**Clinic Management System 1.0任意文件上传漏洞利用**

# 一、漏洞描述

## 1、漏洞简述

Clinic Management System 1.0版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载恶意构建的PHP文件在宿主Web服务器上获得远程代码执行（RCE）。

细节：

以患者身份登录网站，然后访问“/manage\_website.php”页，因为它不检查管理员用户。更改网站logo并上载恶意php文件（<?php echo shell\_exec($\_GET["cmd"]); ?>)。 如果您看到这条消息“Something Went Wrong”，您已成功上载恶意php文件。

你的文件路径： /uploadImage/Logo/your\_file.php

# 二、机理分析

## 1、任意文件上传漏洞

**影响版本：**1.0

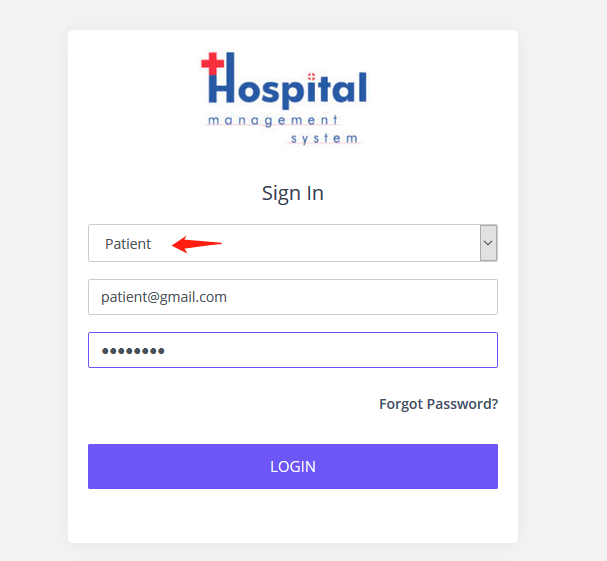
**漏洞编号：**无



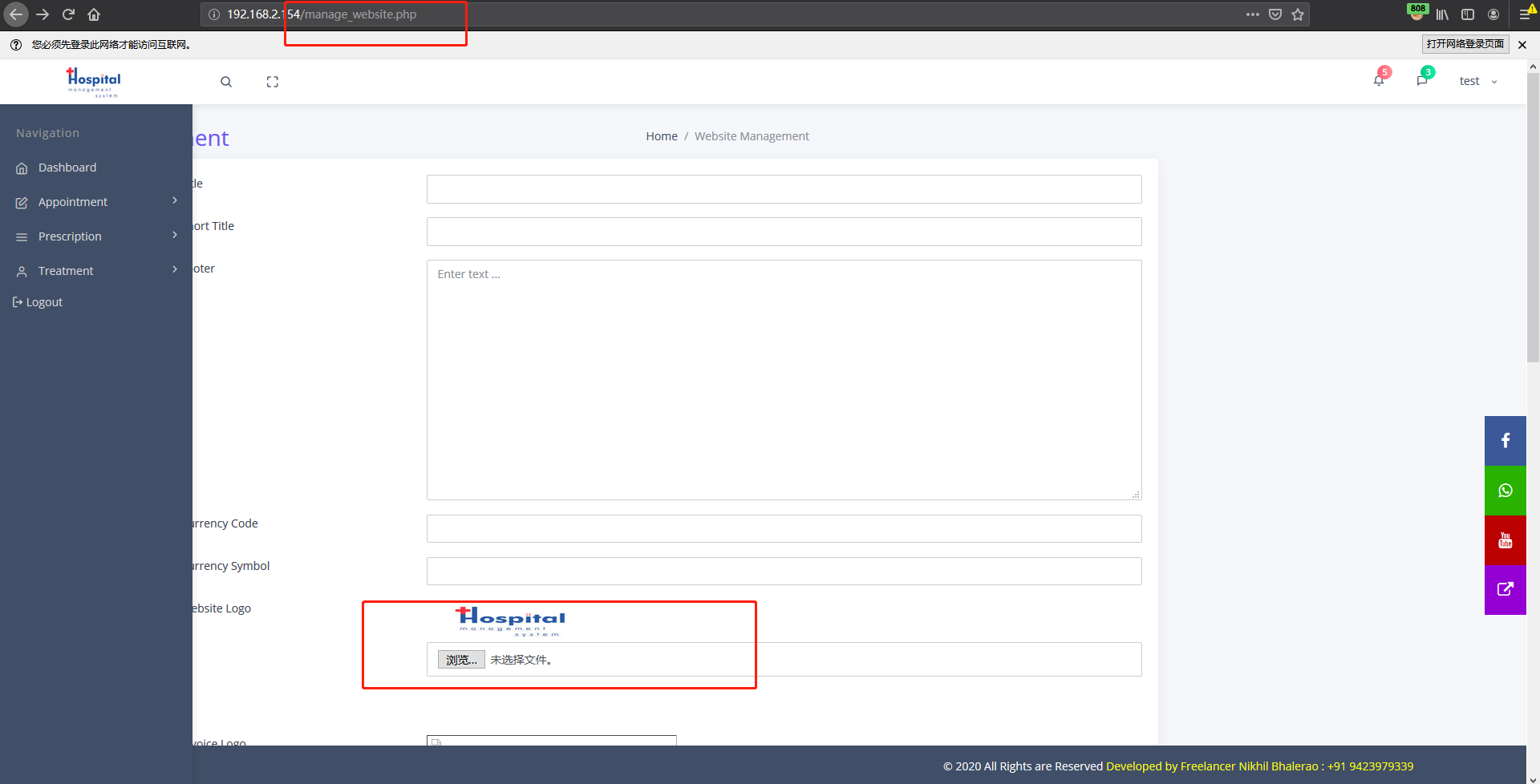
关键代码如图所示，使用了move\_uploaded\_file函数，将上传的文件移动到新位置，并且未限制文件格式。

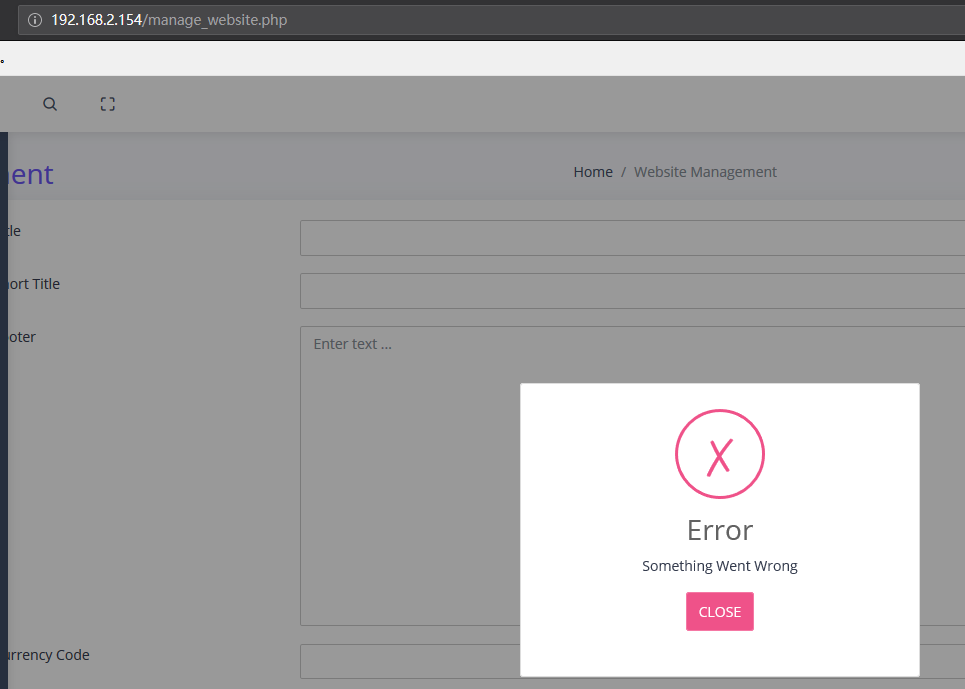
# 三、攻击路径

登录patient或更高权限的用户



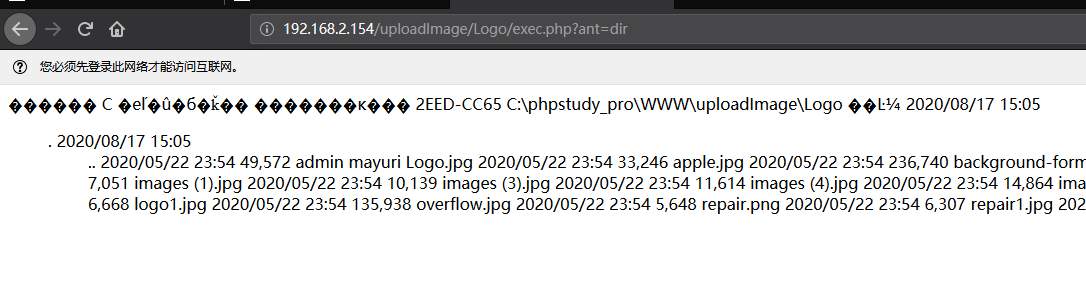
访问“/manage\_website.php”页,logo位置上传php木马





看到这条消息“Something Went Wrong”，您已成功上载恶意php文件。

文件路径： /uploadImage/Logo/your\_file.php



# 四、防御方案

上传logo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。