Authentic 2 - Development #18449

conserver dans la session de l'utilisateur la dernière requête d'authent saml

05 septembre 2017 11:47 - Frédéric Péters

Statut:	Fermé	**Début:**	05 septembre 2017
Priorité:	Normal	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0:00 heure
Version cible:			
Patch proposed:	Oui	**Planning:**	

Description

L'idée derrière c'est ensuite de pouvoir regarder là-dedans pour du traitement spécifique, genre lire le <samlp:Extensions> et en extraire une info qui permettrait de déterminer si la requête d'origine vient d'un frontoffice ou d'un backoffice.

Là-dessus je pensais simplement faire :

```
+++ b/src/authentic2/idp/saml/saml2_endpoints.py
@@ -443,6 +443,7 @@ def sso(request):
     while True:
         try:
             login.processAuthnRequestMsg(message)
+            request.session['saml:authnRequest'] = login.request.dump()
             break
         except (lasso.ProfileInvalidMsgError,
             lasso.ProfileMissingIssuerError,), e:
```

Mais à tester, la gestion de samlp:Extensions dans Lasso ne fait rien, ça laisse juste passer n'importe quoi dedans, sans s'interposer, mais sans le mettre à disposition. Alors comme je ne me sens pas d'engager des modifications dans Lasso pour gérer ça maintenant, ça m'irait de stocker le message d'origine, et le gérer derrière moi-même (à coups d'urlparse, base64.decodestring et zlib.uncompress).

```
+++ b/src/authentic2/idp/saml/saml2_endpoints.py
@@ -443,6 +443,7 @@ def sso(request):
     while True:
         try:
             login.processAuthnRequestMsg(message)
+            request.session['saml:authnRequest'] = message
             break
         except (lasso.ProfileInvalidMsgError,
             lasso.ProfileMissingIssuerError,), e:
```

Révisions associées

Révision 94e9b95b - 09 septembre 2017 19:28 - Frédéric Péters

saml: keep latest authnRequest in session (#18449)

Historique

#1 - 05 septembre 2017 11:55 - Benjamin Dauvergne

Le code de samlp2_extension.c contient ça:

```
>-------nclass->node_data->keep_xmlnode = TRUE;
```

donc normalement au dump on ressort ce qui est rentré, donc tu dois pouvoir t'éviter le decodestring et le zlib.uncompress et n'avoir qu'à faire le ET.fromstring().

Mais après on agit où ? Il faudrait que le décorateur login_required() au lieu d'envoyer vers /login/?next=/idp/saml/continuesso envoie vers /accounts/oidc/login?next=... ou alors faut modifier la vue login pour gérer ce cas.

Ça m'irait qu'on finisse dans la vue login la gestion du comportement "si un seul auth_frontend sans IHM, faire une redirection immédiatement" et qu'on ait un hook à cet endroit qui réduise la liste des frontends en fonction du contexte.

#2 - 05 septembre 2017 12:07 - Frédéric Péters

Et pourtant, le contenu de Extensions ne se retrouve pas lors d'un login.request.dump() (ce que je notais en début de ticket), démonstration :

```
(Pdb) l
442         signed = True
443         while True:
444             try:
445                 login.processAuthnRequestMsg(message)
446                 import pdb; pdb.set_trace()
447  ->             request.session['saml:authnRequest'] = message
448                 break
449             except (lasso.ProfileInvalidMsgError,
450                 lasso.ProfileMissingIssuerError,), e:
451                 logger.warning('invalid message for WebSSO profile with '
452                                'HTTP-Redirect binding: %r exception: %s' \
```

```
(Pdb) print login.request.dump()
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0
:assertion" ID="_7CC6125DC5BA6F2DCD1EF92BD7D75AE6" Version="2.0" IssueInstant="2017-09-05T09:45:37Z" Destinati
on="https://authentic.fred.local.0d.be/idp/saml2/sso" SignType="0" SignMethod="0" ForceAuthn="false" IsPassive
="false"><saml:Issuer>https://combo.fred.local.0d.be/accounts/mellon/metadata/</saml:Issuer><samlp:NameIDPolic
y AllowCreate="true"/></samlp:AuthnRequest>
```

```
(Pdb) import urlparse, base64, zlib
(Pdb) print zlib.decompress(base64.decodestring(urlparse.parse_qs(message)['SAMLRequest'][0]), -15)
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0
:assertion" xmlns:eo="https://www.entrouvert.com/ns/lasso" ID="_7CC6125DC5BA6F2DCD1EF92BD7D75AE6" Version="2.0
" IssueInstant="2017-09-05T09:45:37Z" Destination="https://authentic.fred.local.0d.be/idp/saml2/sso" ForceAuth
n="false" IsPassive="false"><saml:Issuer>https://combo.fred.local.0d.be/accounts/mellon/metadata/</saml:Issuer
><samlp:Extensions>
                            <eo:next_url>hello</eo:next_url>
                          </samlp:Extensions><samlp:NameIDPolicy AllowCreate="true"/></samlp:AuthnRequest>
```

> Mais après on agit où ?

Là sur l'immédiat besoin guichet, très facilement, sans toucher davantage authentic, ça serait :

- un filtre |is_from_backoffice
- un template de login oidc modifié pour avoir :
  - un message de redirection
  -
  - et du js pour envoyer du côté qui convient

Après, avec du temps devant moi, je n'aurai aucun problème pour repasser là-dessus et participé à une conception plus générale.

#3 - 05 septembre 2017 13:12 - Benjamin Dauvergne

Ok ça me va.

#4 - 05 septembre 2017 13:15 - Benjamin Dauvergne

Je viens de regarder on peut obtenir le noeud XML d'origine via LassoNode.getOriginalXmlnode() pour les noeuds qui ont le flag keep_xmlnode, si ça peut éviter de garder toute la requête dans un format pas terrible, me semble qu'on a aussi keep_xmlnode sur les noeuds requêtes, réponses et assertions.

#5 - 05 septembre 2017 13:16 - Benjamin Dauvergne

Et ça renvoie une chaîne avec le XML sérialisé vu que je n'ai pas de passerelle xmlNode <-> lxml dans le binding Lasso.

#6 - 05 septembre 2017 13:29 - Frédéric Péters

- Fichier 0001-saml-keep-latest-authnRequest-in-session-18449.patch ajouté

- Statut changé de Nouveau à En cours

- Patch proposed changé de Non à Oui

Yep, c'est quand même mieux de ne pas devoir refaire le décodage de la requête.

#7 - 09 septembre 2017 14:08 - Frédéric Péters

Ça pourrait être poussé ? (dans l'idée d'introduire ça dans la mise à jour du 14)

#8 - 09 septembre 2017 19:20 - Benjamin Dauvergne

Ack.

#9 - 09 septembre 2017 19:28 - Frédéric Péters

- Statut changé de En cours à Résolu (à déployer)

```
commit 94e9b95b8b2ef3584a6b86d95d91508449a40fe0
Author: Frédéric Péters <fpeters@entrouvert.com>
Date:   Tue Sep 5 13:27:36 2017 +0200

    saml: keep latest authnRequest in session (#18449)
```

#10 - 06 décembre 2017 12:16 - Benjamin Dauvergne

- Statut changé de Résolu (à déployer) à Fermé

Fichiers

0001-saml-keep-latest-authnRequest-in-session-18449.patch	1,04 ko 05 septembre 2017	Frédéric Péters