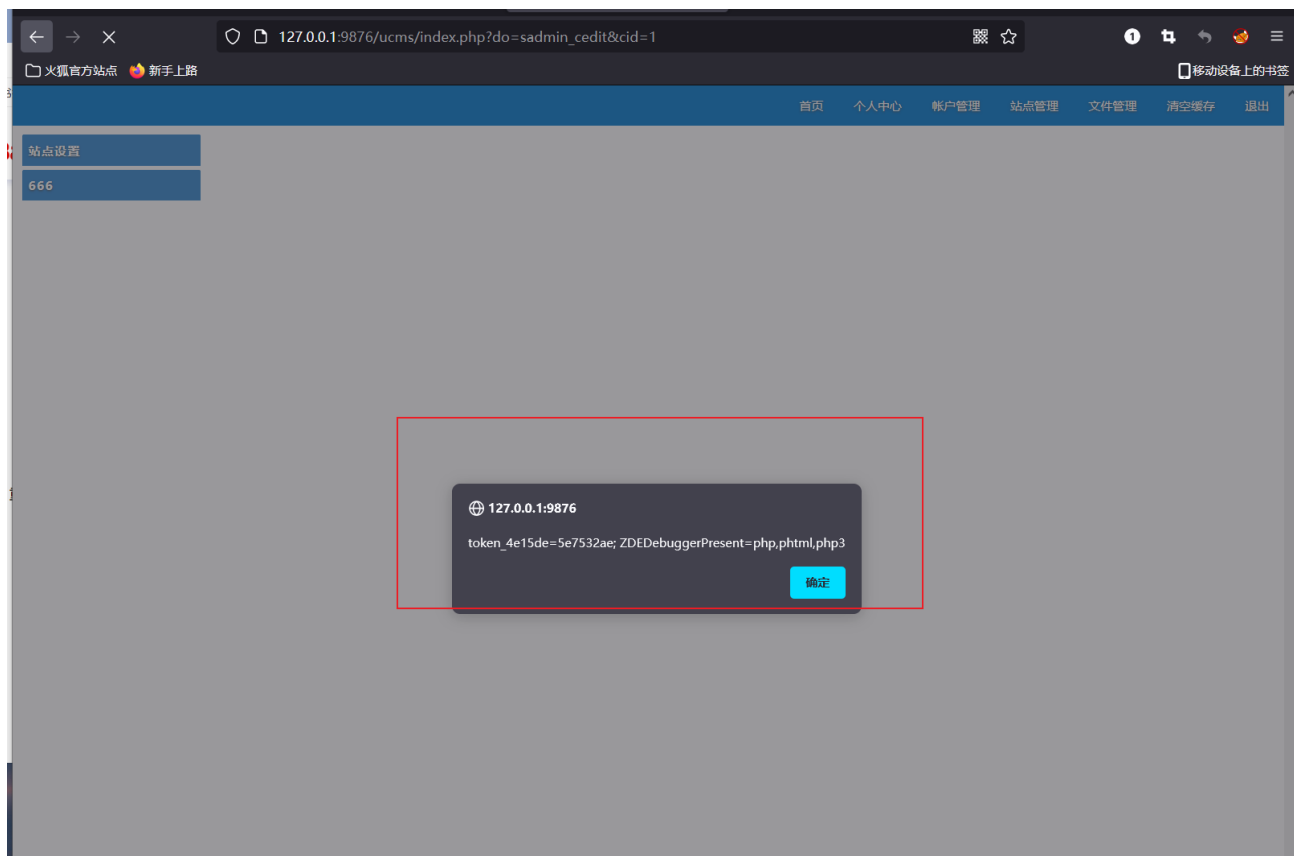
栏目地址:	/(cid)/	页面缓存时间:	0 秒	模板文件:	lst.php	编辑 选择
分页地址:	/(cid)/page_(page).html	页面缓存时间:	0 秒	模板文件:	lst.php	编辑 选择
文章地址:	/(cid)/(id).html	页面缓存时间:	0 秒	模板文件:	article.php	编辑 选择

其他页面[增加]:

栏目排序: 5

2 提交 导入栏目配置

5.Check the submitted content, successfully trigger XSS attack code, pop-up cookie sensitive information



6. Any user visiting the home page will pop up. If he has logged in, the cookie value will be directly disclosed

