CAS V4 ET GESTION D'AUTHENTIFICATION À TELECOM ÉCOLE DE MANAGEMENT ET TELECOM SUDPARIS

Mohamed Hmani -- Telecom SudParis
Christophe Gaboret, Jehan Procaccia -- Institut Mines-Télécom

CONTEXTE

- **CAS version 3.4.7**
  - Un peu vieillissant, sur Tomcat 6
  - Pas de fonctionnalités de sécurité comme throttle, memcache
- **Volonté d'accéder à des partages Windows via le filemanager inclus à l'ENT**
  - Utilisation du ClearPass
- **Credentials fournit aux étudiants lors de leur inscription (qu'ils oublient)**
  - Nécessiter de passer à la DSI
  - Relativement chronophage en début d'année
- **Outil de réinitialisation des mots de passe maison**
  - Nécessiter de peupler annuaire LDAP, un Active Directory et attribut NTPassword
  - Forcer l'utilisation de mots de passe forts

ESUP-DAYS 22

MEMCACHE
CLEARPASS
THROTTLE
ATTAQUE SUR LES LOGS

SECTION #1: MISE EN PLACE DE CAS-TOOLBOX

esup portail

SECTION 1: MISE EN PLACE DE CAS-TOOLBOX

- Installation
  - Git
  - Tomcat
- Problèmes rencontrés lors de la mise en place de CAS
  - Memcache
  - ClearPass
  - Kryo transcoder
  - Attaque sur les logs

INSTALLATION: GIT

- **Gitlab local**
  - **Installation simple : fourni sous forme de paquet rpm**
  - **Nombre illimité de repositories privés**
  - **Interface web**
  - **Intégration avec LDAP et CAS (authentification)**
  - **Intégration avec shibboleth**

INSTALLATION: TOMCAT

- **Tomcat**
  - Version : 7.0.54
  - Utilisation du paquet fourni par les dépôts redhat par défaut
- **Problème de démarrage trop lent sur les machines virtuelles**

```
[root@4cas webapps]# tail -f /var/log/tomcat/catalina.2016-04-25.log
…
INFOS: Creation of SecureRandom instance for session ID generation using [SHA1PRNG] took [239 990] milliseconds.
…
INFOS: Server startup in 241085 ms
```

  - 99,6 % du temps est perdu sur la création du « SecureRandom »
  - **Cause :** manque d'entropy + Tomcat utilise /dev/random par défaut
  - **Solution :** utiliser /dev/urandom ou remplir le bassin d'entropy (haveged)

PROBLÈMES RENCONTRÉS LORS DE LA MISE EN PLACE DE CAS : MEMCACHE

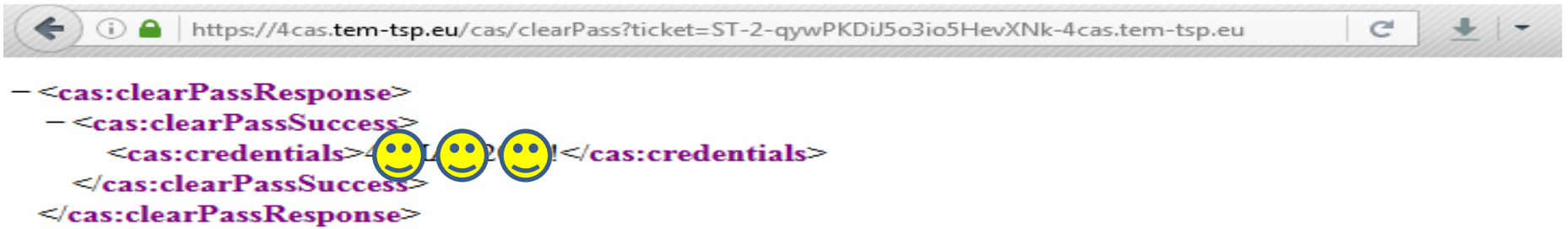
- **Problème**
  - Log de l'erreur

```
[root@4cas webapps]# tail -f /var/log/tomcat/localhost.2016-05-26.log
…
[org.jasig.cas.ticket.registry.MemCacheTicketRegistry] - <Failed fetching TGT-3-
WXqbgzxzg9tzWoJLp403wgWqk7xD6bJabBpuhIWY7orN56BI7e-cas-devel > java.lang.RuntimeException: Exception waiting for value
…
Caused by: java.util.concurrent.ExecutionException: com.esotericsoftware.kryo.SerializationException: Unable to deserialize object of
type: org.jasig.cas.ticket.TicketGrantingTicketImpl
…
Caused by: com.esotericsoftware.kryo.SerializationException: Unable to deserialize object of type:
java.util.Collections$UnmodifiableCollection
```

  - **Cause :** problème dans la dépendance 'cas-server-integration-memcached' v4.0.4-4.0.7
  - **Contournement :** choisir la version 4.0.1 (à définir dans le pom.xml)

PROBLÈMES RENCONTRÉS LORS DE LA MISE EN PLACE DE CAS : CLEARPASS

- **Problème**
  - Le mot de passe est écrit en clair lorsqu'on consulte « https://cas.univ.fr/cas/login?service=https://cas.univ.fr/cas/clearPass »



  - **Implication :** On peut savoir le mot de passe en accédant à la machine + risque de XSS venant du domaine.
  - **Contournement :** Limiter l'accès dans apache pour l'url <domain>/cas/clearPass à l'application cible (µPortal)

PROBLÈMES RENCONTRÉS LORS DE LA MISE EN PLACE DE CAS : KRYO TRANSCODER

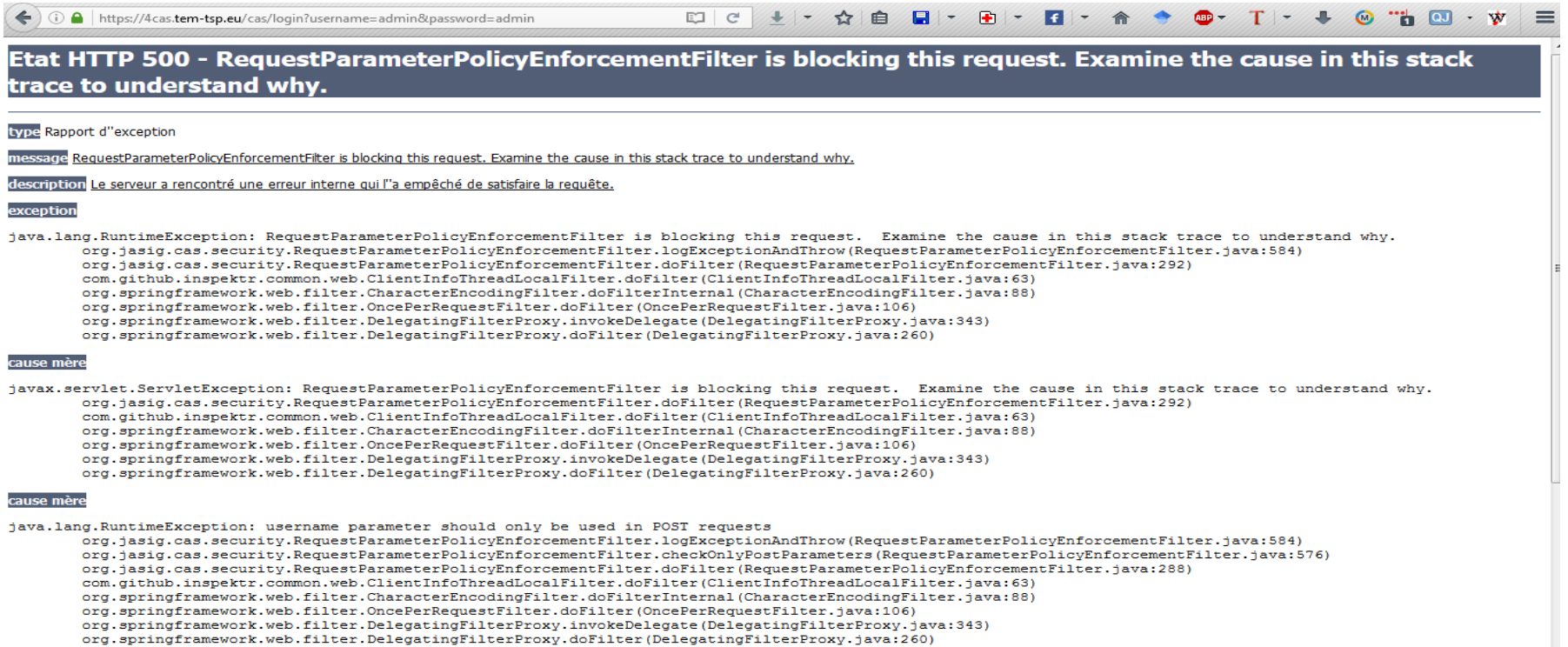
- **Problème**
  - ClearPass activé
  - CAS n'accepte plus les mots de passe contenant des caractères spéciaux
  - **Cause :** KryoTranscoder rencontre un problème d'encodage
  - **Contournement :** enlever KryoTranscoder (V. Bonamy)
    - **Fichier affecté :** cas-toolbox-custom/src/main/webapp/WEB-INF/spring-configuration/ticketRegistry.xml
    - **Modification :** effacer le bean 'kryoTranscoder' ainsi que la référence 'p:transcoder-ref="kryoTranscoder" '

PROBLÈMES RENCONTRÉS LORS DE LA MISE EN PLACE DE CAS : ATTAQUE SUR LES LOGS

- **Problème**
  - L'envoi des paramètres 'username' et 'password' à travers la méthode GET génère une erreur interne pour la servlet.
  - **Cause :** cas-server-security-filter-2.0.3.jar
  - **Symptôme :** l'erreur est logguée 2 fois, par l'application dans cas.log (comportement désiré) et dans localhost.<date>.log par tomcat (comportement non désiré)
  - **Versions où le problème existe :** cas 4.0.7 , 4.2.1, 4.2.2
  - **Risque :** Saturer le disque avec des logs (par exemple à travers une attaque brute force mal configurée qui utilise GET au lieu de POST)
  - **Contournement :** désactiver les logs de tomcat
  - **Correction :** Utiliser cas-server-security-filter-2.0.6.jar

PROBLÈMES RENCONTRÉS LORS DE LA MISE EN PLACE DE CAS : ATTAQUE SUR LES LOGS

- **Détection**
  - Consultation de l'url <cas-server>/login?username=test

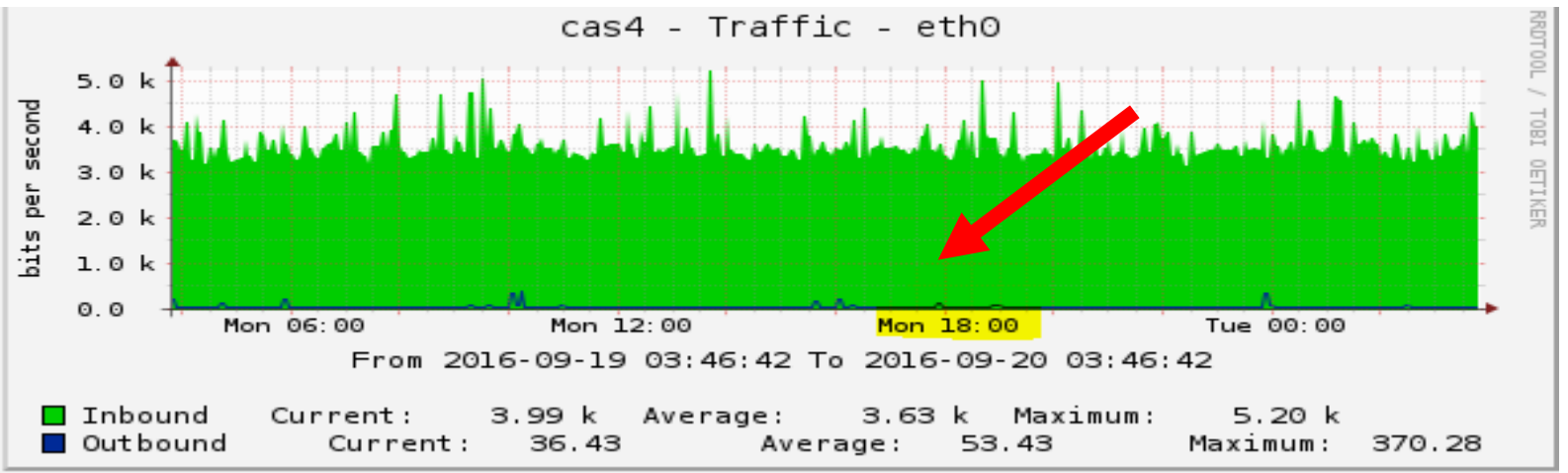


PROBLÈMES RENCONTRÉS LORS DE LA MISE EN PLACE DE CAS : ATTAQUE SUR LES LOGS

- **Simulation d'attaque**
  - Pour simuler une attaque on a exécuté 20 instances du script python suivant pendant 2h à partir d'une seule machine

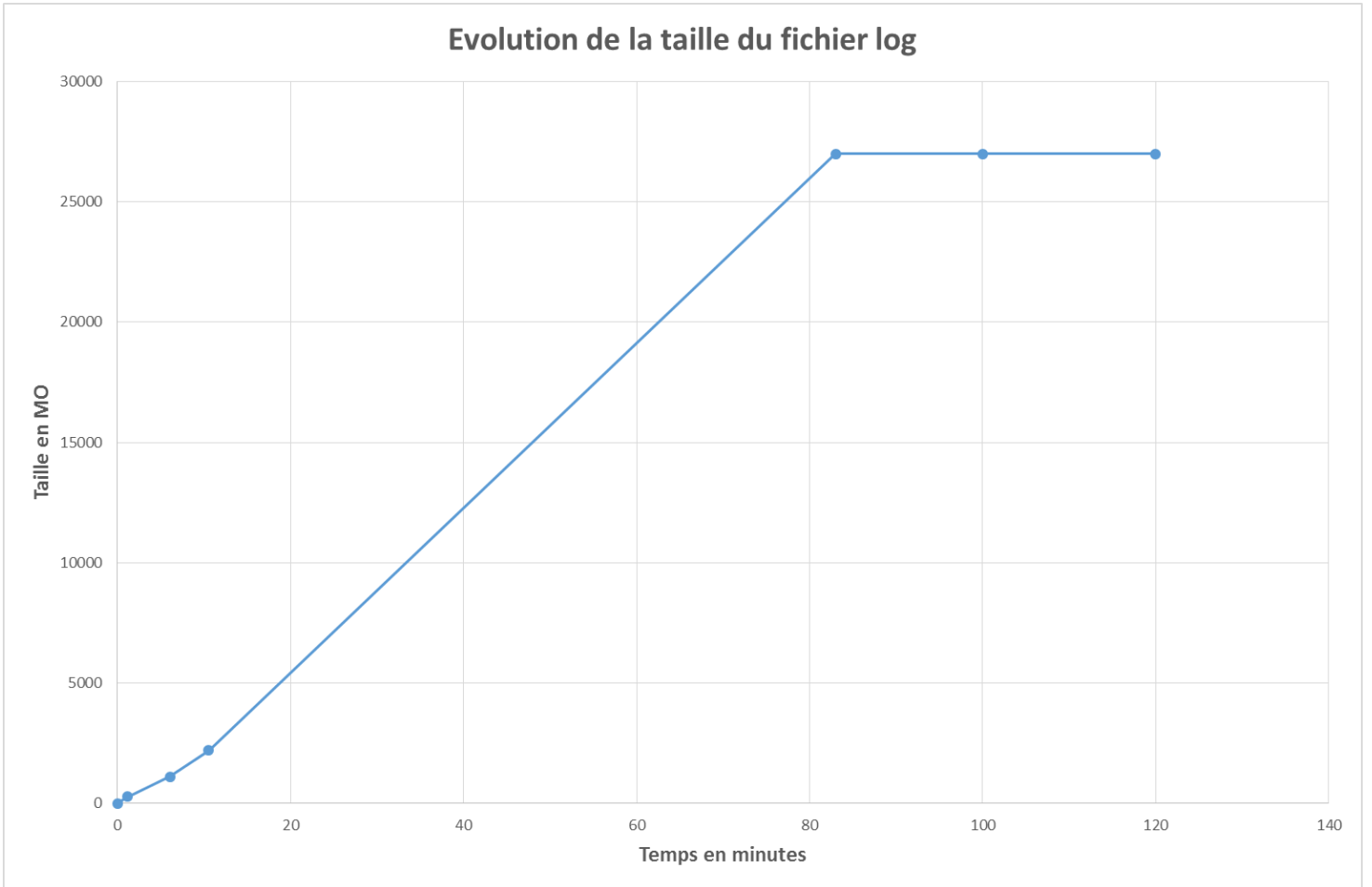
```
import urllib2
url = 'https://4cas.tem-tsp.eu/cas/login?username='
while 1:
        try:
                urllib2.urlopen(url)
        except:
                pass
```

- **Traffic**



PROBLÈMES RENCONTRÉS LORS DE LA MISE EN PLACE DE CAS : ATTAQUE SUR LES LOGS

- **Effets**



PROBLÈMES RENCONTRÉS LORS DE LA MISE EN PLACE DE CAS : ATTAQUE SUR LES LOGS

- **Effet**
  - Le disque est saturé

```
[root@localhost ~]# df -h
Sys. de fichiers          Taille Utilisé Dispo Uti% Monté sur
/dev/mapper/centos-root     39G     39G   20K 100% /
devtmpfs                   1,9G       0  1,9G   0% /dev
tmpfs                      1,9G    8,0K  1,9G   1% /dev/shm
tmpfs                      1,9G    8,6M  1,9G   1% /run
tmpfs                      1,9G       0  1,9G   0% /sys/fs/cgroup
/dev/vda1                  497M    266M  231M  54% /boot
/dev/mapper/centos-home     19G     33M   19G   1% /home
tmpfs                      375M       0  375M   0% /run/user/0
```

  - Les effets de l'attaques ne sont visibles qu'après redémarrage du serveur

PROBLÈMES RENCONTRÉS LORS DE LA MISE EN PLACE DE CAS : ATTAQUE SUR LES LOGS

- **Effets**
  - Impossible de créer des fichiers temporaires

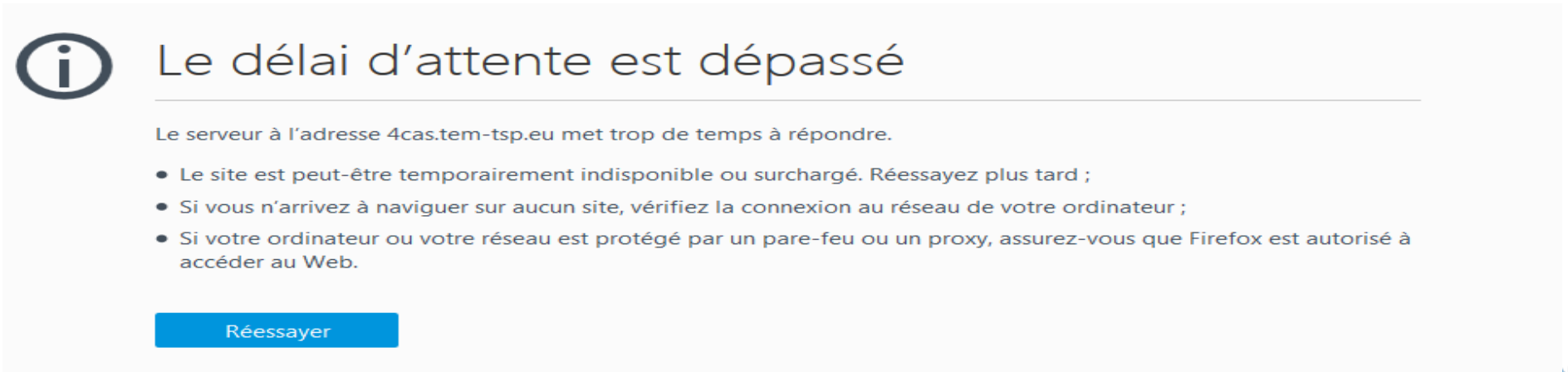
```
-- L'unité (unit) systemd-tmpfiles-setup.service a commencé à démarrer.
sept. 20 01:09:57 localhost.localdomain systemd-tmpfiles[612]: Unable to fix SELinux security context of /var: No space left on
sept. 20 01:09:57 localhost.localdomain systemd-tmpfiles[612]: Unable to fix SELinux security context of /var/log: No space left
sept. 20 01:09:57 localhost.localdomain systemd-tmpfiles[612]: Unable to fix SELinux security context of /tmp: No space left on
sept. 20 01:09:57 localhost.localdomain systemd-tmpfiles[612]: Unable to fix SELinux security context of /var/tmp: No space left
sept. 20 01:09:57 localhost.localdomain systemd-tmpfiles[612]: Unable to fix SELinux security context of /var/tmp/abrt: No space
sept. 20 01:09:57 localhost.localdomain systemd-tmpfiles[612]: Unable to fix SELinux security context of /var/lib: No space left
sept. 20 01:09:57 localhost.localdomain systemd-tmpfiles[612]: Unable to fix SELinux security context of /var/lib/machines: No s
sept. 20 01:09:57 localhost.localdomain systemd-tmpfiles[612]: Unable to fix SELinux security context of /var/cache: No space le
sept. 20 01:09:57 localhost.localdomain systemd-tmpfiles[612]: Unable to fix SELinux security context of /var/log/wtmp: No space
sept. 20 01:09:57 localhost.localdomain systemd-tmpfiles[612]: Unable to fix SELinux security context of /var/spool: No space le
sept. 20 01:09:57 localhost.localdomain systemd-tmpfiles[612]: Unable to fix SELinux security context of /var/lib/systemd: No sp
sept. 20 01:09:57 localhost.localdomain systemd-tmpfiles[612]: Unable to fix SELinux security context of /tmp/.font-unix: No spa
sept. 20 01:09:57 localhost.localdomain systemd-tmpfiles[612]: Unable to fix SELinux security context of /var/lib/systemd/coredu
sept. 20 01:09:57 localhost.localdomain systemd-tmpfiles[612]: Unable to fix SELinux security context of /tmp/.ICE-unix: No spac
sept. 20 01:09:57 localhost.localdomain systemd-tmpfiles[612]: Unable to fix SELinux security context of /var/log/btmp: No space
sept. 20 01:09:57 localhost.localdomain systemd-tmpfiles[612]: Unable to fix SELinux security context of /tmp/.X11-unix: No spac
sept. 20 01:09:57 localhost.localdomain systemd[1]: systemd-tmpfiles-setup.service: main process exited, code=exited, status=1/F
sept. 20 01:09:57 localhost.localdomain systemd[1]: Failed to start Create Volatile Files and Directories.
-- Subject: L'unité (unit) systemd-tmpfiles-setup.service a échoué
```

PROBLÈMES RENCONTRÉS LORS DE LA MISE EN PLACE DE CAS : ATTAQUE SUR LES LOGS

- **Effets**
  - Java ne peut pas démarrer

```
sept. 20 01:10:13 localhost.localdomain server[1338]: java.io.IOException: Aucun espace disponible sur le périphérique
sept. 20 01:10:13 localhost.localdomain server[1338]: at java.io.FileOutputStream.writeBytes(Native Method)
sept. 20 01:10:13 localhost.localdomain server[1338]: at java.io.FileOutputStream.write(FileOutputStream.java:345)
sept. 20 01:10:13 localhost.localdomain server[1338]: at sun.nio.cs.StreamEncoder.writeBytes(StreamEncoder.java:221)
sept. 20 01:10:13 localhost.localdomain server[1338]: at sun.nio.cs.StreamEncoder.implFlushBuffer(StreamEncoder.java:291)
```

  - Tomcat ne peut pas démarrer



PROBLÈMES RENCONTRÉS LORS DE LA MISE EN PLACE DE CAS : ATTAQUE SUR LES LOGS

- **Effets**
  - Pas de session SSH

```
[med@mah16 ~]$ ssh root@4cas
ssh: connect to host 4cas port 22: Connection timed out
```

- **Conclusion**
  - Traffic normal: attaque passe inaperçue
  - Après l'attaque (sans redémarrage) on ne peut plus logguer les authentifications et les évènements sur CAS
  - Après l'attaque (avec redémarrage de la machine) : on perd l'accès à CAS, pas de ssh: nécessite l'intervention à partir de l'hyperviseur

https://github.com/apereo/cas/issues/1848

JUSTIFICATION DU CHOIX
FAILLES DE SÉCURITÉ DÉCOUVERTES DANS LTB
APPORT À L'APPLICATION

SECTION #2: LTB (LDAP TOOL BOX)

http://ltb-project.org

ESUP-ACTIV (PARIS 1)
LEMON LDAP (PARIS 6)
UNICON
PWM (GPL)
SELF SERVICE RESET PASSWORD MANAGER (TOOLS4EVER)
DÉVELOPPEMENTS MAISON UNIV. VALENCIENNES

SOLUTIONS ÉTUDIÉES

LDAP TOOL BOX

- **Justification du choix**
  - **Application Open Source**
  - **Application relativement simple**
  - **Répond à nos besoins : Changement de mot de passe + Réinitialisation par Email et SMS**
  - **Possibilité d'activer le Recaptcha**
  - **Application activement maintenue**
  - **Après de simples modifications l'application intervient sur openLDAP et AD d'une façon parallèle.**

LDAP TOOL BOX

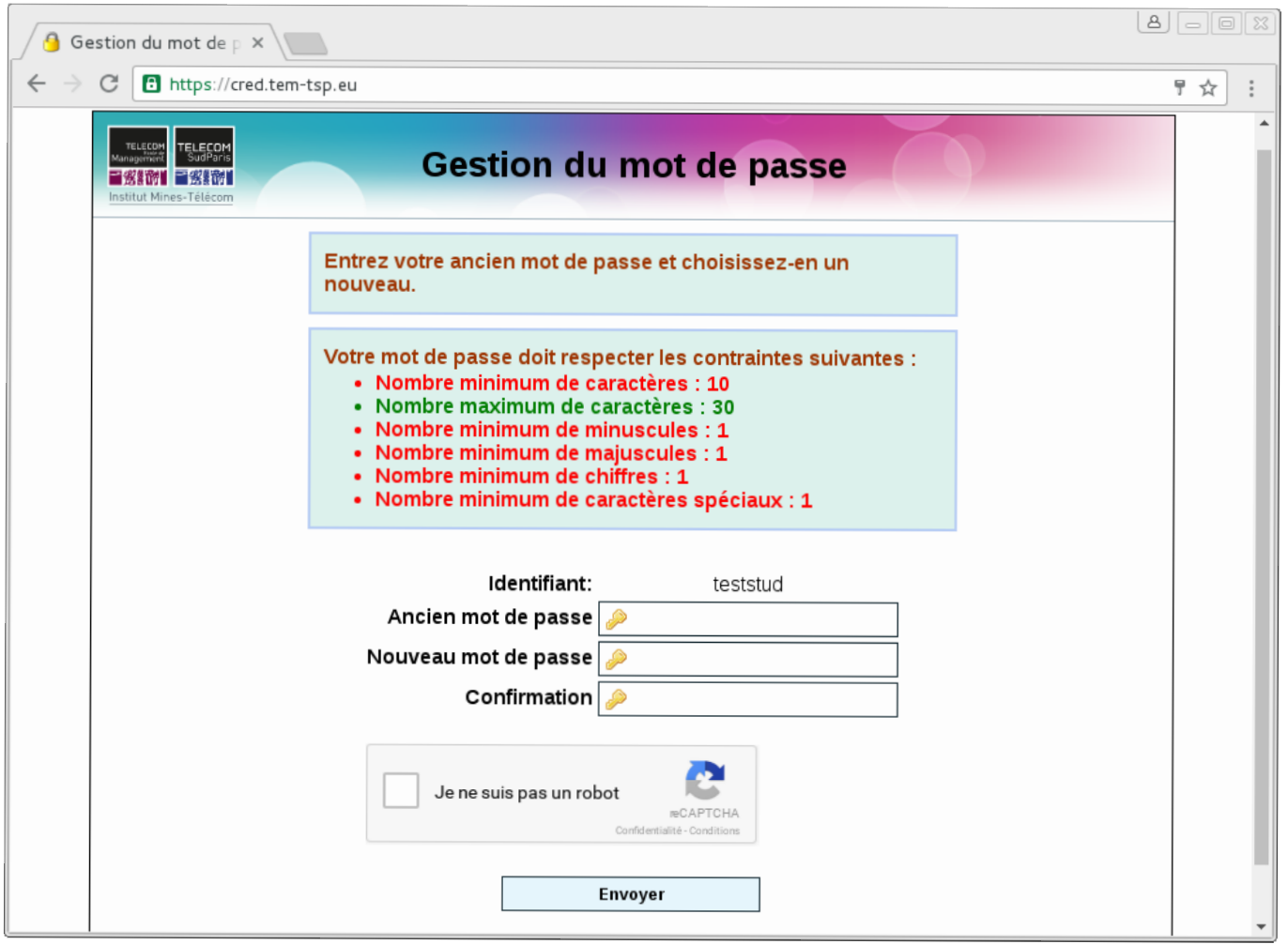
- **Failles de sécurité découvertes: concentrées dans la composante réinitialisation par SMS**
  - **Jeton SMS valide indéfiniment**
  - **On peut modifier le numéro de téléphone de quelqu'un de sorte qu'on reçoive son jeton**
  - **On peut utiliser un seul jeton pour réinitialiser le mot de passe de tout le monde d'une façon infinie.**

LDAP TOOL BOX

- **Nos apports au projet**
  - **Cassification de l'application en utilisant phpCAS**
  - **Patcher les failles de la composante SMS**
  - **Utiliser une base de données SqLite pour relier le jeton à l'identité de l'utilisateur**
  - **Ajout d'une page de statistiques**
  - **Ajout d'une page pour afficher l'historique des changement ainsi que la réinitialisation de mot de passe (page cassifiée)**
  - **Rendre l'application responsive**
  - **Internationalisation de LTB**
  - **Mise à jour le reCAPTCHA en noCAPTCHA reCAPTCHA**

LDAP TOOL BOX

- **Cassification de l'application en utilisant phpCAS**

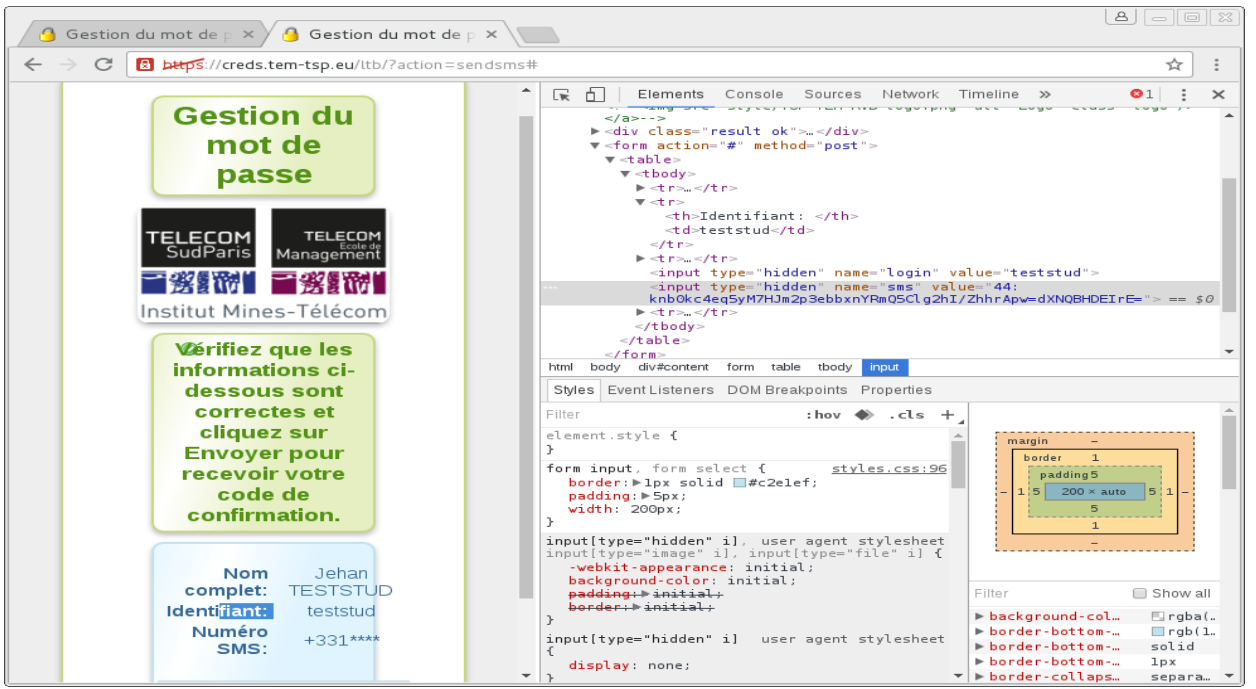


LDAP TOOL BOX

- **Patcher les failles de la composante SMS**

LDAP TOOL BOX

- **Patcher les failles de la composante SMS**
  - On peut modifier le numéro de téléphone avant l'envoi du jeton de sorte qu'on reçoive les jetons des autres
  - **Solution:** Réapprovisionner le numéro de téléphone dynamiquement à partir de l'annuaire plutôt que par des champs hidden !

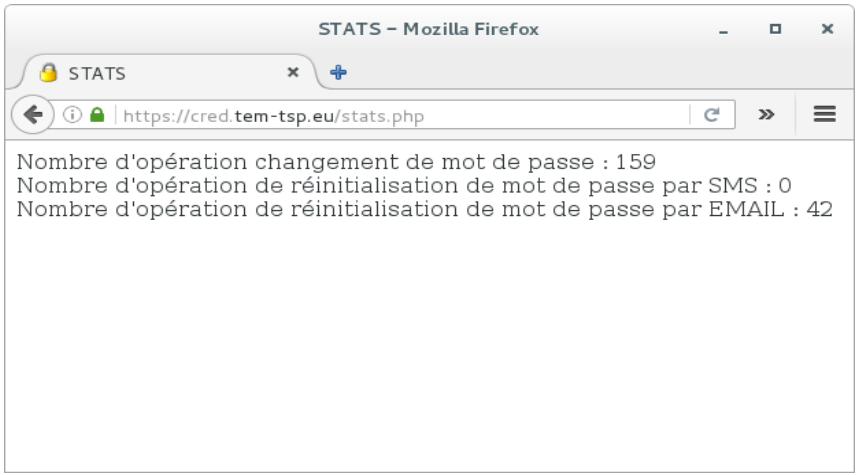


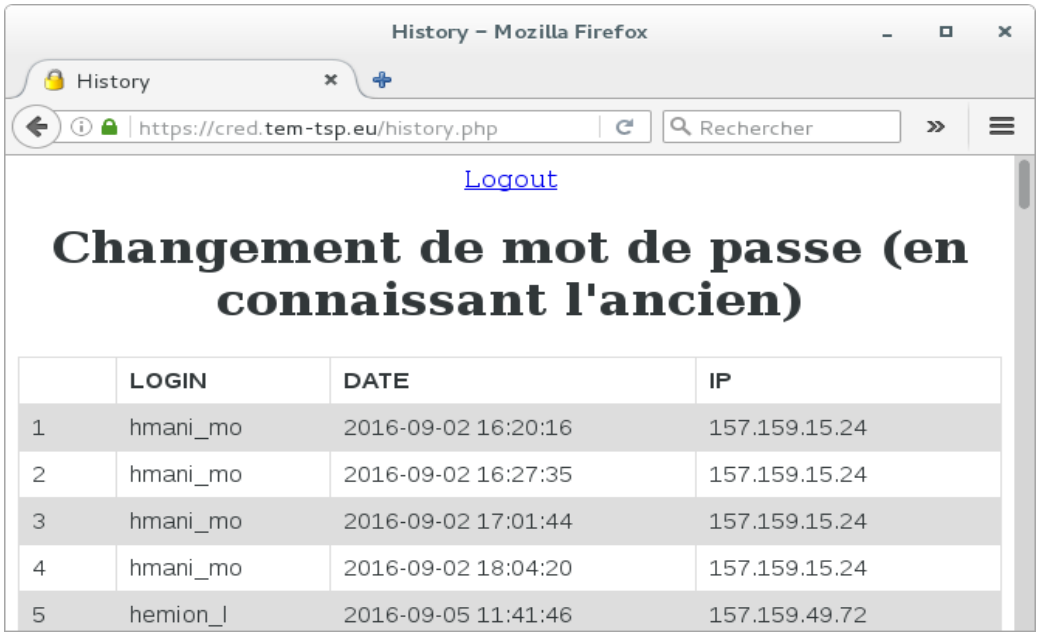
LDAP TOOL BOX

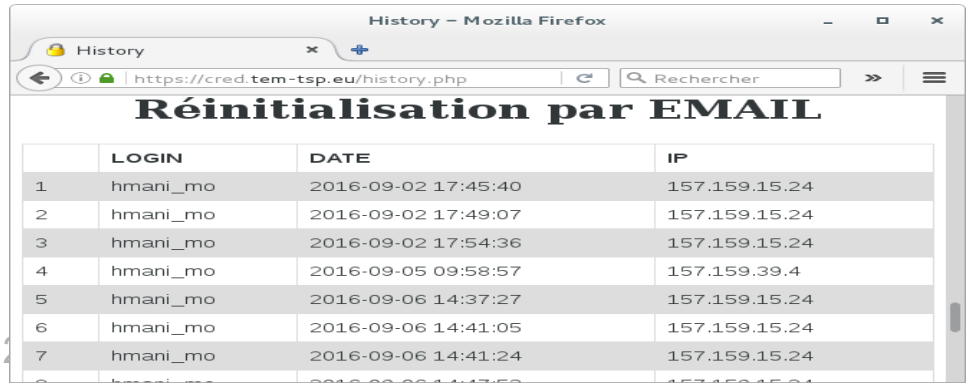
- **Utiliser une base de données SQLite pour relier le jeton à l'identité de l'utilisateur**
  - On peut réutiliser un jeton généré indéfiniment (session destroyed mais pas le jeton). On peut ainsi changer le mot de passe de n'importe quel autre utilisateur de l'annuaire en ne connaissant que son identifiant.
  - **Solution:** Utilisation d'une base de données (SQLite) pour relier le jeton à l'identité de l'utilisateur et limiter la durée de vie du jeton.

LDAP TOOL BOX

- **Ajout de pages administrateur pour statistiques et history**







REMPLI NOTRE BESOIN … ET RIEN QUE NOTRE BESOIN
SÉCURITÉ DES « IDENTITÉS NUMÉRIQUES » COUPLÉ À L'AUDIT DU CODE NOUS A PERMIS DE CONTRIBUER À CES 2 PROJETS (PROJET GITHUB AVEC L'AUTEUR DU PROJET)
ENSEMBLE DES 2 PROJETS (CAS ET LTB) INTÉGRÉS À L'ENT ET À LA BANNIÈRE DE LOGIN

CONCLUSIONS