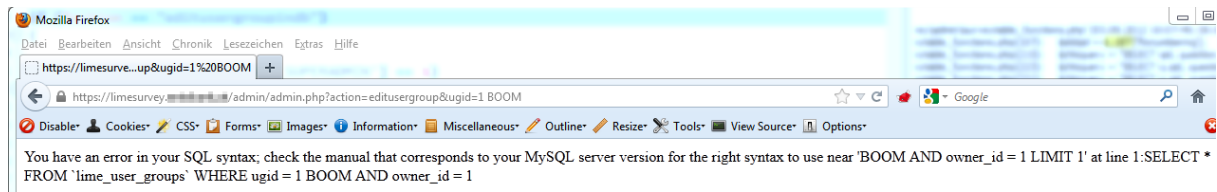


1.4 EditUserGroup – parameter: “ugid”



The vulnerable SQL statement gets constructed in “userrighthandling.php”:

```
userrighthandling.php x
636 if ($action == "editusergroup")
637 {
638     if ($_SESSION['USER_RIGHT_SUPERADMIN'] == 1)
639     {
640         $query = "SELECT * FROM ".db_table_name('user_groups')." WHERE ugid = ".$_GET['ugid']."' AND owner_id = ".$_SESSION[
641         $result = db_select_limit_assoc($query, 1);
642         $esrow = $result->FetchRow();
```