**Online Marriage Registration System 1.0 – 远程代码执行漏洞利用**

# 一、漏洞描述

## 1、漏洞简述

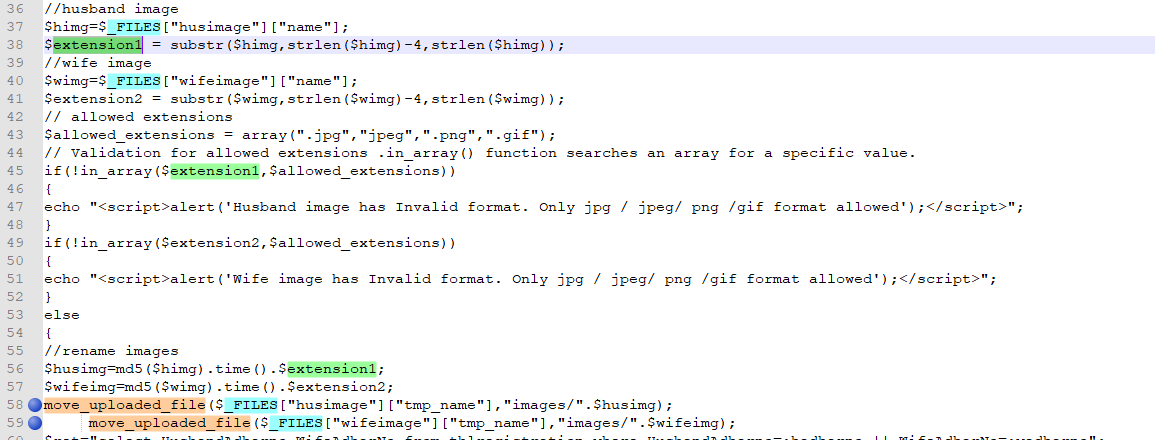
Online Marriage Registration System 1.0存在任意文件上传漏洞，利用漏洞需要身份验证，但您可以免费注册为用户，这足以攻击系统。

# 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



/user/marriage-reg-form.php文件处理丈夫和妻子照片，对文件格式做了限制，然后使用move\_uploaded\_file函数处理上传的文件。

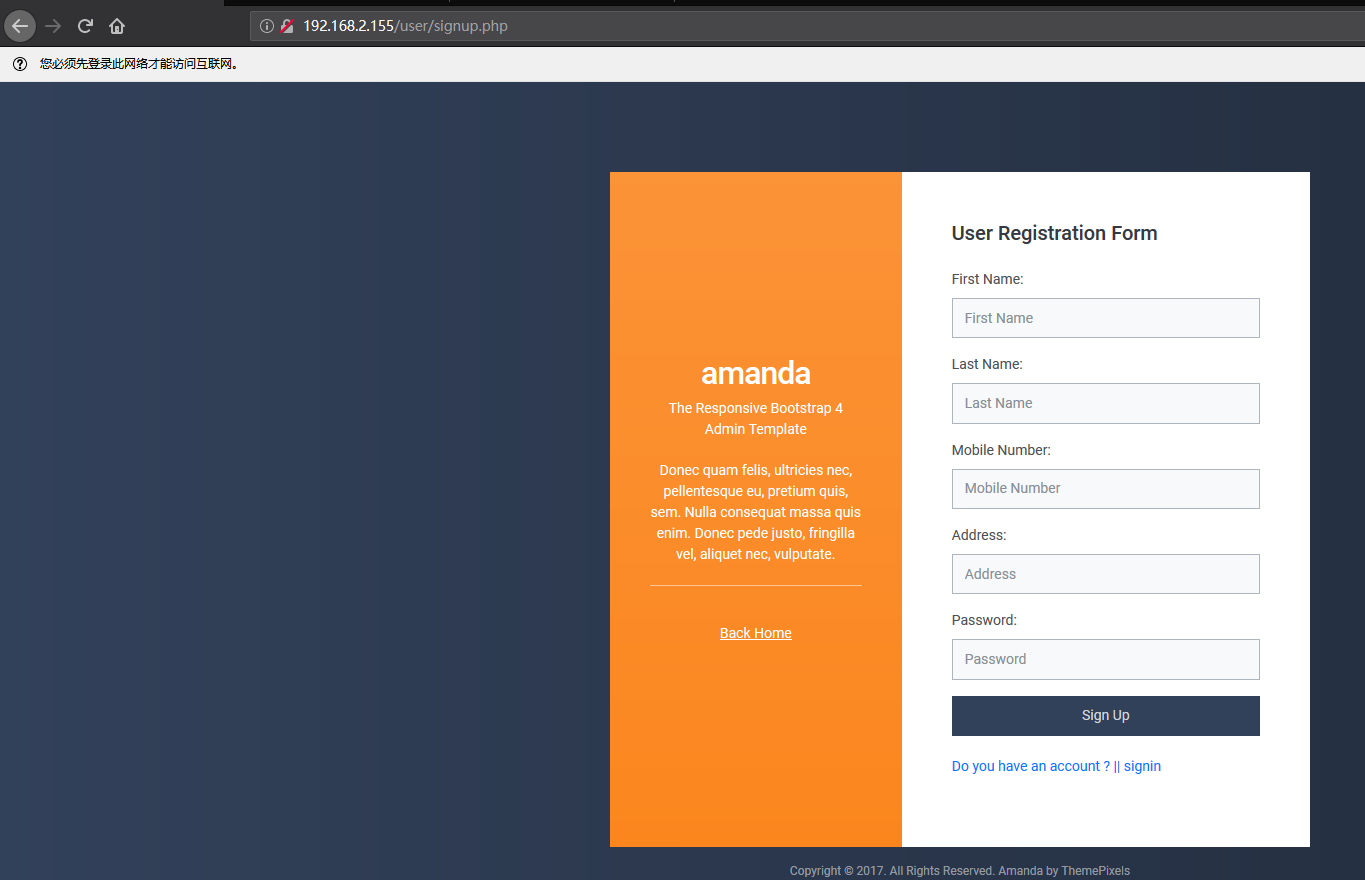
乍一看对图片格式进行了限制，好像没毛病，实际读一下代码可知：

看49行，当extension2不在数组中时，会alert提醒，当extension2在数组中时，会保存文件（husimage和wifeimage）。但是对extension1没有做逻辑上的验证。

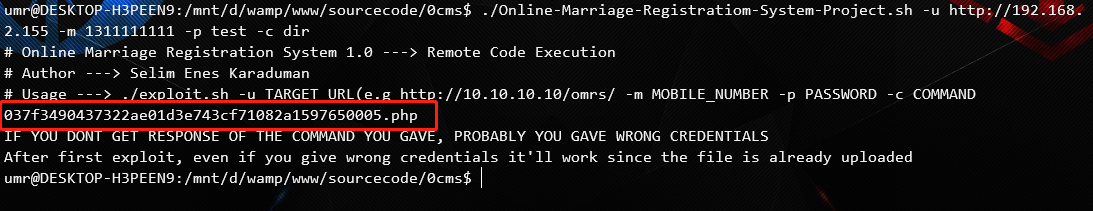
这里存在一个逻辑问题，当husimage为php并且wifeimage为jpg时，也就是extension1==.php，extension2==.jpg时，经过45行时因为extension1不满足格式要求，所以会alert提示，然后往下走，经过49行因为extension2满足格式要求，所以走else。然后在else中保存husimage为php，wifeimage为jpg。

# 三、攻击路径

注册账号/user/signup.php

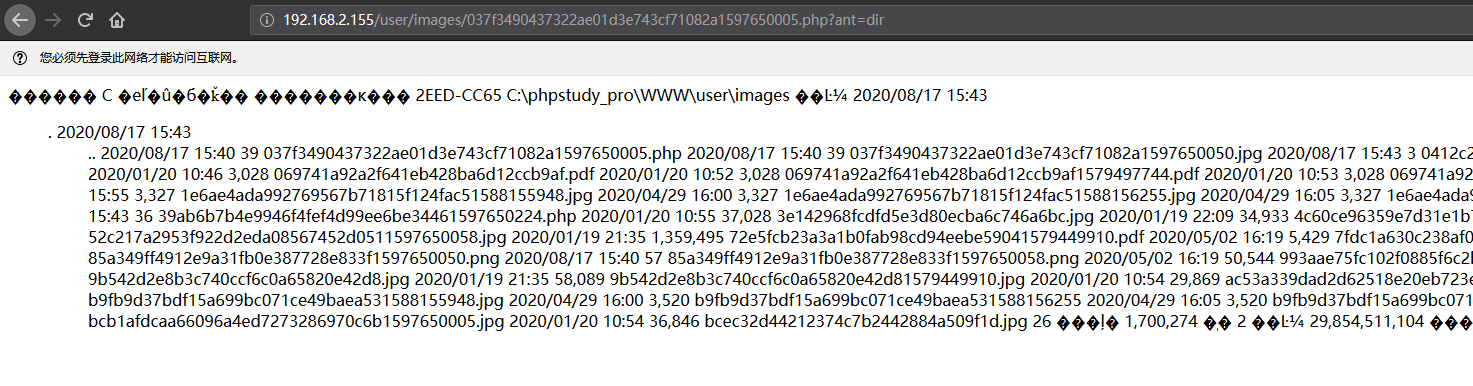


使用poc攻击，会返回文件名





/user/images/文件.php执行命令



# 四、防御方案

对husimage和wifeimage分别做格式校验，满足格式才保存文件，有一方不满足均不保存。