Lazy Session

Általában a Shibboleth SP Apache modul csak akkor enged hozzáférést az erőforráshoz (oldalhoz), ha sikerült autentikálnia és autorizálnia a felhasználót (azaz shibboleth session-t létrehozni).

Elképzelhető azonban olyan alkalmazás is, amely azonosítatlan (anonymous) felhasználók számára **is** szolgáltat információkat. Ez a wiki is ezen az elven épül fel: bárki olvashatja, de csak bejelentkezett felhasználók szerkeszthetik.

A *lazy session* csak a Shibboleth szempontjából "lusta"; a modul csak akkor hoz létre Shibboleth session-t, ha az alkalmazás erre kifejezetten utasítja. Ez azzal jár, hogy:

- az alkalmazásnak tudnia kell, hogy mikor van érvényes Shibboleth session
- az alkalmazás felhasználói interfészén el kell helyezni egy olyan elemet (linket), melynek segítségével a session létrehozható
- magyarul: *csak Shibboleth-et "beszélő" alkalmazások védhetők lazy session-nel*.

Lazy session az alkalmazás szemszögéből

Session érvényességének ellenőrzése

Az alkalmazás a Shibboleth attribútumok vizsgálatával győződhet meg arról, hogy létezik-e Session. Célszerű olyan attribútumot választani, amely minden session létrehozáskor biztosan létrejön, ilyen például a **_SERVER** tömbből kinyerhető **Shib-Application-ID** (Shibboleth 1.3 esetén: **HTTP_SHIB_APPLICATION_ID**) header. Ha ez létezik, akkor biztosan van session.

Session létrehozás

Mivel a webszerveren futó alkalmazás és a Shibboleth webszerver modul közvetlenül nem tud kommunikálni, ezért szükséges, hogy a felhasználót valahogyan egy megfelelő URL-re (a SessionInitiator URL-jére). Ez az URL általában így áll össze:

- metódus: `http://` vagy `https://`
- hostnév

- Shibboleth SP modul elérhetősége (általában: `/Shibboleth.sso`)
- SessionInitiator "location"-je, pl. `/WAYF/HREF`
  - Milyen jó is lenne, ha a default session initiator akkor is menne, ha nem adunk meg location-t. De sajnos jelenleg nem ez a helyzet.
- `?target=` + az az URL, amelyre a Shibboleth session létrehozás után szeretnénk, hogy a felhasználónk kerüljön. Általában az éppen aktuális Request URI-t szoktuk használni.

Példa URL:

```
https://dev.aai.niif.hu/Shibboleth.sso/WAYF/NIIF-
WAYF?target=https://dev.aai.niif.hu/drupal/shiblazy.php
```

Request headerek megbízhatósága, lazy session biztonság

A Shibboleth modul gondoskodik arról, hogy kiszűrje a **HTTP_SHIB_** kezdetű header elemeket, mivel azokat csak ez a modul állíthatja be. Bárki más is állítaná be, az visszaélést jelentene (header spoofing). A header spoofing elleni védelem lazy session esetén is működik, függetlenül attól, hogy létrejött-e a Shibboleth session. Ez azt jelenti, hogy nem lehet létező "sessiont hazudni", mivel a **HTTP_SHIB_IDENTITY_PROVIDER** header védett.

Természetesen a spoofing védelem csak akkor működik, ha

- a Shibbleth webszerver modul (mod_shib) be van töltve ÉS
- az adott Directoryra vagy Location-re be van konfigurálva, hogy hallgasson

A _SERVER tömb elemeit csak webszerver modulok tölthetik fel, ezért az ebből kivett értékek többé-kevésbé megbízhatóak header spoofing védelem nélkül is (megbízhatóságuk megegyezik a webszerver megbízhatóságával). Problémát okoz azonban, ha ezeket az elemeket összekeverjük a requestből kinyerhető értékekkel (pl. PHP-ban a `register_globals` használatával). Ez amúgy is kerülendő eljárás, lazy session-ök esetén pedig egyenesen öngyilkosság!

Változat #1
document-uploader hozta létre 2025-08-07 12:03:29 CEST
document-uploader frissítette 2025-08-07 12:03:29 CEST