

devcode-it / openstamanager Public

<> Code Issues 188 Pull requests 11 Actions Projects Security and qu

Commit 50b9089



Pek5892 committed on Mar 5

fix: Time-Based Blind SQL Injection via options[stato] Parameter

v2.10 · v2.10.3 v2.10.2

1 parent [679c40f](#) commit 50b9089

3 files changed +3 -2 lines changed

[↑ Top](#)

- ✓ modules
 - ✓ contratti/ajax
 - select.php
 - ✓ ordini/ajax
 - select.php
 - ✓ preventivi/ajax
 - select.php

3 files changed +3 -2 lines changed



modules/contratti/ajax/select.php ...

```

@@ -57,7 +57,7 @@
57 57          $stato = !empty($superselect['stato']) &&
          in_array($superselect['stato'], $allowed_stati)
58 58          ? $superselect['stato']
59 59          : 'is_pianificabile';
60 -          $where[] = ' `idstato` IN (SELECT `id` FROM `co_staticcontratti` WHERE
          '.$stato.' = 1)';

```

```

60 +           $where[] = '`idstato` IN (SELECT `id` FROM `co_staticontratti` WHERE
        `'.str_replace('`', '`', $stato).` = 1)';
61 61         }
62 62
63 63         if (!empty($search)) {

```

modules/ordini/ajax/select.php

```

@@ -53,6 +53,7 @@
53 53         ? $superselect['stato']
54 54         : 'is_fatturabile';
55 55         $where[] = '`or_statiordine`.`.$stato.` = 1';
56 +           $where[] = '`or_statiordine`.`'.str_replace('`', '`', $stato).`
        = 1';
56 57         }
57 58     }
58 59

```

modules/preventivi/ajax/select.php

```

@@ -60,7 +60,7 @@
60 60         $stato = !empty($superselect['stato']) &&
        in_array($superselect['stato'], $allowed_stati)
61 61         ? $superselect['stato']
62 62         : 'is_pianificabile';
63 -           $where[] = '(`.$stato.` = 1)';
63 +           $where[] = '(`'.str_replace('`', '`', $stato).` = 1)';
64 64         }
65 65
66 66         if (!empty($search)) {

```

Comments 0



Please [sign in](#) to comment.