**CuteNews 2.1.2远程代码执行漏洞利用**

# 一、漏洞描述

## 1、漏洞简述

在“Media Manager”区域，具有低权限（编辑器）的用户可以绕过文件上载限制，修改文件扩展为PHP，从而导致执行任意命令。

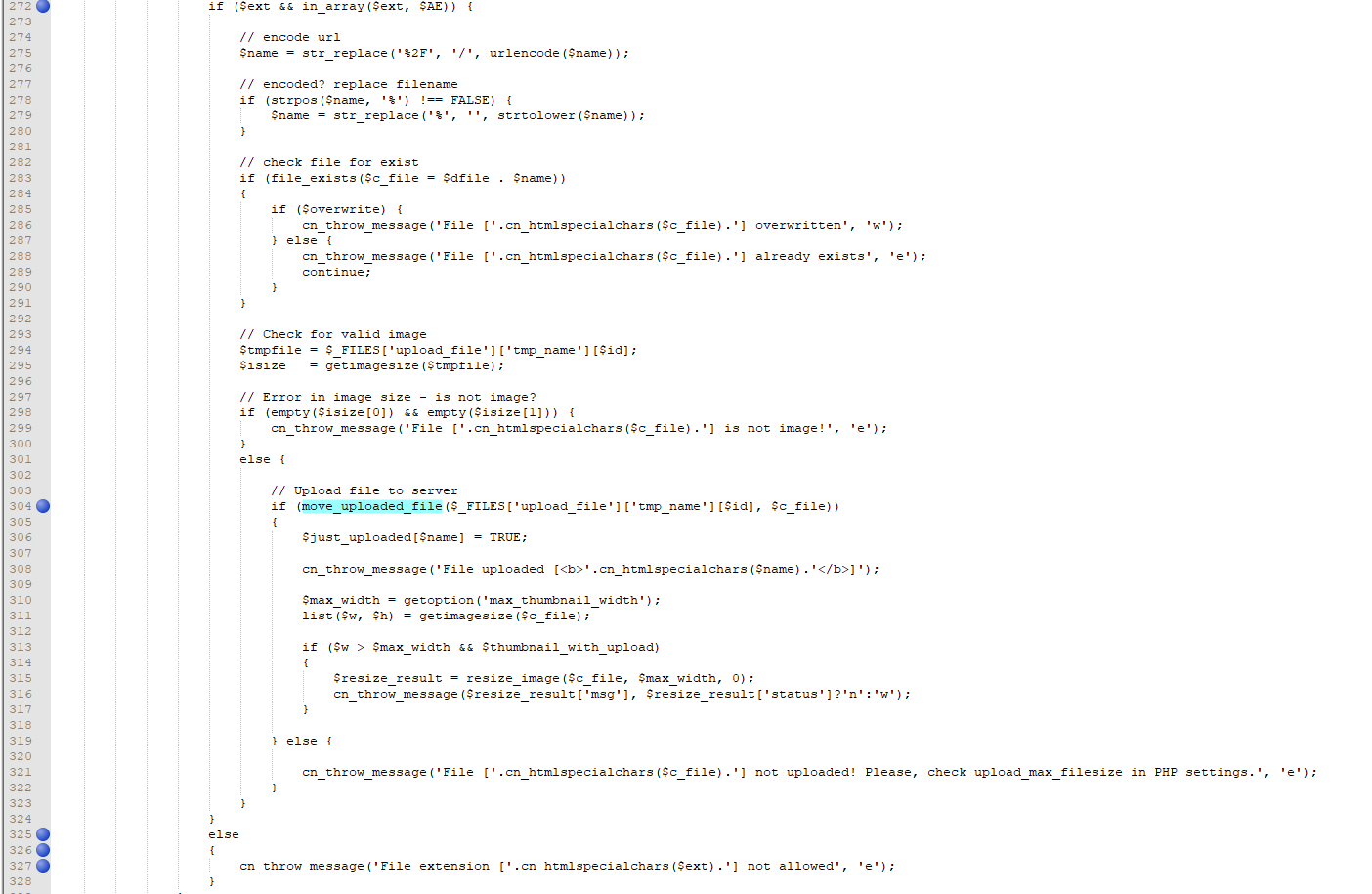
# 二、机理分析

## 1、远程代码执行漏洞

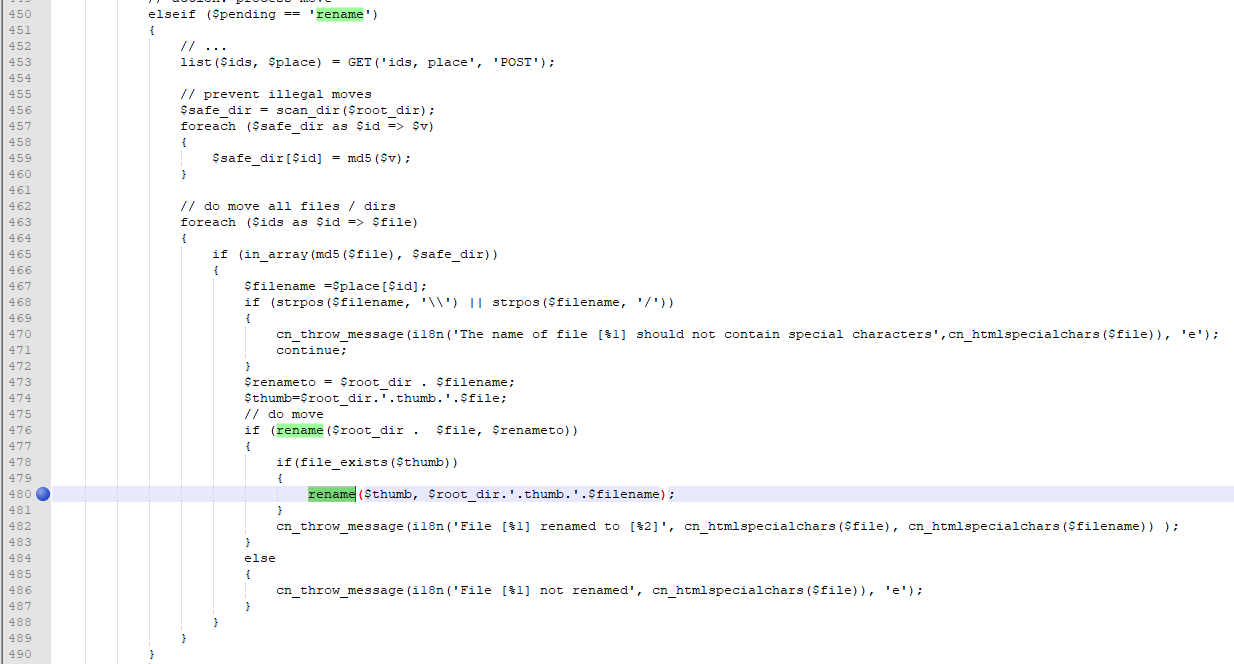
**影响版本：**v2.1.2

**漏洞编号：**无

找到关键代码，上传会校验文件扩展，符合要求扩展的文件才能上传，否则执行325行的else。图片可以上传，所以可以上传图片木马。

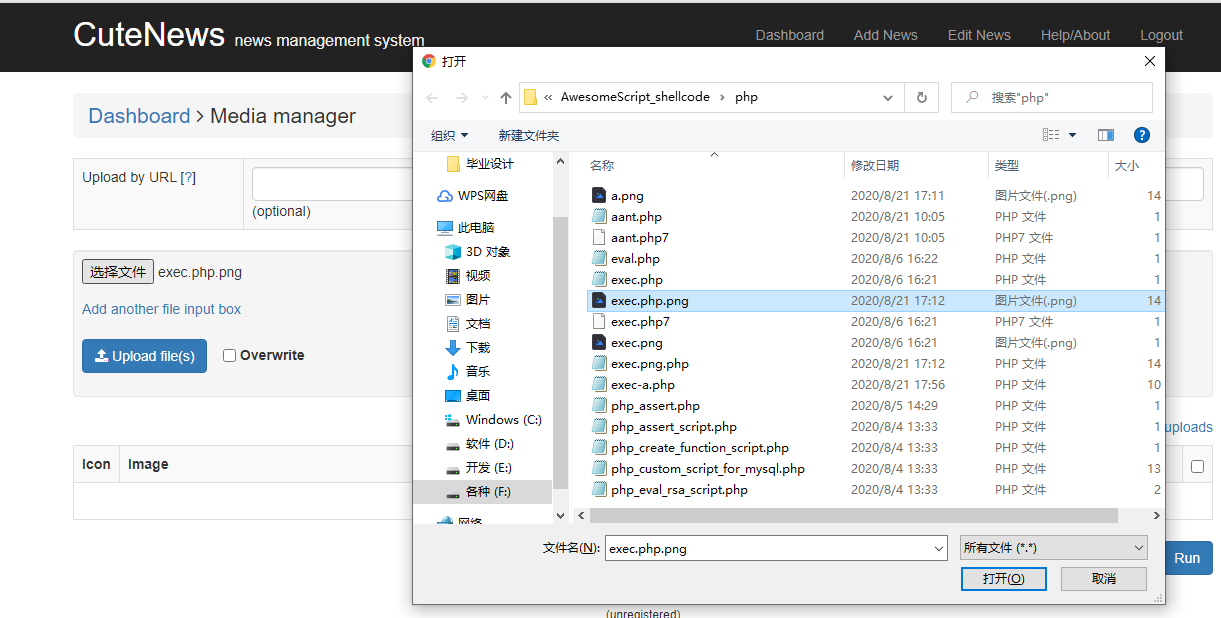


重命名逻辑如下，未限制重命名之后的文件扩展名，所以可以修改文件名为php

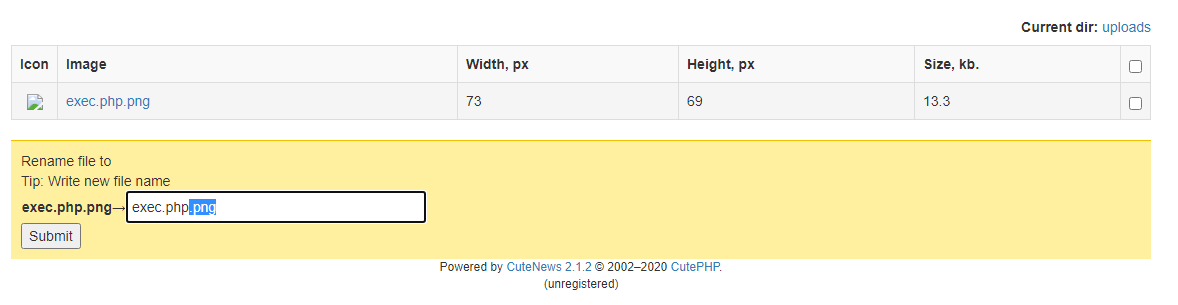


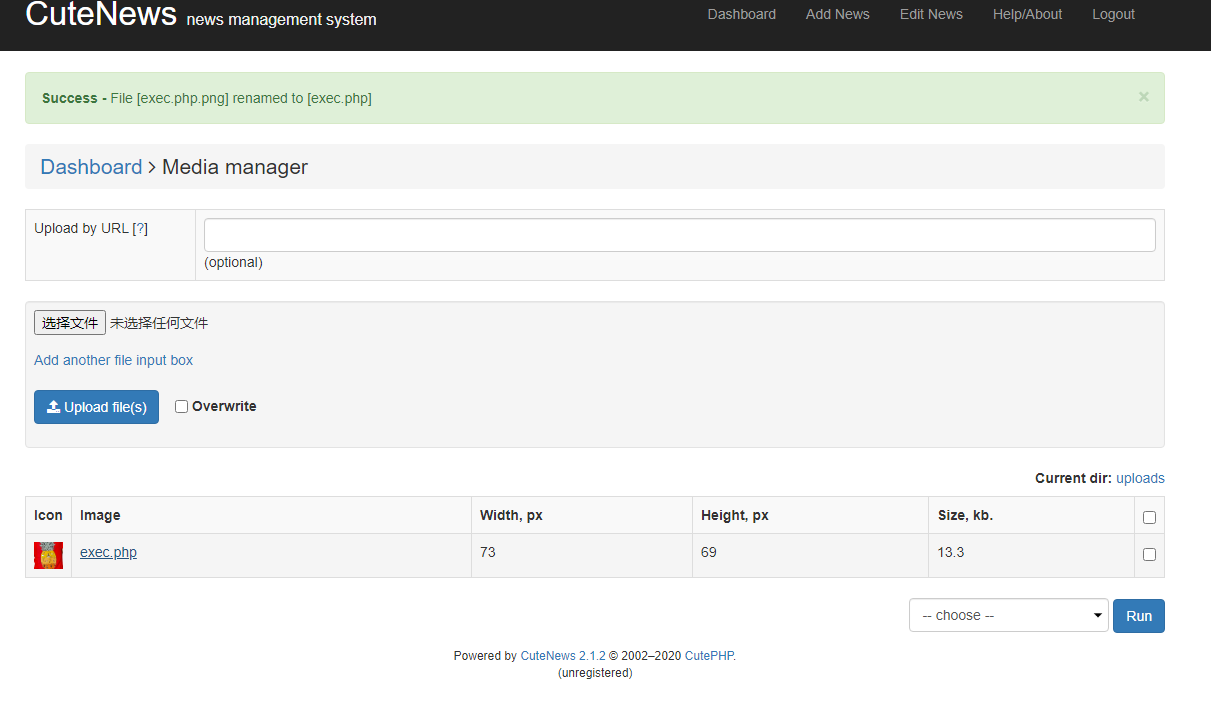
# 三、攻击路径

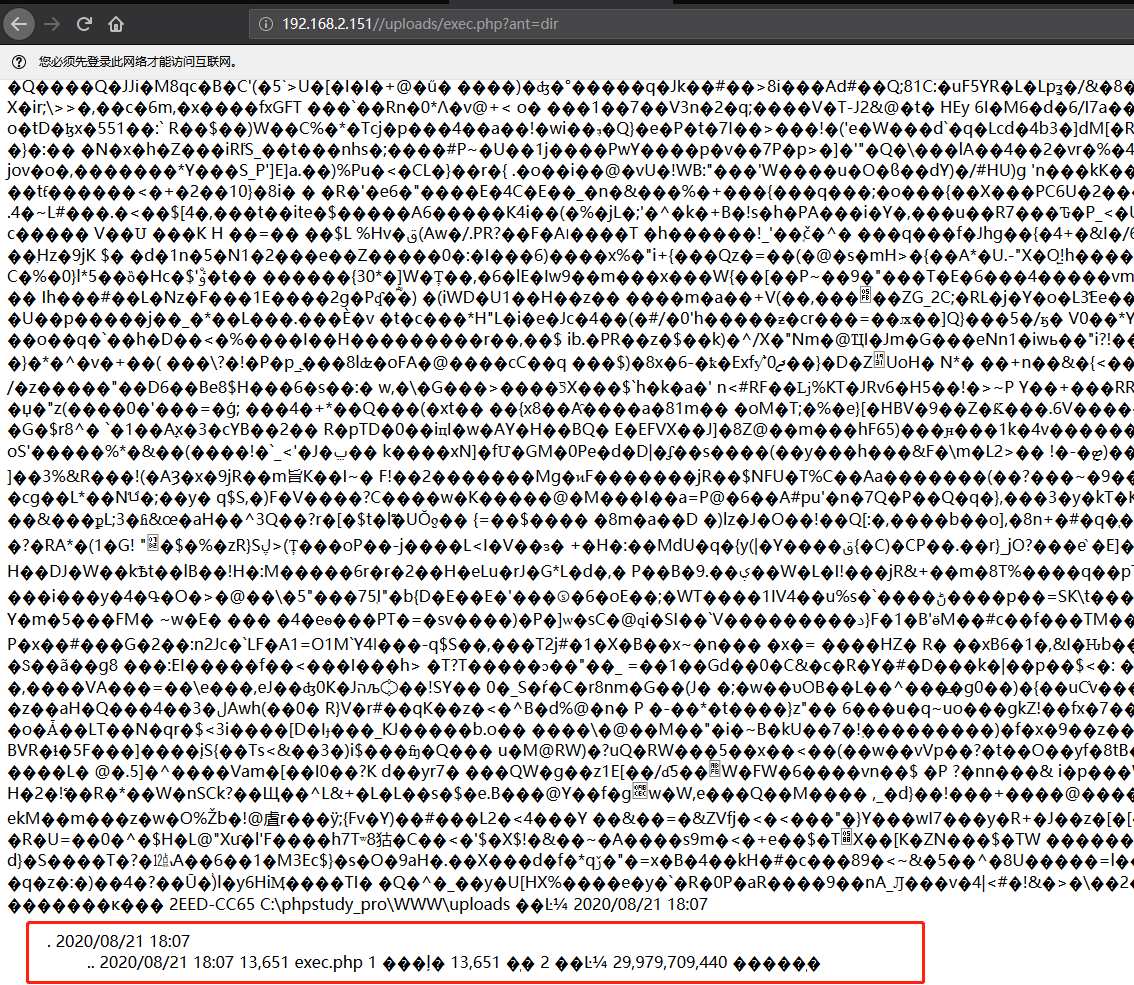
登录之后选择Media Manager，然后上传图片马



重命名文件为php







# 四、防御方案

重命名对文件类型和文件名称等做限制，仅允许png、jpg等扩展。