Authentic 2 - Bug #89451

sur un/idp/saml2/slo_return ne pas afficher de bouton vers l'URL "next" en cas d'erreur

11 avril 2024 17:15 - Thomas Noël

Statut:	Nouveau	**Début:**	11 avril 2024
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Non	**Planning:**	Non

Description

On imagine qu'un attaquant forge une URL /idp/saml2/slo_return?next=//autre-site.fr

Dans ce cas, on arrive sur une page d'erreur « slo no relay state in response », mais sur laquelle il y a un bouton « Continuer » qui pointe vers « autre-site.fr » L'utilisateur pourrait cliquer dessus pensant rester "en confiance", alors que non.

Il faudrait interdire ça, ie ne pas afficher le bouton dans ce cas.

Une autre solution serait de vérifier la valeur de next= mais j'ai l'impression qu'on peut toujours permettre un retour vers le site de départ, qui peut être "n'importe où" ?