**Online Student Enrollment System 1.0任意文件上传漏洞利用**

# 一、漏洞描述

## 1、漏洞简述

在线学生注册系统版本1.0存在未经验证的文件上载漏洞，使得远程攻击者能够通过上传恶意构建的PHP文件，在托管Web服务器上获得远程代码执行（RCE）。

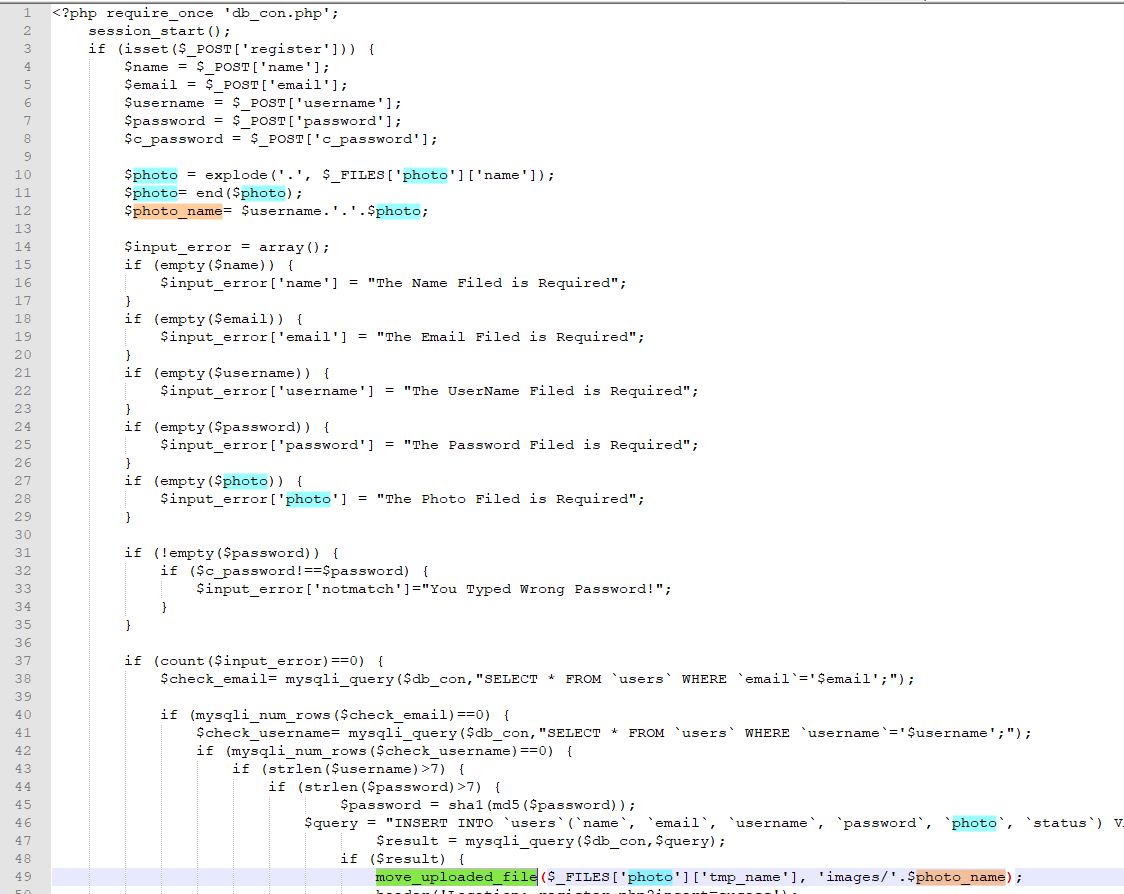
# 二、机理分析

## 1、任意文件上传漏洞

**影响版本：**1.0

**漏洞编号：**无

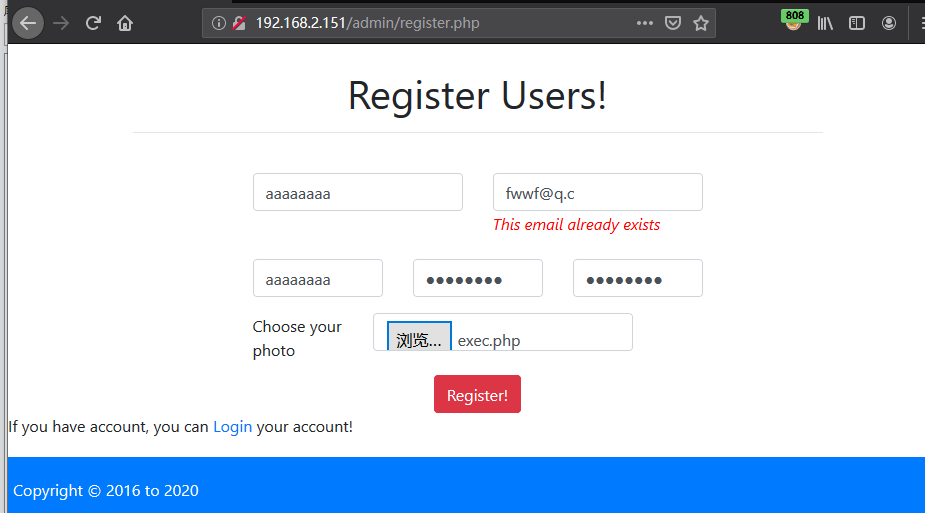
该系统有注册功能，允许用户注册账号，在注册功能中要求用户上传图片，然而未对图片做处理。

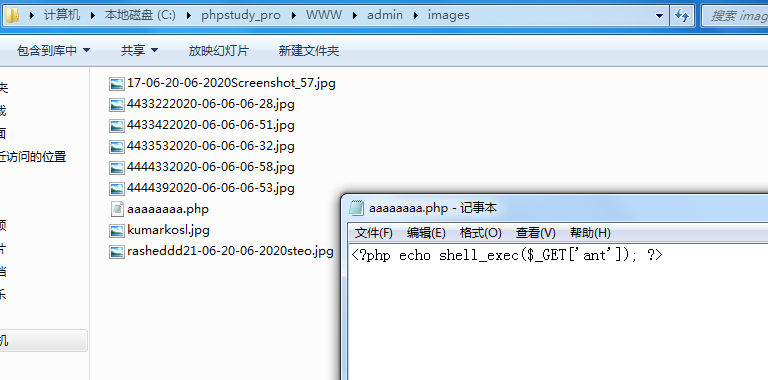


关键代码如上。$photo是上传的图片文件，$photo\_name是文件名，先用“.”将上传的文件名分割然后取最后一个作为文件格式，如果上传的文件有多个扩展名只取最后一个。文件名最后得到用户名加格式。然后在49行使用move\_uploaded\_file（）函数将上传的文件移动到新位置，由此可以得到文件路径。

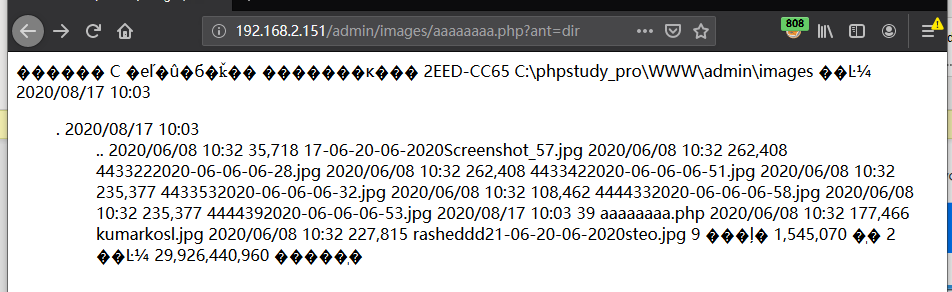
# 三、攻击路径

访问/admin/register.php，图片上传php木马。





可以看到文件上传成功。然后访问/admin/images/aaaaaaaa.php执行任意命令



# 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。