SQL Injection in Online Class and Exam Scheduling System via /salut_del.php endpoint

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\salut_del.php(8) 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

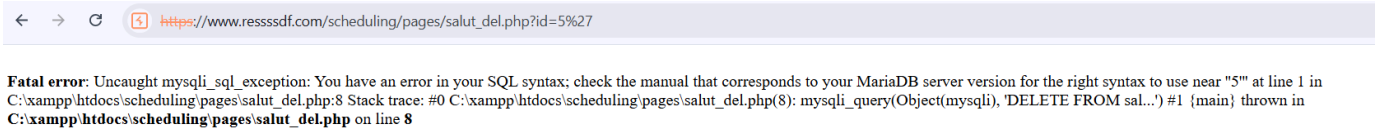
Description of the vulnerability

/salut_del.php endpoint 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.

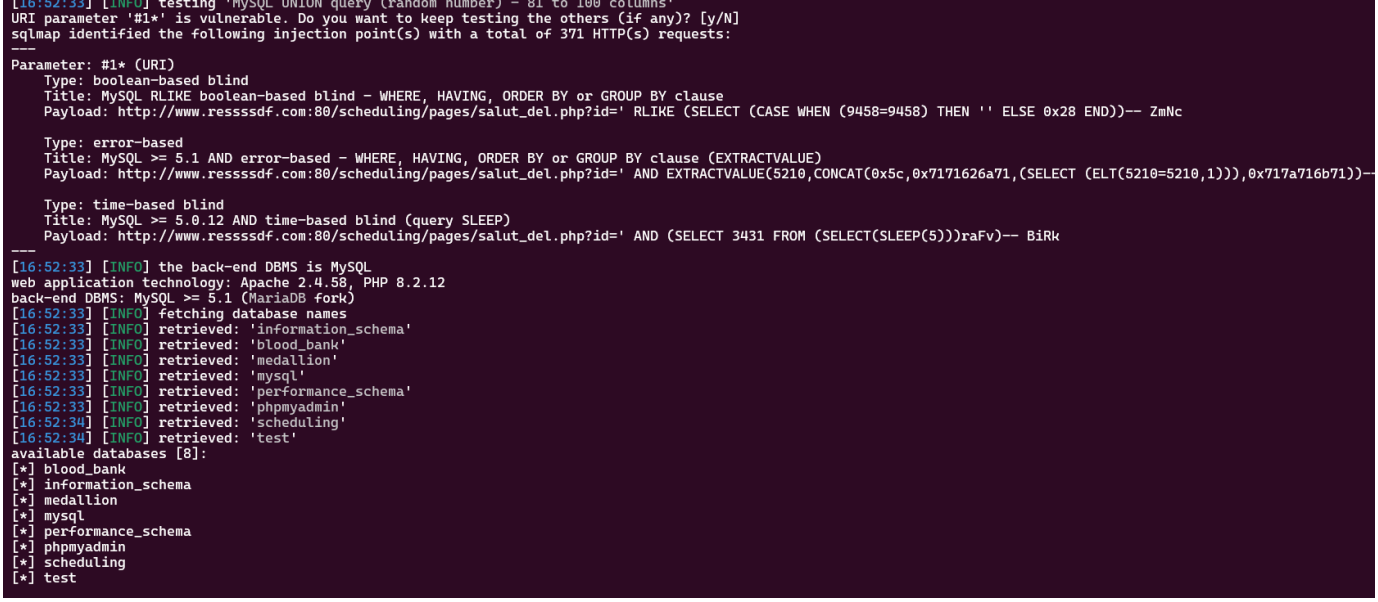
Vulnerability recurrence

POC

1. Login into the application as Admin privilege user
2. Once logged in, navigate to /scheduling/pages/salut_del.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.



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/salut_del.php?id=
```