Commit f743b97

phili67 authored last week · ✓ 3 / 3 · Verified

```
Merge pull request #2861 from phili67/phili67-queryview-sql-injecttion-res
src/v2/templates/query/queryview.php : sql injection + gui update
```

master (#2861)

2 parents 0e827d5 + f204e92 commit f743b97

1 file changed +36 -7 lines changed ↑ Top

Filter files…

src/v2/templates/query

queryview.php

1 file changed +36 -7 lines changed Search within code

src/v2/templates/query/queryview.php

```
@@ -13,6 +13,7 @@
13 13   use EcclesiaCRM\Utils\InputUtils;
14 14   use EcclesiaCRM\Utils\MiscUtils;
15 15   use EcclesiaCRM\dto\Cart;
   16 + use EcclesiaCRM\SessionUser;
16 17
17 18   //Loops through all the parameters and ensures validation rules have been followed
18 19   function ValidateInput($rsParameters, $POST)
@@ -35,6 +36,8 @@ function ValidateInput($rsParameters, $POST)
35 36               $aErrorText[$qrp_Alias] = _('This value is required.');
36 37           } //Assuming there was no error above...
37 38           else {
```

```
      39  +             $ret = '';
      40  +
  38  41                //Validate differently depending on the contents of the
                      qrp_Validation field
  39  42                switch ($qrp_Validation) {
  40  43                    //Numeric validation
          @@ -56,7 +59,7 @@ function ValidateInput($rsParameters, $POST)
  56  59                            }
  57  60                        }
  58  61
  59      -                     $vPOST[$qrp_Alias] =
                      InputUtils::LegacyFilterInput($POST[$qrp_Alias], 'int');
      62  +                     $ret = InputUtils::LegacyFilterInput($POST[$qrp_Alias],
                      'int');
  60  63                        break;
  61  64
  62  65                    //Alpha validation
          @@ -72,13 +75,17 @@ function ValidateInput($rsParameters, $POST)
  72  75                            $aErrorText[$qrp_Alias] = _('This value cannot be less
                      than ') . $qrp_AlphaMinLength . _(' characters long');
  73  76                        }
  74  77
  75      -                     $vPOST[$qrp_Alias] =
                      InputUtils::LegacyFilterInput($POST[$qrp_Alias]);
      78  +                     $ret = InputUtils::LegacyFilterInput($POST[$qrp_Alias]);
  76  79                        break;
  77  80
  78  81                    default:
  79      -                     $vPOST[$qrp_Alias] = $POST[$qrp_Alias];
      82  +                     $ret = InputUtils::LegacyFilterInput($POST[$qrp_Alias]);
  80  83                        break;
  81  84                }
      85  +
      86  +             if (!empty($ret) || $ret === '0') {
      87  +                 $vPOST[$qrp_Alias] = $ret;
      88  +             }
  82  89            }
  83  90        }
  84  91
          @@ -95,10 +102,16 @@ function ProcessSQL($vPOST, $qry_SQL, $rsParameters)
```

```
95  102         while ($aRow = mysqli_fetch_array($rsParameters)) {
96  103             extract($aRow);
97  104
    105 +         if (!isset($vPOST[$qrp_Alias])) {
    106 +             return "";
    107 +         }
    108 +
98  109             //Debugging code
    110 +         if (SessionUser::getUser()->isAdmin()) {
99  111             ?>
100 112             <?= "--" . $qry_SQL ?><br>-- ~<?= $qrp_Alias ?>~<br>--<?=
                $vPOST[$qrp_Alias] ?><p>
101 113             <?php
    114 +         }
102 115             //Replace the placeholder with the parameter value
103 116             $qry_SQL = str_replace('~' . $qrp_Alias . '~', $vPOST[$qrp_Alias],
                $qry_SQL);
104 117         }
                @@ -238,15 +251,23 @@ class="btn btn-danger btn-sm"> <i class="fas fa-
                times"></i> <?= _('Remove From C
238 251             </div>
239 252
240 253         </div>
    254 +     </div>
241 255
    256 +     <?php if (SessionUser::getUser()->isAdmin()) { ?>
242 257         <div class="card card-info">
243 258             <div class="card-header border-1">
244 259                 <div class="card-title">Query</div>
245 260             </div>
246 261             <div class="card-body">
247     -               <code><?= str_replace(chr(13), '<br>', htmlspecialchars($qry_SQL));
                ?></code>
    262 +               <code>
    263 +               <?php
    264 +                       echo str_replace(chr(13), '<br>',
                htmlspecialchars($qry_SQL));
    265 +               ?>
    266 +               </code>
248 267             </div>
```

```
249  268          </div>
     269  +       <?php }
     270  +       ?>
250  271
251  272          <script nonce="<?= $CSPNonce ?>">
252  273              var aAddToCartIDs = <?= json_encode($aAddToCartIDs) ?>;
     @@ -450,8 +471,9 @@ function DisplayParameterForm($rsParameters, $iQueryID,
     $sRootPath)
450  471                              } ?>
451  472
452  473                              <div class="form-group text-right">
453       -                              <input class="btn btn-primary" type="Submit"
     value="<?= _("Execute Query") ?>"
454       -                                      name="Submit">
     474  +                              <button class="btn btn-success btn-lg shadow-sm
     font-weight-bold py-2 px-4" type="submit" name="Submit">
     475  +                                  <i class="fas fa-play mr-2"></i> <?= _("Execute
     Query") ?>
     476  +                              </button>
455  477                              </div>
456  478                          </form>
457  479
     @@ -488,7 +510,14 @@ function DisplayParameterForm($rsParameters, $iQueryID,
     $sRootPath)
488  510              //No errors; process the SQL, run the query, and display the results
489  511              DisplayQueryInfo($qry_Name, $qry_Description);
490  512              $qry_SQL = ProcessSQL($vPOST, $qry_SQL, $rsParameters);
491       -            DoQuery($cnInfoCentral, $aRowClass, $rsQueryResults, $qry_SQL,
     $iQueryID, $qry_Name, $qry_Count, $CSPNonce, $sRootPath);
     513  +            if (empty($qry_SQL)) {
     514  +                echo '<div class="alert alert-danger">' . _('An error occurred
     while processing the SQL for this query. Please check your parameter values and
     try again.') . '</div>';
     515  +                DisplayParameterForm($rsParameters, $iQueryID, $sRootPath);
     516  +                require $sRootDocument . '/Include/Footer.php';
     517  +                exit;
     518  +            } else {
     519  +                DoQuery($cnInfoCentral, $aRowClass, $rsQueryResults, $qry_SQL,
     $iQueryID, $qry_Name, $qry_Count, $CSPNonce, $sRootPath);
     520  +            }
```

```
492  521          } else {
493  522              //Yes, there were errors; re-display the parameter form (the
                 DisplayParameterForm function will
494  523              //pick up and display any error messages)
```

Comments 0

Please sign in to comment.