

# CAS Logger

Systeme de log externe des tentatives de connexions au serveur CAS en temps réel

Jérôme Bousquié  
IUT de Rodez

CAS Logger

CAS

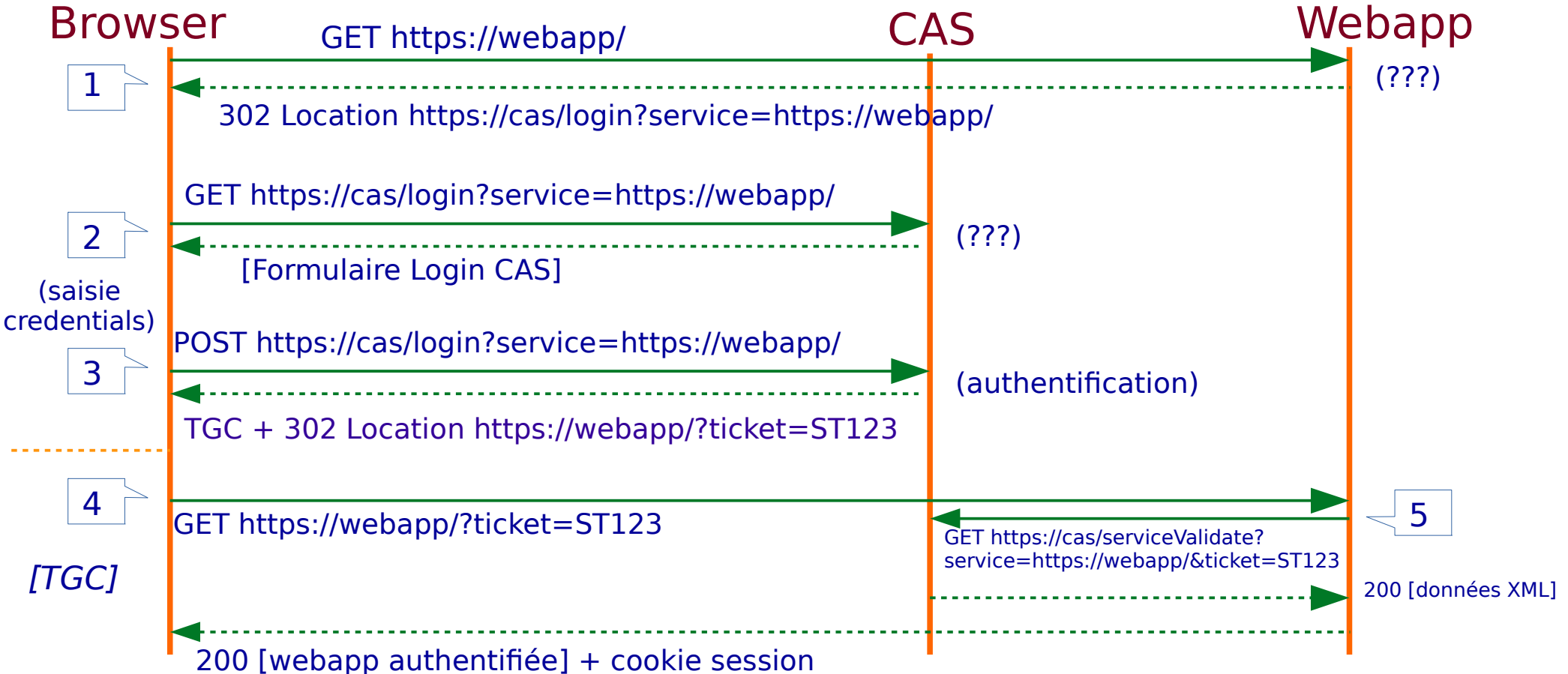
Central Authentication Service

SSO Web conçu par Yale

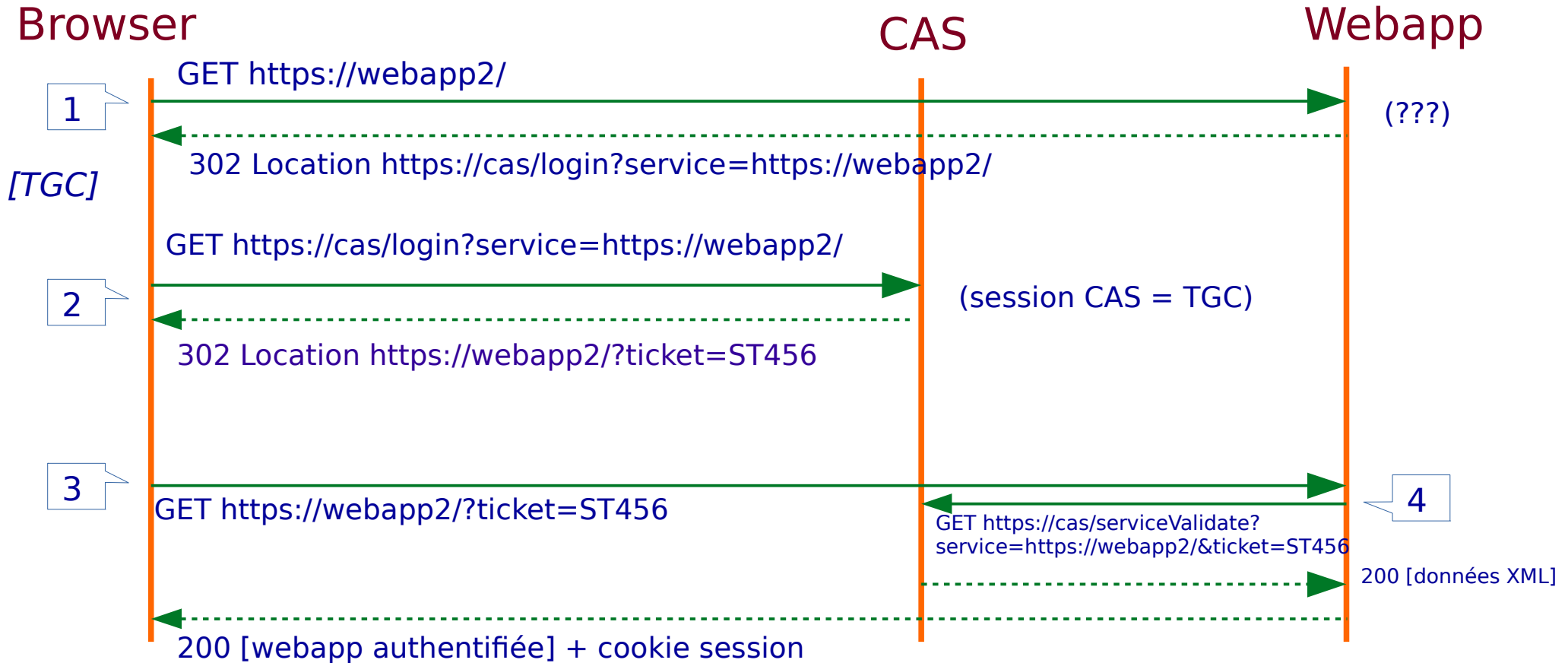
c'est un protocole et une architecture

Rappel ...

# CAS : premier accès



# CAS : applications suivantes



# CAS Logger

CAS est un point d'entrée majeur.

C'est donc bien de savoir en permanence :

Qui tente de l'utiliser ?

Depuis où ?

Pour faire quoi ?

Qui réussit à se connecter ?

CAS Logger

Mais CAS / JA-SIG c'est ...

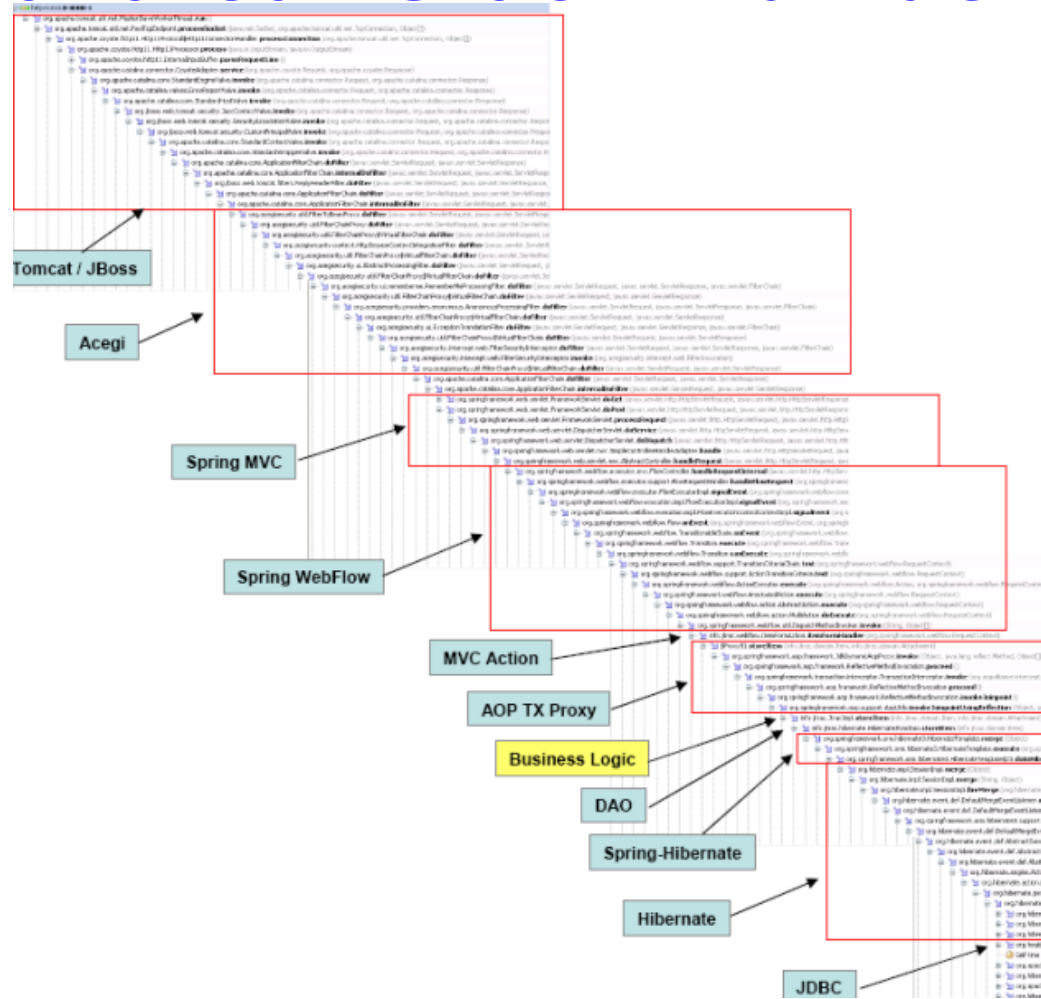
CAS Logger

Mais CAS / JA-SIG c'est ...



***TOMCAT JAVA ANT SPRING  
Aaaargggg...***

# Java Call Stack... un délice





# CAS Logger

Et pourtant ...

Que fait CAS 90 % du temps ?

Il compare deux chaînes de caractères :  
soit celle du TGC et de la session CAS,  
soit celles du ST du browser et de la  
webapp

Il renvoie un header http 302

# CAS Logger

On ne veut pas toucher au serveur.

Donc,  
on demande au client de logger.

CASLogger :

un tout petit serveur php/mysql  
un script javascript

# CAS Logger



```
<script src = https://caslogger/caslogger.js></script>
```

Entrez votre e-mail et votre mot de passe de l'IUT.

E-mail (ne pas saisir "@iut-rodez.fr"):

mister.magoo @iut-rodez.fr

Mot de passe:

Prévenez-moi avant d'accéder à d'autres services.

Pour des raisons de sécurité, veuillez vous déconnecter et fermer votre navigateur lorsque vous avez fini d'accéder aux services authentifiés.

Languages:  
[English](#) [Spanish](#) [French](#) [Russian](#) [Nederlands](#) [Svenskt](#) [Italiano](#) [Urdu](#) [Chinese](#)  
[\(Simplified\)](#) [Deutsch](#) [Japanese](#) [Croatian](#) [Czech](#) [Slovenian](#) [Polish](#) [Portuguese \(Brazil\)](#) [Turkish](#)

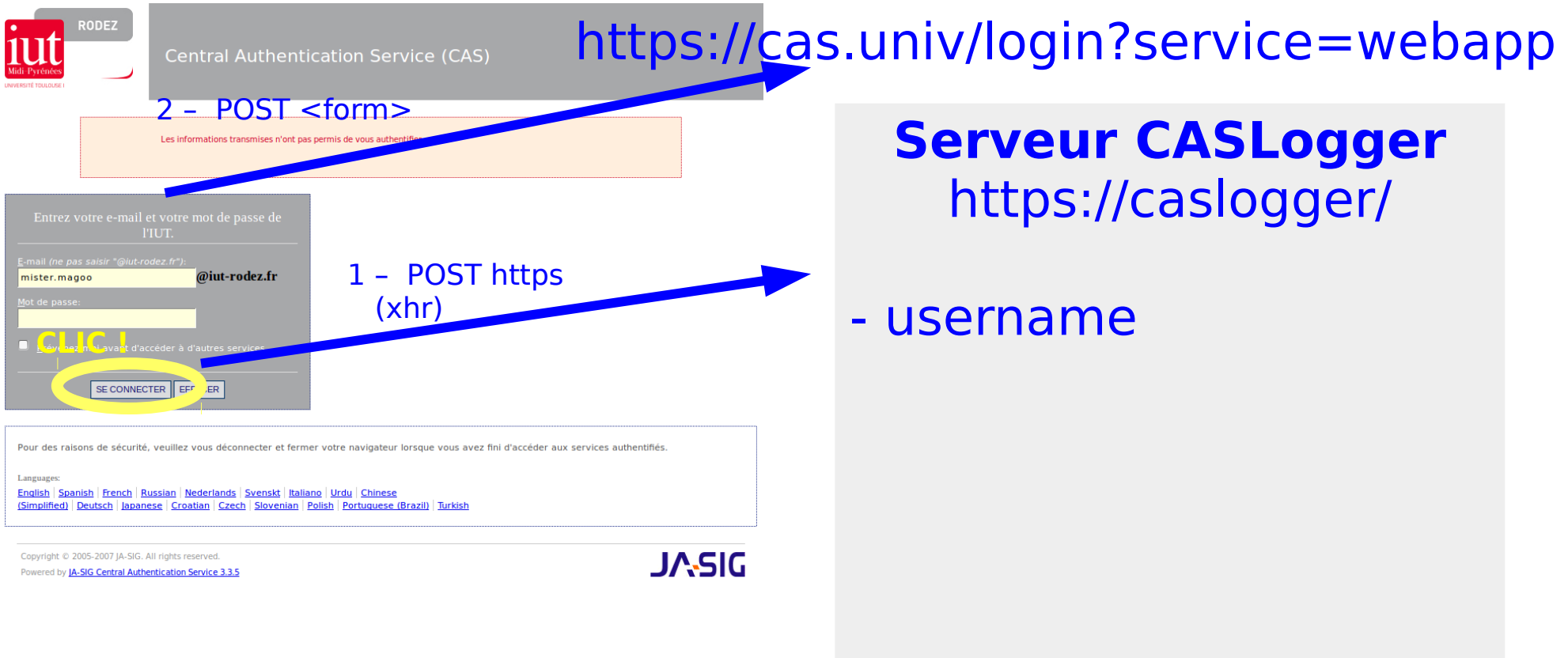
Copyright © 2005-2007 JA-SIG. All rights reserved.  
Powered by [JA-SIG Central Authentication Service 3.3.5](#)

JA-SIG

Une balise html `<script>` est ajoutée dans le fichier `top.jsp` pour charger le code dans le navigateur.

Pas besoin de redémarrer le serveur CAS.

# CAS Logger



# CAS Logger

Mais aussi ...

RODEZ  
iut  
Midi-Pyrénées  
UNIVERSITÉ TOULOUSE I

Central Authentication Service (CAS)

Les informations transmises n'ont pas permis de vous authentifier.

Entrez votre e-mail et votre mot de passe de l'IUT.

E-mail (ne pas saisir "@iut-rodez.fr"):  
mister.magoo@iut-rodez.fr

Mot de passe:  
CUCU!

Je m'inscris maintenant avant d'accéder à d'autres services.

SE CONNECTER EFFETUER

Pour des raisons de sécurité, veuillez vous déconnecter et fermer votre navigateur lorsque vous avez fini d'accéder aux services authentifiés.

Languages:  
[English](#) [Spanish](#) [French](#) [Russian](#) [Nederlands](#) [Svenskt](#) [Italiano](#) [Urdu](#) [Chinese](#)  
[\(Simplified\)](#) [Deutsch](#) [Japanese](#) [Croatian](#) [Czech](#) [Slovenian](#) [Polish](#) [Portuguese \(Brazil\)](#) [Turkish](#)

Copyright © 2005-2007 JA-SIG. All rights reserved.  
Powered by [JA-SIG Central Authentication Service 3.3.5](#)

JA-SIG

1 - POST https  
(xhr)

## Serveur CASLogger

https://caslogger/

- username
- message d'erreur
- ip
- x-forwarded-for
- user-agent
- referer
- url demandée
- ouatéveur ↓

**BdD MySQL :**  
insert into tentatives

# CAS Logger

Les tentatives de connexion à CAS,  
c'est bien joli ...

mais quid des connexions  
effectives ?

```
mustRedirect = true;
```

# CAS Logger

La ruse :

Le script js ré-écrit à la volée l'URL vers  
la web app cassifiée  
« Caslogger »

qui s'immisce alors en première  
position

# CAS Logger

RODEZ  
iut  
Midi-Pyrénées  
UNIVERSITÉ TOULOUSE I

Central Authentication Service (CAS)

Les informations transmises n'ont pas permis de vous authentifier.

Entrez votre e-mail et votre mot de passe de l'IUT.

E-mail (ne pas saisir "@iut-rodez.fr"):  
mister.magoo@iut-rodez.fr

Mot de passe:

Je n'ai pas encore de compte. Cliquez ici pour en créer un.

**CLIC!**  
SE CONNECTER EFFACER

Pour des raisons de sécurité, veuillez vous déconnecter et fermer votre navigateur lorsque vous avez fini d'accéder aux services authentifiés.

Languages:  
[English](#) [Spanish](#) [French](#) [Russian](#) [Nederlands](#) [Svenskt](#) [Italiano](#) [Urdu](#) [Chinese \(Simplified\)](#) [Deutsch](#) [Japanese](#) [Croatian](#) [Czech](#) [Slovenian](#) [Polish](#) [Portuguese \(Brazil\)](#) [Turkish](#)

Copyright © 2005-2007 JA-SIG. All rights reserved.  
Powered by [JA-SIG Central Authentication Service 3.3.5](#)

JA-SIG

<https://cas.univ/login?service=https://caslogger/redirect.php&s=webapp>

Serveur CASLogger  
redirect.php

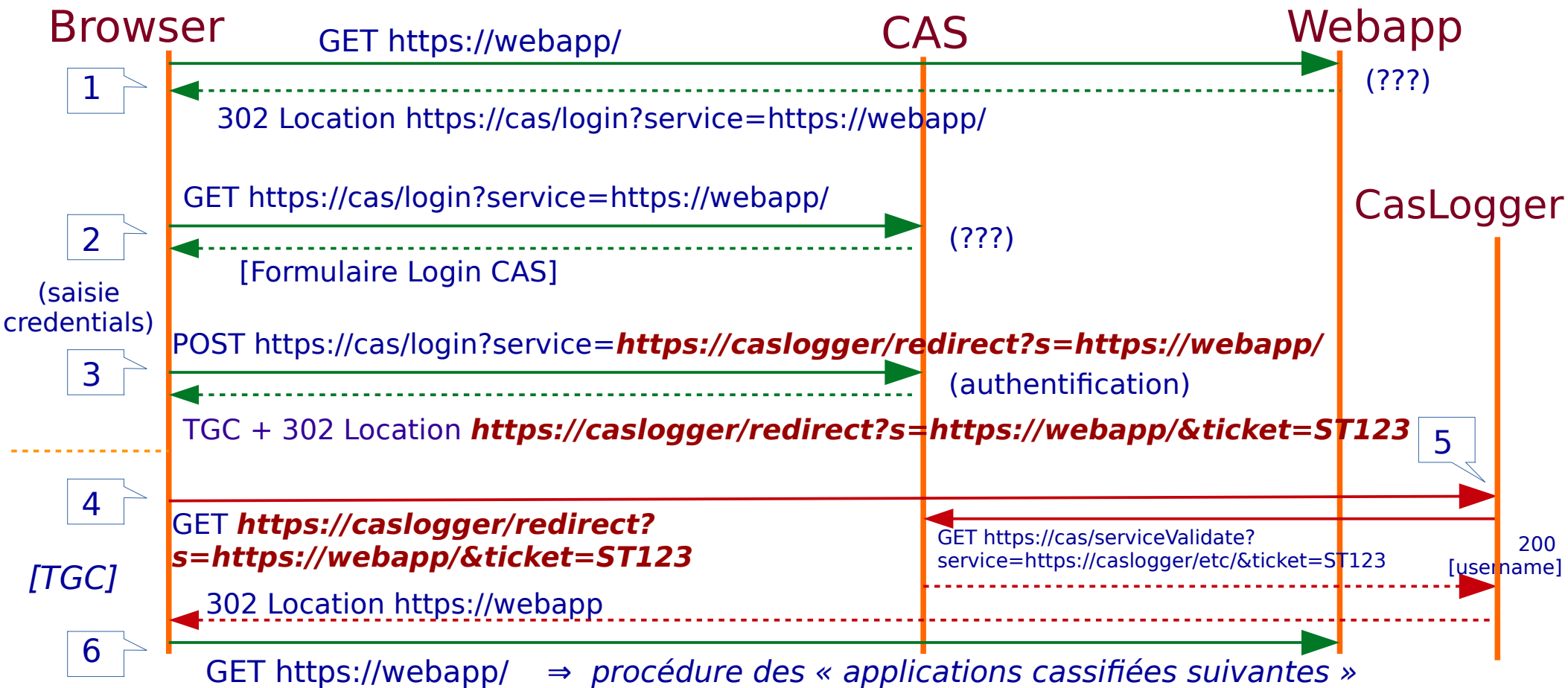
retourne code http 302  
'Location: webapp'

appli cassifiée ! → username

BdD MySQL :  
update tentatives ...



# CAS Logger : redirect



# CAS Logger

				SAMLRequest=fVLJT			
629	marc mand	193.54.203.133	10.2.14.13	http://ego.iut-rodez.fr/caslogger/redirect.php?_cLt=1wCvsVxo99&SAMLRequest=fVLJT	https://cas.iut-rodez.fr/cas/login?SAMLRequest=fVLJTsMwEL0j8Q%2BR70maqghkNUEFhKj		2015-12-04 15:47:44
628	d...ce	193.54.203.133	10.10.0.2	http://ego.iut-rodez.fr/caslogger/redirect.php?_cLt=91Lg1Z75dU&_cLs=https://kane	https://cas.iut-rodez.fr/cas/login?service=https://kanet.iut.rdz:445/login_cas/		2015-12-04 15:47:28
627	aud...uillat	193.54.203.133	10.10.0.2	http://ego.iut-rodez.fr/caslogger/redirect.php?_cLt=q4U3MnrXDv&_cLs=https://kane	https://cas.iut-rodez.fr/cas/login?service=https://kanet.iut.rdz:445/login_cas/		2015-12-04 15:47:18
626	vinc...nad	193.54.203.133	10.2.14.22	http://ego.iut-rodez.fr/caslogger/redirect.php?_cLt=6XtxJcAaNS&SAMLRequest=fVLLT	https://cas.iut-rodez.fr/cas/login?service=http%3A%2F%2Fego.iut-rodez.fr%2Fcaslo	Les informations transmises n'ont pas permis de vous authentifier.	2015-12-04 15:46:50
625	aud...uillat	193.54.203.133	10.10.0.2	http://ego.iut-rodez.fr/caslogger/redirect.php?_cLt=ihqDhqoivP&_cLs=https://kane	https://cas.iut-rodez.fr/cas/login?service=https://kanet.iut.rdz:445/login_cas/		2015-12-04 15:46:39
624	guilla...mens	193.54.203.133	192.168.0.157	http://ego.iut-rodez.fr/caslogger/redirect.php?_cLt=Wi6BulQ8AV&_cLs=http%3A%2F%2	https://cas.iut-rodez.fr/cas/login?service=http%3A%2F%2Ffedt.iut-rodez.fr%2Fgpu%2		2015-12-04 15:45:46
623	vinc...nad	193.54.203.133	10.2.14.22	http://ego.iut-rodez.fr/caslogger/redirect.php?_cLt=6XtxJcAaNS&SAMLRequest=fVLLT	https://cas.iut-rodez.fr/cas/login?SAMLRequest=fVLLTsMwELwj8Q%2BW70ma0krlaolKCFG		2015-12-04 15:45:39
622	ma...ulet	193.54.203.133	80.12.42.21	http://ego.iut-rodez.fr/caslogger/redirect.php?_cLt=DCOA4aEyiQ&SAMLRequest=fVJNT	https://cas.iut-rodez.fr/cas/login?SAMLRequest=fVJNT%2BMwEL2vxH%2BIfE%2FSdLsSspq		2015-12-04 15:44:54
621	timoth...binet	193.54.203.133	77.144.216.84	http://ego.iut-rodez.fr/caslogger/redirect.php?_cLt=5M8i3Gc388	https://cas.iut-rodez.fr		2015-12-04

# CAS Logger

Ok, mais si ...

l'utilisateur désactive javascript :

CASLogger ne loggue plus et le client CAS continue de fonctionner comme avant

(note : on peut forcer l'usage de js)

# CAS Logger

Ok, mais si ...

le serveur CASLogger est down ou  
inaccessible :

le script js n'est pas chargé et le client CAS  
continue de fonctionner comme avant

# CAS Logger

est

léger : 2 scripts php, 1 js,  
facile à déployer : 1 serveur lamp  
peu intrusif : un tag `<script>`  
facile à exploiter : 1 table + SQL  
marche avec CAS et SAML  
FF, Chrome, Safari, IE8+, mobiles

CAS Logger

est

gratos, bio, fait à la main en Aveyron,

disponible dans tous les bonnes épiceries et  
chez Guy Teub :

<https://github.com/jbousquie/Caslogger>