Authentic 2 - Bug #53716

Ne pas afficher le message invalide sur un pépin SAMLv2

04 mai 2021 11:38 - Thomas Noël

Statut:	Fermé	**Début:**	04 mai 2021
Priorité:	Normal	**Echéance:**	
Assigné à:	Thomas Noël	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	Non

Description

Exemple cette URL :

```
https://connexion.example.net/idp/saml2/sso?<html><br><script>alert('xss')</script></html>
```

Va afficher ce message en text/plain :

```
SAMLv2 Single Sign On: message invalide pour le profil utilisant le binding HTTP-RedirectÂ : '%3Ch
tml%3E%3Cbr%3E%3Cscript%3Ealert(%27xss%27)%3C/script%3E%3C/html%3E'
```

Or certains navigateurs interprètent tout de même cela comme du HTML avec du Javascript... et exécute ce dernier.

De là pourra émerger une injection javascript.

Pour l'éviter on pourrait tout simplement ne pas afficher le message invalide.

Révisions associées

Révision fb43ef51 - 04 mai 2021 14:32 - Thomas Noël

saml: do not show invalid SSO message to end-user (#53716)

Historique

#1 - 04 mai 2021 12:14 - Thomas Noël

- Assigné à mis à Thomas Noël

#2 - 04 mai 2021 12:17 - Thomas Noël

- Fichier 0001-saml-do-not-show-invalid-SSO-message-to-end-user-537.patch ajouté

- Statut changé de Nouveau à Solution proposée

- Patch proposed changé de Non à Oui

#3 - 04 mai 2021 13:08 - Benjamin Dauvergne

- Statut changé de Solution proposée à Solution validée

Ok.

#4 - 04 mai 2021 14:32 - Thomas Noël

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

```
commit fb43ef51e13fd650d3962ca96c7c8a0eec9f1f5c
Author: Thomas NOËL <tnoel@entrouvert.com>
Date:   Tue May 4 12:15:49 2021 +0200

    saml: do not show invalid SSO message to end-user (#53716)
```

#5 - 07 mai 2021 15:16 - Frédéric Péters

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

Fichiers

0001-saml-do-not-show-invalid-SSO-message-to-end-user-537.patch	1,14 ko	04 mai 2021	Thomas Noël