**Victor CMS 1.0任意文件上传漏洞利用**

# 一、漏洞描述

## 1、漏洞简述

管理页面新建用户-上传头像位置可以上传任意文件漏洞，可导致远程代码执行。

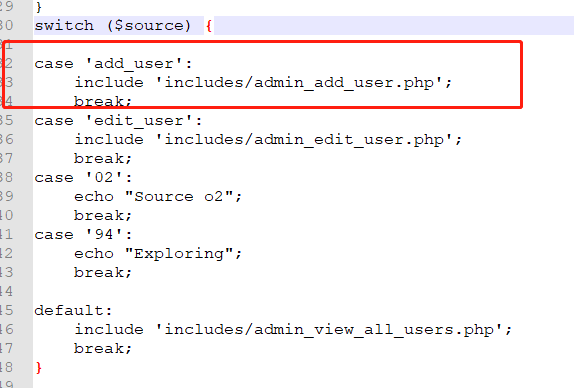
# 二、机理分析

## 1、任意文件上传漏洞

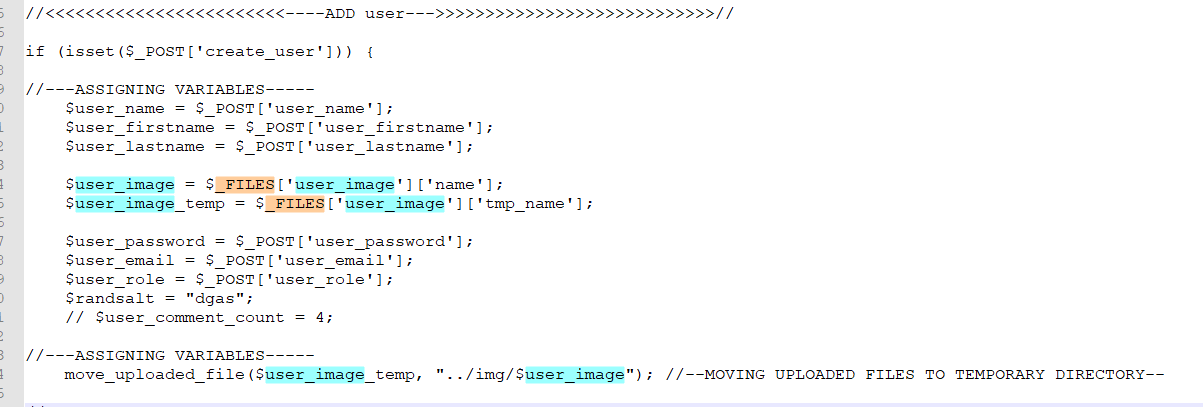
**影响版本：**1.0

**漏洞编号：**无

添加用户路径为/admin/users.php?source=add\_user



关键代码如图所示，当source=add\_user时，包含includes/admin\_add\_user.php文件，跟踪到admin\_add\_user.php文件。

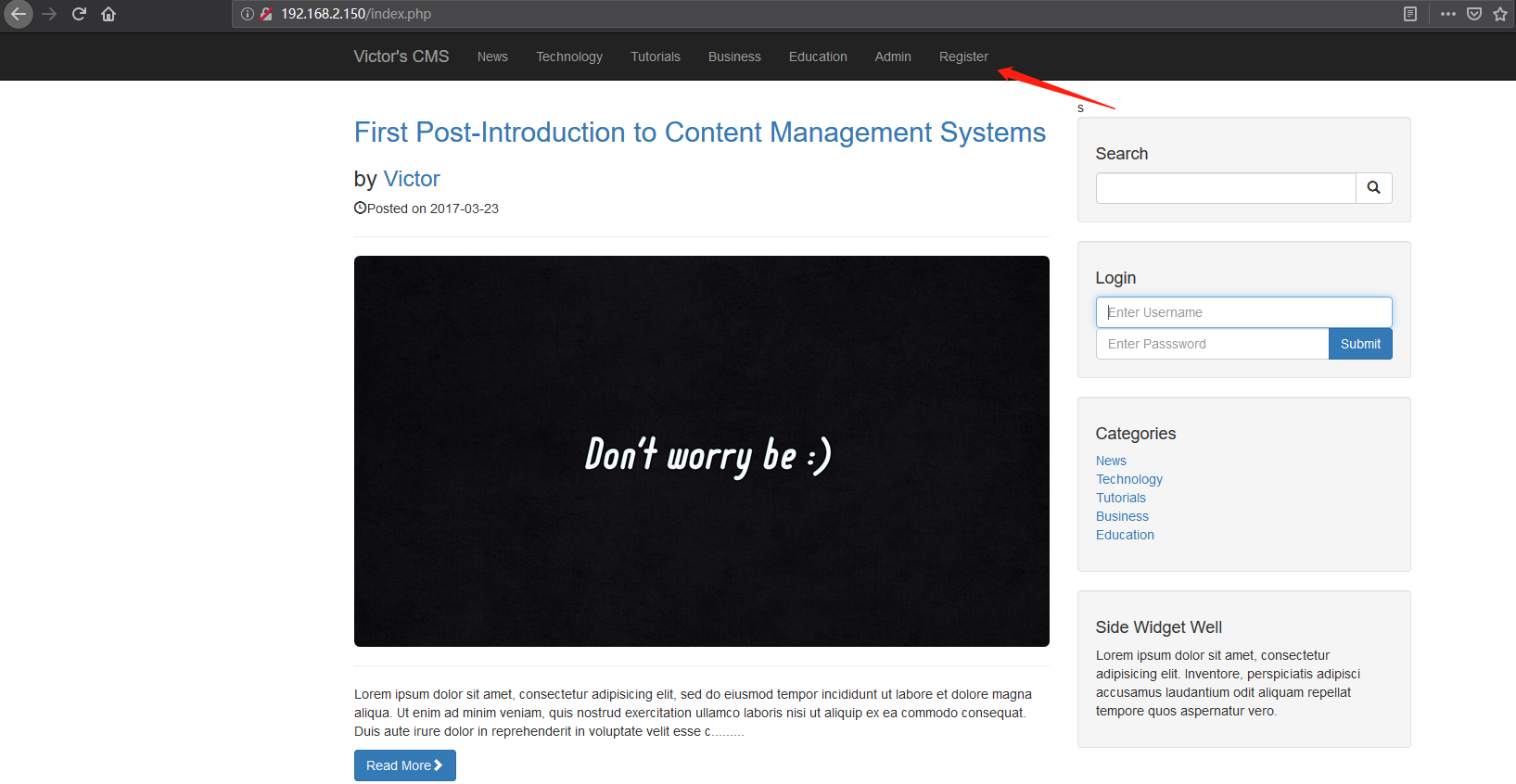


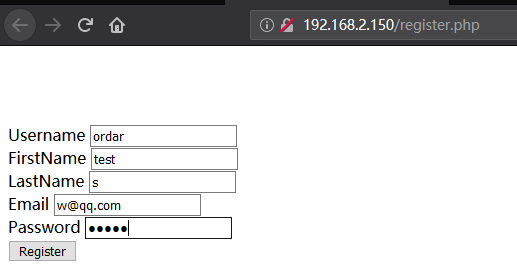
$\_FILES是HTTP文件上传变量，表示上传的头像，但是并没有对文件类型和文件名称等做限制，导致可以上传php文件，执行php代码。

move\_uploaded\_file（）将上传的文件移动到新位置，由此可知文件上传路径。

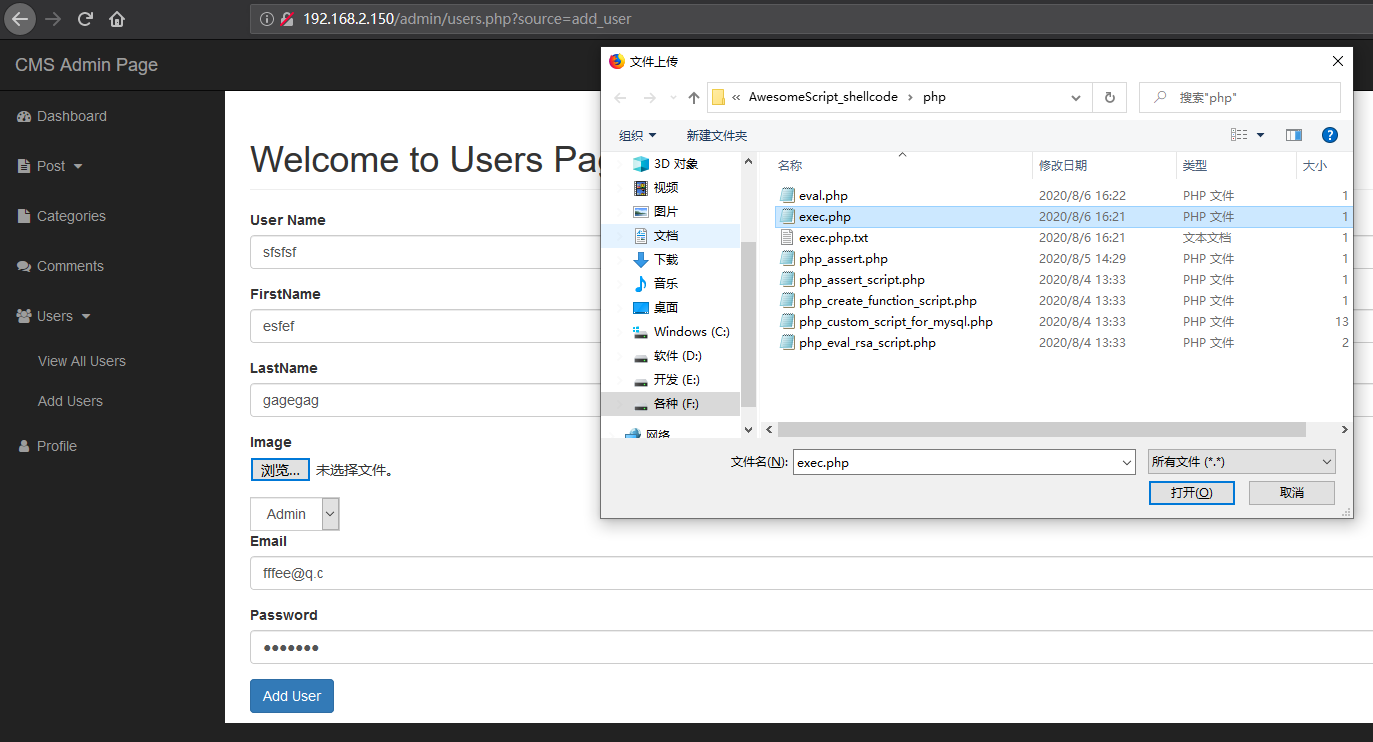
# 三、攻击路径

点击注册按钮，访问/register.php注册账号。

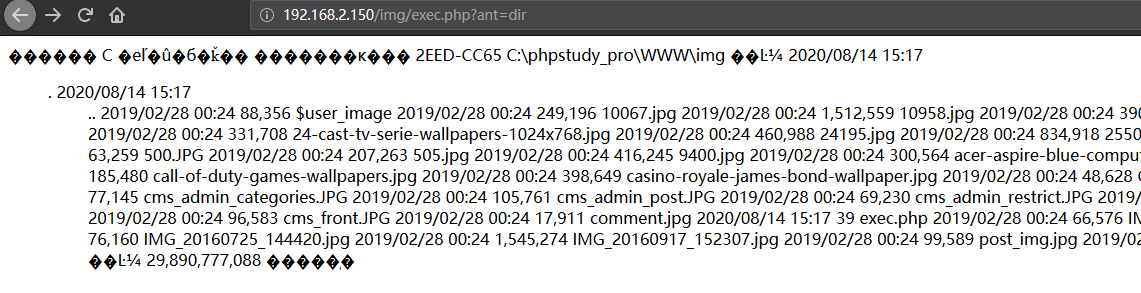




登录账号，然后add user，头像上传php木马



确定新建之后访问/img/exec.php?ant=dir



# 四、防御方案

上传头像位置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。