

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

UPDATE lime.questions SET qid=6 WHERE qid=

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "" at line 1

Burp Suite Professional v1.4.12 - licensed to it.sec GmbH and Co. KG

#	Host	URL	Meth...	Para...	Modif...	Status	Length	MIME ty...	Extensi...	Title	Comment
467	https://limesurvey.	/admin/admin.php?action=activate&sid=23642	GET	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	200	642	script	php		
466	https://limesurvey.	/images/defaultanswers.png	GET	<input type="checkbox"/>	<input type="checkbox"/>	200	1580	PNG	png		
465	https://limesurvey.	/images/conditions.png	GET	<input type="checkbox"/>	<input type="checkbox"/>	200	1833	PNG	png		

Original request | Edited request | Response

Raw Params Headers Hex

```
GET /admin/admin.php?action=activate&sid=23642&fixnumbering= HTTP/1.1
Host: limesurvey. ....
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:14.0) Gecko/20100101 Firefox/14.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://limesurvey. .... /admin/admin.php
Cookie: ls629946811259e4253974-runtime-publicportal=pkc7b5ueie3d63k37mrdd750; ls629946811259e4253974-runtime-1=bk54aiu3sbcenj80hlc0k3eou0; ls629946811259e4253974-runtime-519c8=m38fddj3eampmrbeo4g67pi3b3; ls629946811259e4253974=60q3gc49quDo6av221o7edb1v5
DNT: 1
Connection: keep-alive
```

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

```
activate.php x
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 x
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());
```