**Online Discussion Forum Site 1.0远程代码执行漏洞利用**

# 一、漏洞描述

## 1、漏洞简述

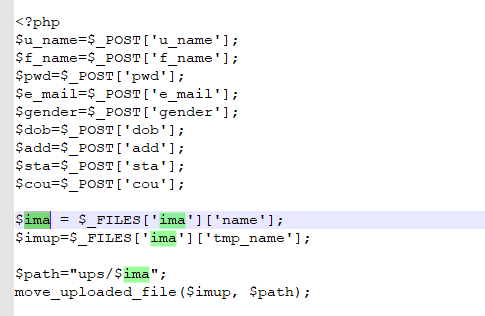
/register.php注册页面进行注册账号。注册页面允许上传图片并且可以上传php文件。

# 二、机理分析

## 1、远程代码执行漏洞

**影响版本：**1.0

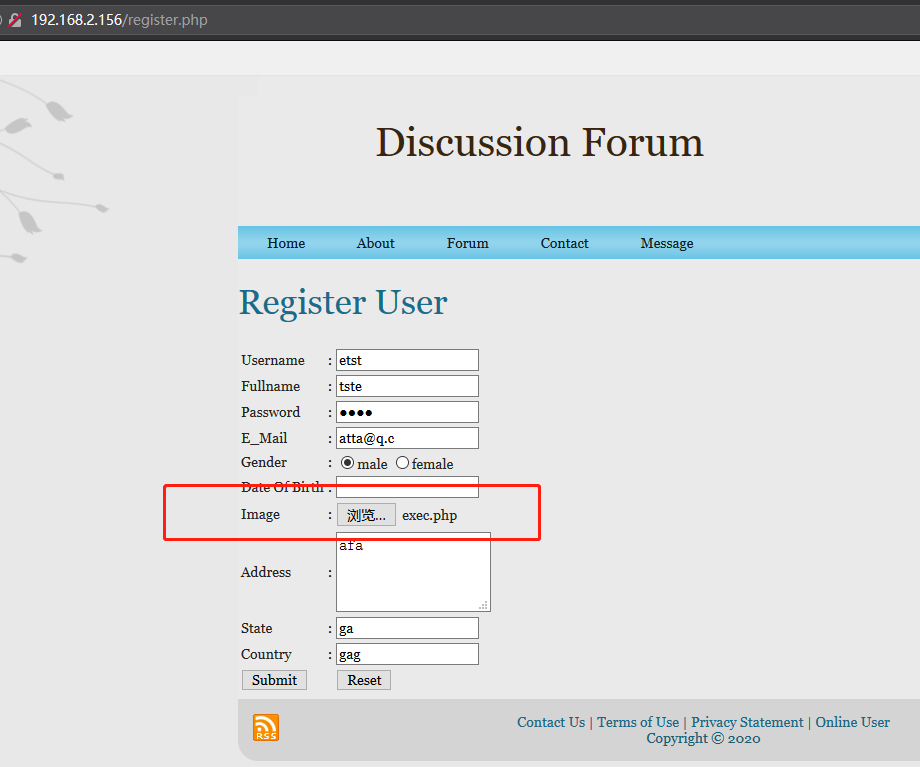
**漏洞编号：**无



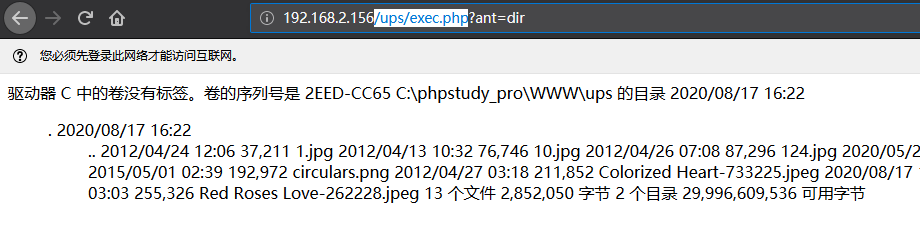
关键代码如图：move\_uploaded\_file处理上传文件，并且未限制文件格式，并且路径可知。

# 三、攻击路径

访问/register.php



上传文件路径/ups/exec.php



# 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。