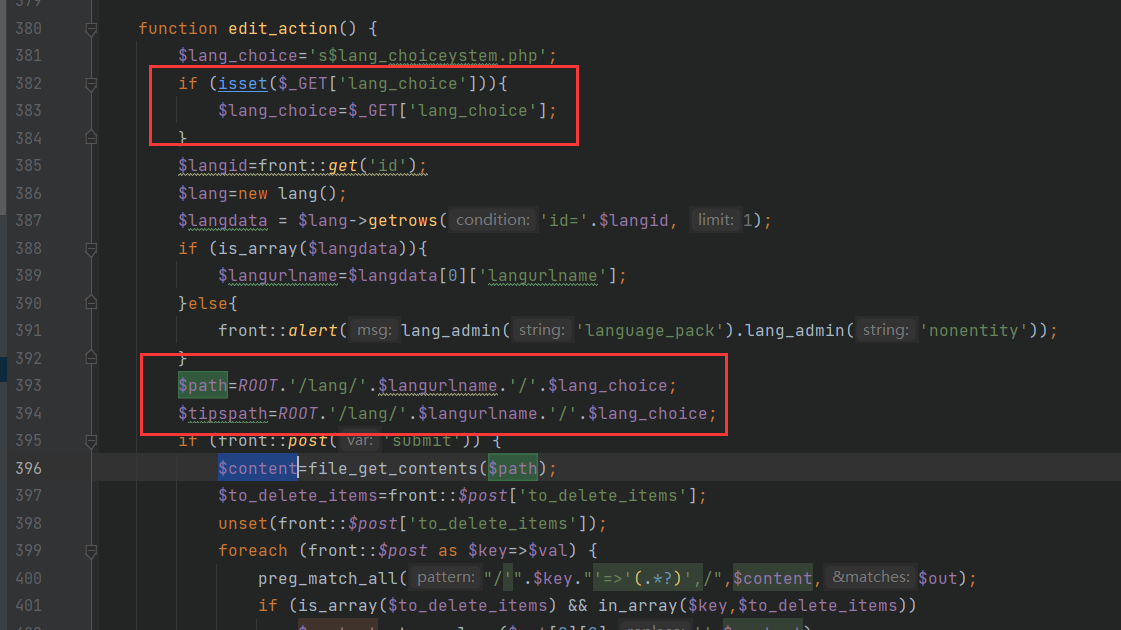
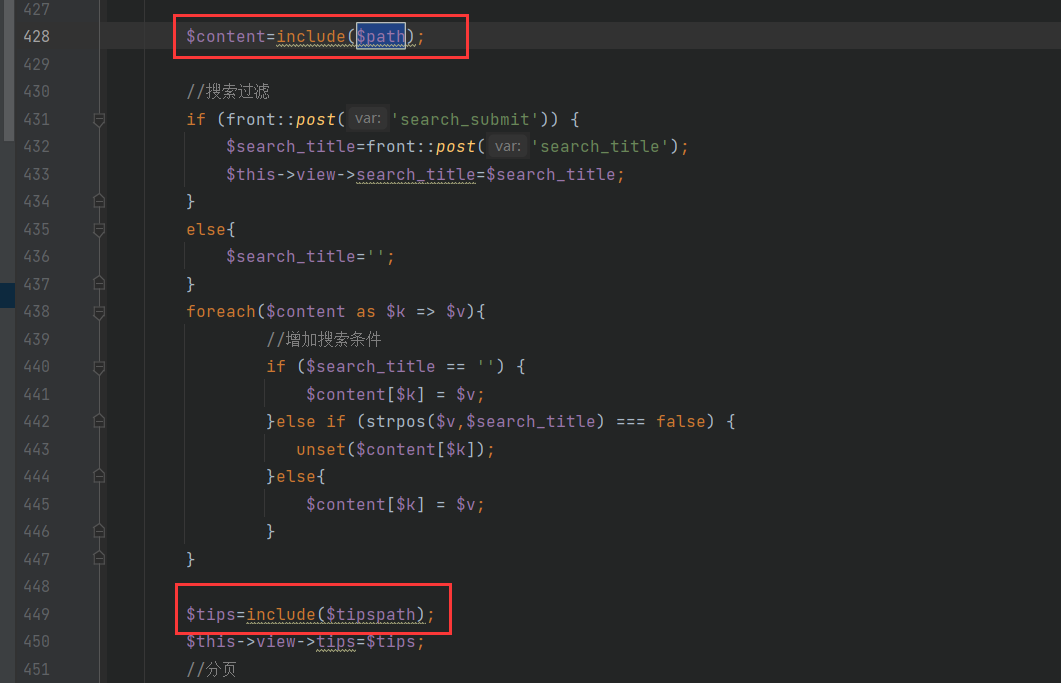
CmsEsay7.7.6后台管理系统存在本地文件包含漏洞

供应商：<https://www.cmseasy.cn/>

漏洞文件：CmsEasy\_7.7.6\_UTF-8\_20220420\lib\admin\language\_admin.php

代码分析：

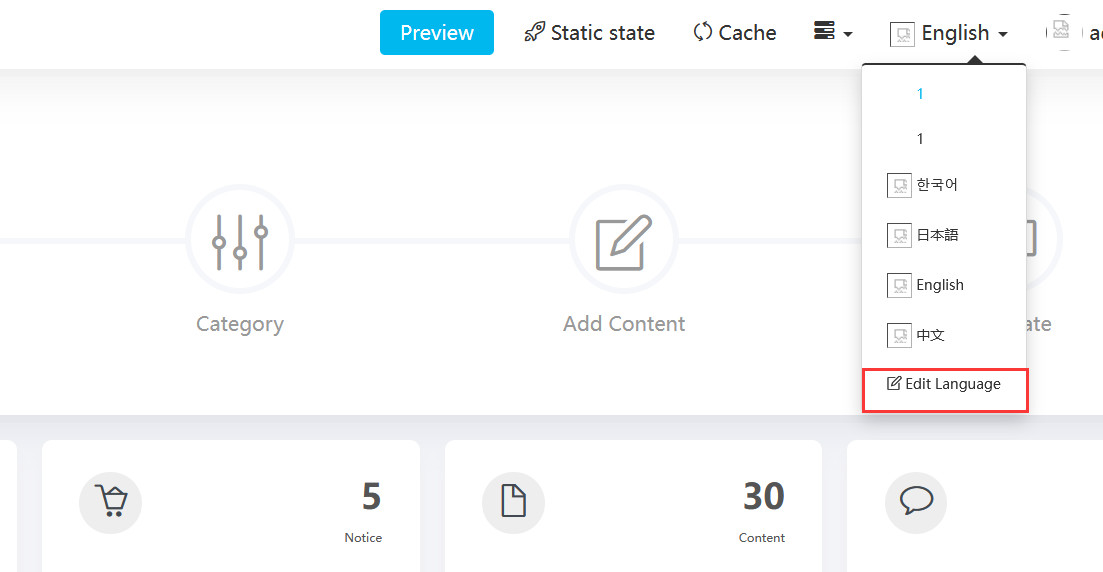
382行中lang\_choice参数可由用户控制，在393、394行中拼接并赋值给$path、$tipspath变量，428行、449行中用include函数处理这两个变量，这样会造成本地文件包含漏洞。  


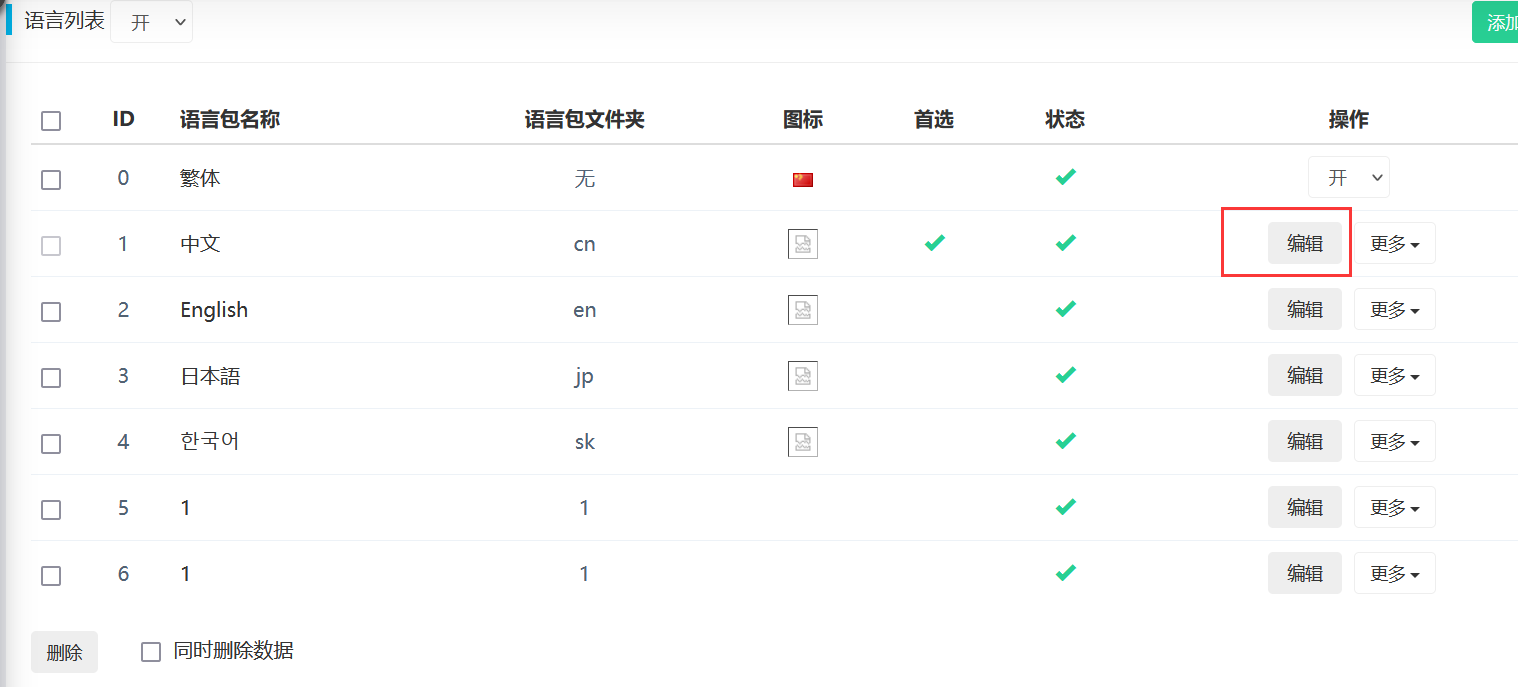


重现步骤：

1. 以管理员角色登录后台管理页面

2．点击 Edit Language-> edit





3.上传一个可执行的PHP图片木马



4.返回点击”系统语言项”并用burpsuite抓包，lang\_choice参数修改为刚才上传的图片木马即可造成命令执行

