Lasso - Bug #45581

Lasso fail to properly escape single quotes in RelayState

30 juillet 2020 03:25 - Emmanuel Dreyfus

Statut:	Fermé	**Début:**	30 juillet 2020
Priorité:	Normal	**Echéance:**	
Assigné à:	Benjamin Dauvergne	**% réalisé:**	0%
Catégorie:	Core	**Temps estimé:**	0:00 heure
Version cible:	2.6.2		
Patch proposed:	Oui	**Planning:**	Non

Description

lasso uses libxml2's xmlURIEscapeStr() to URL-encode parameters in query strings. This function implements RFC 2396 URL encoding, which does not mandates escaping the single quote. As a result, lasso produces RelayState parameters with single quotes unescaped in the query string.

Unfortunately, browers automatically replace single quotes in query string by %27. The IdP gets a RelayState where the single quote was replaced by %27, while the signature is based on a RelayState containing an unescaped single quote. This causes the IdP to reject the request because the signature does not match.

The proposed fix in attached patch is to implement RFC 3986 compliant URL encoding, where all characters except the unreserved class [A-Za-z0-9._~-] are escaped. This is done in a lasso_xmlURIEscapeStr() function which is a drop-in replacement for xmlURIEscapeStr()

Révisions associées

Révision 0b742b1f - 14 août 2020 10:58 - Benjamin Dauvergne

tools: reimplement xmlURIEscapeStr to respect RFC3986 (#45581)

Bugfix by Emmanuel Dreyfus.

License: MIT

Historique

#1 - 11 août 2020 11:17 - Benjamin Dauvergne

- Assigné à mis à Benjamin Dauvergne

#2 - 11 août 2020 11:30 - Benjamin Dauvergne

I need a statement here that you contribute under MIT license then I will commit your patch with attribution.

#3 - 11 août 2020 15:31 - Benjamin Dauvergne

- Statut changé de Nouveau à Solution validée

#4 - 11 août 2020 15:32 - Benjamin Dauvergne

- Version cible changé de future à 2.6.2

#5 - 12 août 2020 01:42 - Emmanuel Dreyfus

> I need a statement here that you contribute under MIT license then I will commit your patch with attribution.

I contribute the patch under MIT license.

#6 - 14 août 2020 10:58 - Benjamin Dauvergne

- Statut changé de Solution validée à Résolu (à déployer)

```
commit 390d306e6e87619bd56f766897332d76f81ddd39
Author: Benjamin Dauvergne <bdauvergne@entrouvert.com>
```

```
Date:   Tue Aug 11 11:30:51 2020 +0200

    tools: reimplement xmlURIEscapeStr to respect RFC3986 (#45581)

    Bugfix by Emmanuel Dreyfus.

    License: MIT
```

#7 - 04 septembre 2021 10:05 - Benjamin Dauvergne

- Statut changé de Résolu (à déployer) à Fermé

Fichiers

rfc3986.patch	6,18 ko	30 juillet 2020	Emmanuel Dreyfus