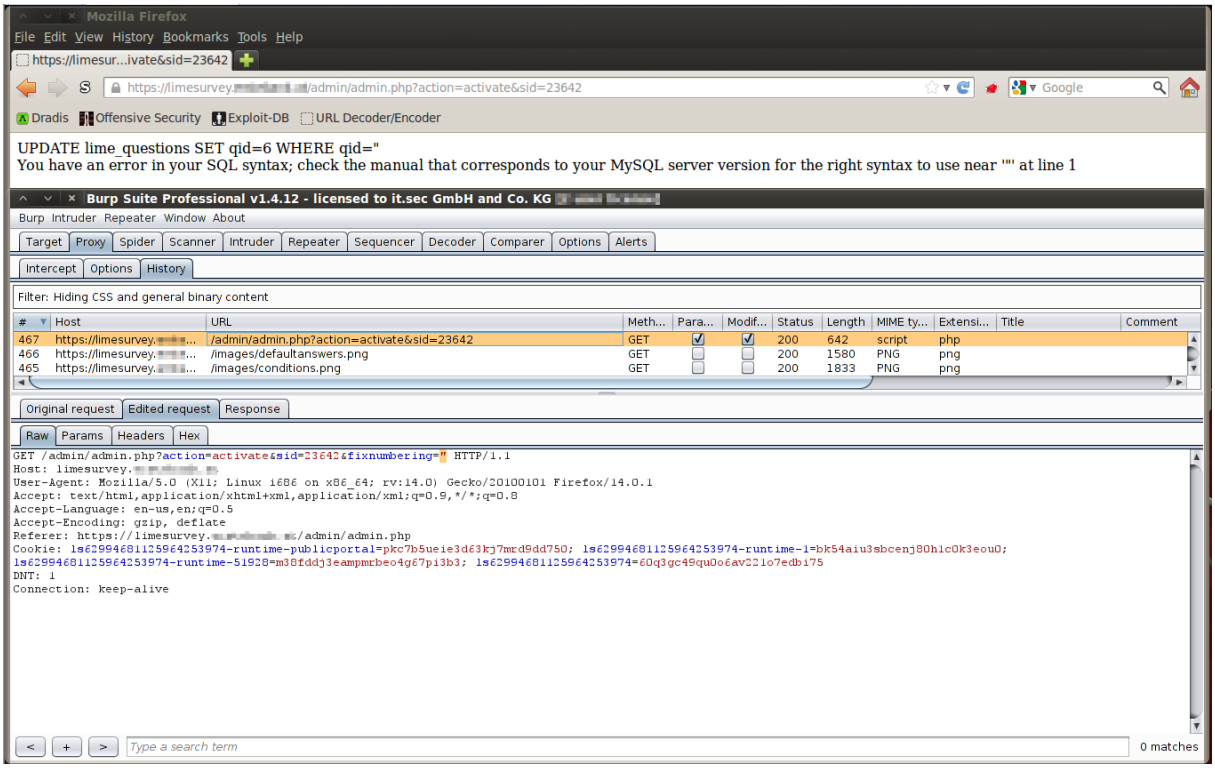
1.2 Activate Survey (activate_functions.php) – parameter: "fixnumbering"



The vulnerable parameter gets passed in file "**activate.php**" to the function fixNumbering:

```
activate.php
24  if (!isset($_POST['ok']) || !$_POST['ok'])
25  {
26      if (isset($_GET['fixnumbering']) && $_GET['fixnumbering'])
27      {
28          fixNumbering($_GET['fixnumbering']);
29      }
```

This value is then used to update a database entry in file "**activate_functions.php**":

```
activate.php | activate_functions.php
23  function fixNumbering($fixnumbering)
24  {
25
26      global $dbprefix, $connect, $clang, $surveyid;
27
28      LimeExpressionManager::RevertUpgradeConditionsToRelevance($surveyid);
29      //Fix a question id - requires renumbering a question
30      $oldqid = $fixnumbering;
31      $query = "SELECT qid FROM {$dbprefix}questions ORDER BY qid DESC";
32      $result = db_select_limit_assoc($query, 1) or safe_die($query."<br />".$connect->ErrorMsg());
33      while ($row=$result->FetchRow()) {$lastqid=$row['qid'];}
34      $newqid=$lastqid+1;
35      $query = "UPDATE {$dbprefix}questions SET qid=$newqid WHERE qid=$oldqid";
36      $result = $connect->Execute($query) or safe_die($query."<br />".$connect->ErrorMsg());
37      // Update subquestions
38      $query = "UPDATE {$dbprefix}questions SET parent_qid=$newqid WHERE parent_qid=$oldqid";
39      $result = $connect->Execute($query) or safe_die($query."<br />".$connect->ErrorMsg());
```