devcode-it / **openstamanager** Public

Code | Issues 188 | Pull requests 11 | Actions | Projects | Security and qu

Commit `679c40f`

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 d2e38cb commit 679c40f

3 files changed +12 -3 lines changed

Top

Filter files...

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

3 files changed +12 -3 lines changed

Search within code

modules/contratti/ajax/select.php

```
@@ -53,7 +53,10 @@
53  53
54  54             if (empty($elements)) {
55  55                 $where[] =
    '`an_anagrafiche`.`idanagrafica`='.prepare($superselect['idanagrafica']);
56      -              $stato = !empty($superselect['stato']) ? $superselect['stato'] :
    'is_pianificabile';
```

```
                $allowed_stati = ['is_pianificabile', 'is_completato', 'is_fatturabile'];
                $stato = !empty($superselect['stato']) && in_array($superselect['stato'], $allowed_stati)
                    ? $superselect['stato']
                    : 'is_pianificabile';
                $where[] = '`idstato` IN (SELECT `id` FROM `co_staticontratti` WHERE '.$stato.' = 1)';
            }
```

modules/ordini/ajax/select.php

```
@@ -48,7 +48,10 @@
                if (empty($elements)) {
                    $where[] = '`an_anagrafiche`.`idanagrafica`='.prepare($superselect['idanagrafica']);

-                   $stato = !empty($superselect['stato']) ? $superselect['stato'] : 'is_fatturabile';
+                   $allowed_stati = ['is_fatturabile', 'is_evadibile', 'is_completato'];
+                   $stato = !empty($superselect['stato']) && in_array($superselect['stato'], $allowed_stati)
+                       ? $superselect['stato']
+                       : 'is_fatturabile';
                    $where[] = '`or_statiordine`.'.$stato.' = 1';
                }
            }
```

modules/preventivi/ajax/select.php

```
@@ -56,7 +56,10 @@
                    $where[] = '`an_anagrafiche`.`idanagrafica`='.prepare($superselect['idanagrafica']);
                    $where[] = '`co_preventivi`.`default_revision`=1';

-                   $stato = !empty($superselect['stato']) ? $superselect['stato'] : 'is_pianificabile';
```

```
59  +                   $allowed_stati = ['is_pianificabile', 'is_completato',
    'is_fatturabile', 'is_concluso'];
60  +                   $stato = !empty($superselect['stato']) &&
    in_array($superselect['stato'], $allowed_stati)
61  +                       ? $superselect['stato']
62  +                       : 'is_pianificabile';
60  63                  $where[] = '('.$stato.' = 1)';
61  64              }
62  65
```

Comments 0

Please sign in to comment.