

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 · v2.10.2

1 parent [d2e38cb](#) commit 679c40f

3 files changed +12 -3 lines changed

[↑ Top](#)

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

3 files changed +12 -3 lines changed



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';

```

```

56 +         $allowed_stati = ['is_pianificabile', 'is_completato',
57 +         'is_fatturabile'];
58 +         $stato = !empty($superselect['stato']) &&
59 +         in_array($superselect['stato'], $allowed_stati)
60 +         ? $superselect['stato']
61 +         : 'is_pianificabile';
62
63 $where[] = `idstato` IN (SELECT `id` FROM `co_staticontratti` WHERE
64 `.$stato.` = 1)';
65
66 }
67
68 }
69
70 }

```

modules/ordini/ajax/select.php

```

@@ -48,7 +48,10 @@
48 48         if (empty($elements)) {
49 49             $where[] =
50 50                 '`an_anagrafiche`.`idanagrafica`='.prepare($superselect['idanagrafica']);
51 51             $stato = !empty($superselect['stato']) ? $superselect['stato'] :
52 52                 'is_fatturabile';
53 53             $allowed_stati = ['is_fatturabile', 'is_evadibile',
54 54                 'is_completato'];
55 55             $stato = !empty($superselect['stato']) &&
56 56                 in_array($superselect['stato'], $allowed_stati)
57 57                 ? $superselect['stato']
58 58                 : 'is_fatturabile';
59 59
60 60             $where[] = `or_statiordine`.`.$stato.` = 1';
61 61
62 62         }
63 63     }
64 64 }

```

modules/preventivi/ajax/select.php

```

@@ -56,7 +56,10 @@
56 56         $where[] =
57 57             '`an_anagrafiche`.`idanagrafica`='.prepare($superselect['idanagrafica']);
58 58             $where[] = `co_preventivi`.`default_revision`=1';
59 59
60 60             $stato = !empty($superselect['stato']) ? $superselect['stato'] :
61 61                 'is_pianificabile';

```

```
59 +         $allowed_stati = ['is_pianificabile', 'is_completato',
60 +         'is_fatturabile', 'is_concluso'];
61 +         $stato = !empty($superselect['stato']) &&
62 +         in_array($superselect['stato'], $allowed_stati)
63 +         ? $superselect['stato']
64 +         : 'is_pianificabile';
65
66     $where[] = '('.$stato.' = 1)';
67 }
68 }
```

Comments 0



Please [sign in](#) to comment.