**Online Clothing Store 1.0任意文件上传漏洞利用**

# 一、漏洞描述

## 1、漏洞简述

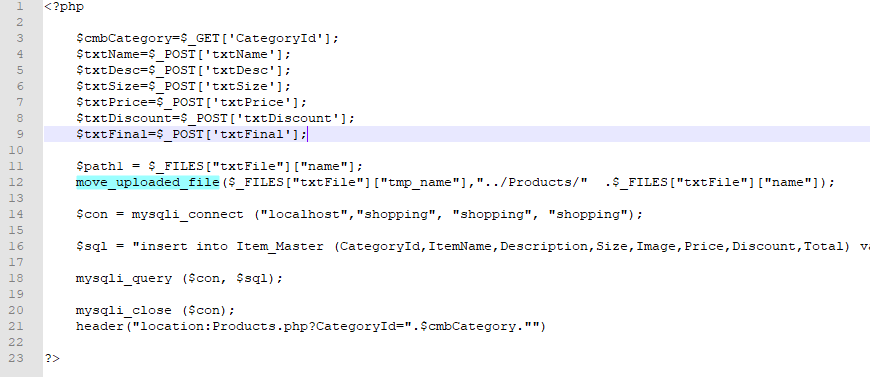
Online Clothing Store对商品图片的文件格式未做限制导致可以上传php文件执行php代码。

# 二、机理分析

## 1、任意文件上传漏洞

**影响版本：**1.0

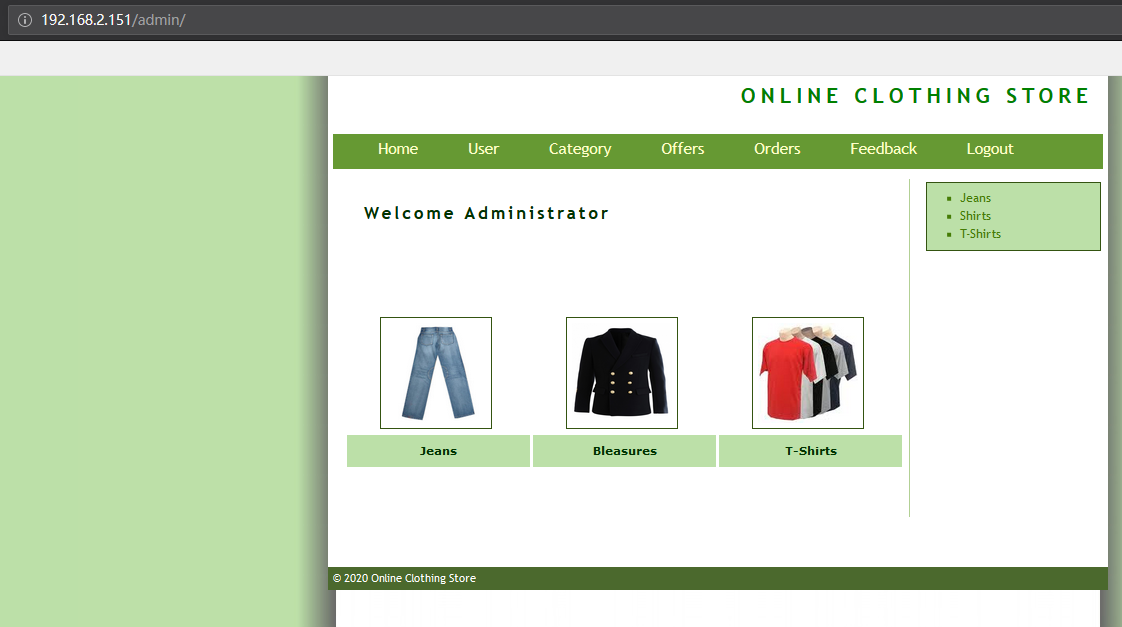
**漏洞编号：**无



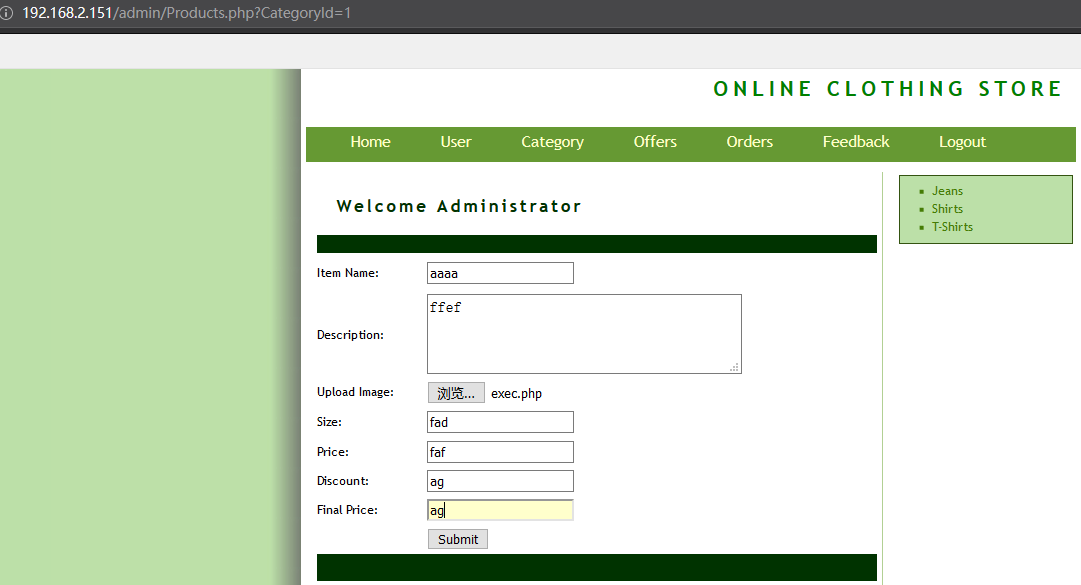
关键代码如图：上传的文件未做任何限制，然后用move\_uploaded\_file函数来处理上传文件。

# 三、攻击路径

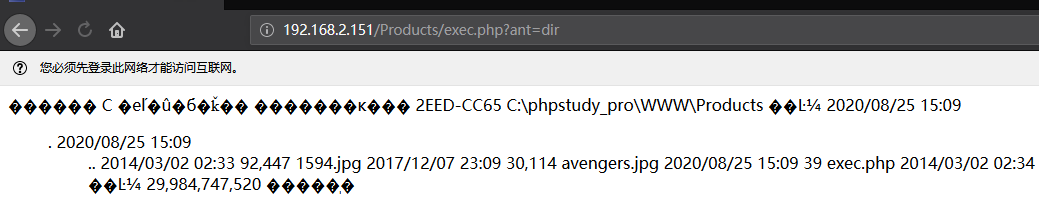
访问/admin即可无密码到后台



上传php木马



文件路径为/Products/exec.php



# 四、防御方案

上传图片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。