

# Systemes d'informations: définir le seuil de compétence des acteurs

(s'il existe et si cela est possible, bien entendu...)



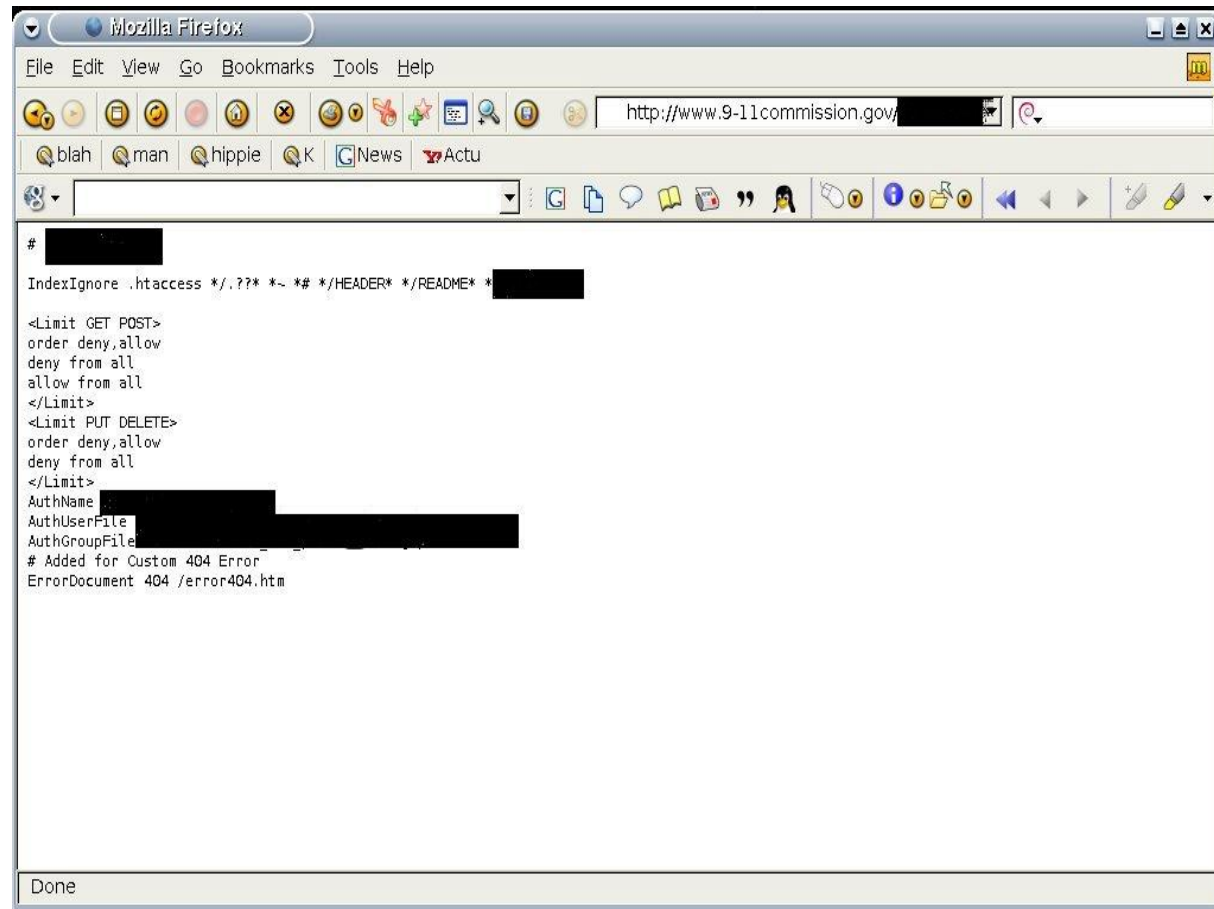
# sécurité nulle part?

---

- n La question d'un développement interne ou externe pour assurer une meilleure sécurité n'est pas neuve...
- n Et s'il n'y avait de sécurité nulle part?
- n Ou presque...

# La commission 9/11

n Développement  
maison...



```
# [REDACTED]
IndexIgnore .htaccess */.??* *~ *# */HEADER* */README* * [REDACTED]

<Limit GET POST>
order deny,allow
deny from all
allow from all
</Limit>
<Limit PUT DELETE>
order deny,allow
deny from all
</Limit>
AuthName [REDACTED]
AuthUserFile [REDACTED]
AuthGroupFile [REDACTED]
# Added for Custom 404 Error
ErrorDocument 404 /error404.htm
```

www.kitetoa.com - we will hack  
your pizzas for free



# Axi.fr

---

- n Quelques spams pour des machines à café plus loin...
- n Les fichiers de configuration du système permettant de poster et des milliers d'adresses e-mail.

# Axi.fr (suite)

- n Nom de la base
- n Login
- n Password
- n Etc.

```
clean_delay_queueauth 3

## Subscription expiration spool (Cf EXPIRE command)
queueexpire /var/spool/sympa/queueexpire

## Bounce queue
#queuebounce /var/spool/sympa/queuebounce
queuebounce /var/www/bounce/spool

## Outgoing queue
queueoutgoing /var/spool/sympa/queueoutgoing

## Directory for task files created by the task manager
queuetask /var/spool/sympa/queuetask

## Delay between two scan of the main spool (queue). Avoid Zero value !
sleep 5

## Temporary directory
tmpdir /var/spool/sympa/tmp

## S/MIME configuration begin
# DO NOT REMOVE SURROUNDING COMMENTS

# DO NOT MODIFY TEMPLATE VARIABLES
# If you want to reconfigure Sympa for using S/MIME, please run
# dpkg-reconfigure -plow sympam

# Location of the openssl binary
openssl /usr/bin/openssl

# Openssl CA Options
capath /etc/ssl/certs
cafile /usr/share/sympa/ca-bundle.crt

# Password to the lists private key (template variable)
key_passwd [REDACTED]

# SSL certificates directory
ssl_cert_dir /var/lib/sympa/x509-user-certs

## S/MIME configuration end

## Database configuration begin
# DO NOT REMOVE SURROUNDING COMMENTS

# DO NOT EDIT BY HAND
# USE dpkg-reconfigure -plow sympam TO RECONFIGURE

## Database driver (DBD)
db_type [REDACTED]

## Name of your database
db_name [REDACTED]

## Your database hostname
db_host [REDACTED]

## Username to connect to the DB
db_user [REDACTED]

## Password for the user
db_passwd [REDACTED]

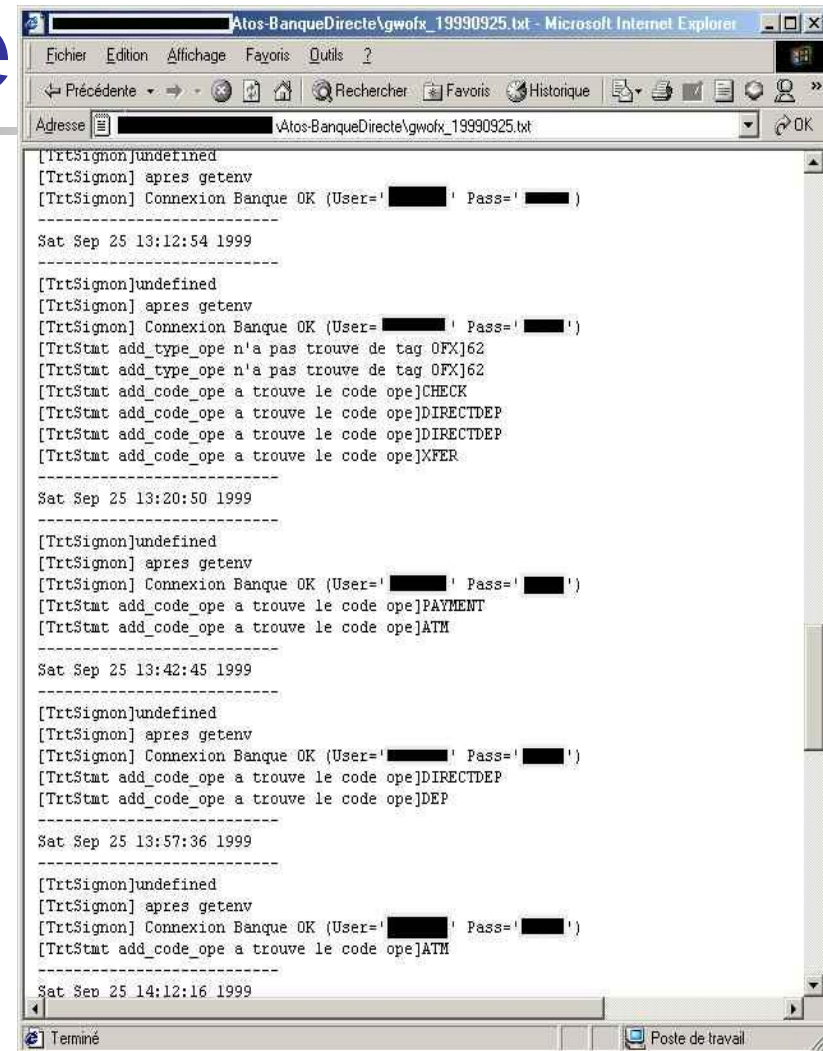
## Database options
db_options [REDACTED]

## Database configuration end

Terminé 217.174.197.8
```

# Banque Directe

n Développement externe...



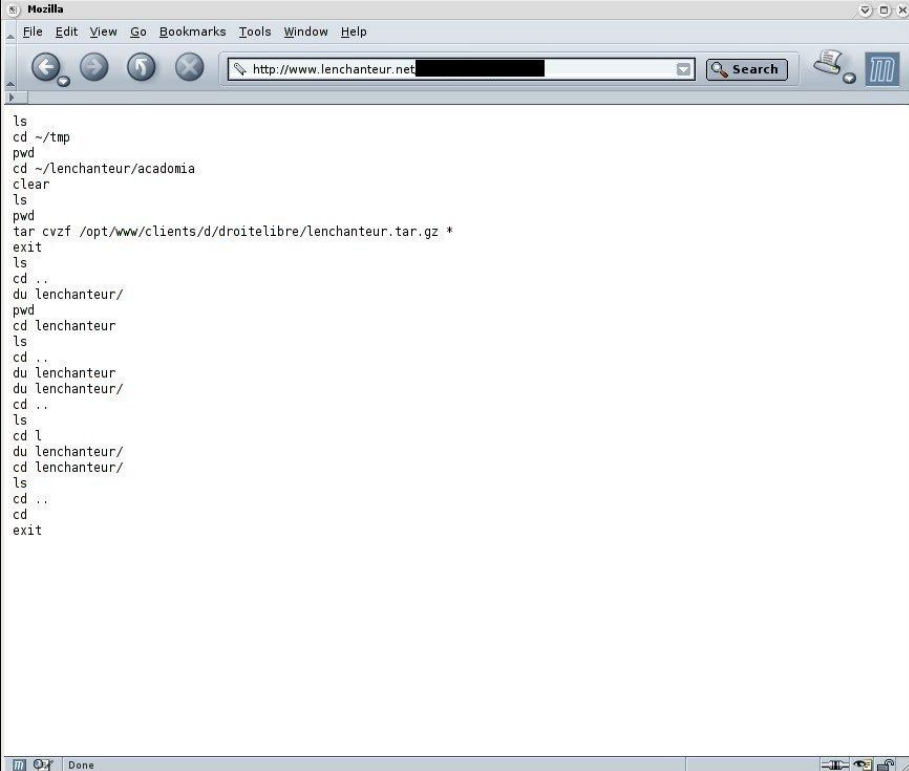
```
Atos-BanqueDirecte\gwofx_19990925.txt - Microsoft Internet Explorer
Fichier Edition Affichage Favoris Outils ?
Précédente Recherche Favoris Historique
Adresse \Atos-BanqueDirecte\gwofx_19990925.txt OK

[TrtSigmon]undefined
[TrtSigmon] apres getenv
[TrtSigmon] Connexion Banque OK (User=' ' Pass=' ')
-----
Sat Sep 25 13:12:54 1999
-----
[TrtSigmon]undefined
[TrtSigmon] apres getenv
[TrtSigmon] Connexion Banque OK (User=' ' Pass=' ')
[TrtStat add_type_ope n'a pas trouve de tag OFX]62
[TrtStat add_type_ope n'a pas trouve de tag OFX]62
[TrtStat add_code_ope a trouve le code ope]CHECK
[TrtStat add_code_ope a trouve le code ope]DIRECTDEP
[TrtStat add_code_ope a trouve le code ope]DIRECTDEP
[TrtStat add_code_ope a trouve le code ope]XFER
-----
Sat Sep 25 13:20:50 1999
-----
[TrtSigmon]undefined
[TrtSigmon] apres getenv
[TrtSigmon] Connexion Banque OK (User=' ' Pass=' ')
[TrtStat add_code_ope a trouve le code ope]PAYMENT
[TrtStat add_code_ope a trouve le code ope]ATM
-----
Sat Sep 25 13:42:45 1999
-----
[TrtSigmon]undefined
[TrtSigmon] apres getenv
[TrtSigmon] Connexion Banque OK (User=' ' Pass=' ')
[TrtStat add_code_ope a trouve le code ope]DIRECTDEP
[TrtStat add_code_ope a trouve le code ope]DEP
-----
Sat Sep 25 13:57:36 1999
-----
[TrtSigmon]undefined
[TrtSigmon] apres getenv
[TrtSigmon] Connexion Banque OK (User=' ' Pass=' ')
[TrtStat add_code_ope a trouve le code ope]ATM
-----
Sat Sep 25 14:12:16 1999
-----
Terminé Poste de travail
```

www.kitetoa.com - we will hack  
your pizzas for free

# Sarkospam: maison ou externe?

- n L'enchanteur Nouveaux Médias: externe ou interne ?
- n Ce fichier laisse entendre que des données ont été fournies par la Droite Libre



```
ls
cd ~/tmp
pwd
cd ~/lenchanteur/acadomia
clear
ls
pwd
tar cvzf /opt/www/clients/d/droitelibre/lenchanteur.tar.gz *
exit
ls
cd ..
du lenchanteur/
pwd
cd lenchanteur
ls
cd ..
du lenchanteur
du lenchanteur/
cd ..
ls
cd l
du lenchanteur/
cd lenchanteur/
ls
cd ..
cd
exit
```



# Le grand méchant Net

---

- n Combien de millions dépensés pour protéger la porte qui relie l'entreprise à Internet...?
- n Il existe d'autres portes
- n Pourquoi cette focalisation?



# Porte blindée, murs en carton

n Blinder la porte ne suffisait pas, même à la Maison-Blanche...

| File &               | Size  | Modified           | Owner |
|----------------------|-------|--------------------|-------|
| www.whitehouse.gov   |       |                    |       |
| .pickup              | 3072  | 31 mai 00 10:05:00 |       |
| Africa               | 6656  | 3 jun 99 14:54:33  |       |
| CEG                  | 10752 | 26 mai 00 22:55:00 |       |
| Initiatives          | 512   | 10 mai 00 16:43:32 |       |
| Jobs                 | 512   | 30 mai 00 16:37:01 |       |
| New                  | 512   | 3 jun 99 14:56:08  |       |
| OMB                  | 1024  | 6 déc 99 18:35:01  |       |
| ONAP                 | 1536  | 13 avr 00 16:05:01 |       |
| PCSD                 | 512   | 29 jun 99 23:18:03 |       |
| ROTP                 | 512   | 4 jul 99 21:22:39  |       |
| WH                   | 1024  | 30 mai 00 21:35:01 |       |
| WHTeens              | 512   | 28 avr 00 17:35:02 |       |
| WH_Fellows           | 512   | 3 jun 99 15:10:24  |       |
| audio                | 2560  | 27 mai 00 16:14:03 |       |
| cgi-bin              | 512   | 10 avr 00 16:35:42 |       |
| fsbr                 | 512   | 12 mai 00 14:05:35 |       |
| imagemap             | 512   | 21 jul 99 22:25:58 |       |
| images               | 512   | 3 jun 99 15:10:46  |       |
| initiatives          | 512   | 10 mai 00 16:43:32 |       |
| internship           | 512   | 4 mai 00 18:25:01  |       |
| library              | 512   | 29 sep 99 20:13:22 |       |
| .hot                 | 6656  | 31 mai 00 07:30:00 |       |
| EMBARGOED            | 512   | 22 sep 99 18:12:58 |       |
| HoldRelease          | 512   | 13 oct 99 17:12:42 |       |
| OldReleases          | 512   | 31 déc 99 07:30:01 |       |
| 19991214-3.hot.bak   | 985   | 14 déc 99 18:30:04 |       |
| 19991217-2.brief.bak | 15481 | 17 déc 99 22:05:00 |       |
| 19991217-3.hot.bak   | 4182  | 17 déc 99 21:20:01 |       |
| 19991217-4.hot.bak   | 8630  | 17 déc 99 23:00:02 |       |
| OIRelases            | 31824 | 12 nov 98 21:34:26 |       |
| bad1204              | 41583 | 4 déc 98 21:12:37  |       |

Selected: /library/.hot/EMBARGOED/

www.kitetoa.com - we will hack  
your pizzas for free



# Porte blindée, murs en carton II

---

n Blinder la porte ne suffit toujours pas...

# Lance Armstrong

n Quelques milliers d'e-mails a disposition des spammers.

```
- <viewentries t
- <viewentry p children="4" descendants="4" siblings="6152">
- <entrydata " category="true">
  <text>199
</entrydata
- <entrydata
  <number
</entrydata
</viewentry>
- <viewentry p A44F96BA86256BF9001D44ED" noteid="2136" siblings="4">
- <entrydata 444F96BA86256BF9001D44ED" name">
  <text>Ca
</entrydata
- <entrydata
  <text/>
</entrydata
</viewentry>
- <viewentry p 6ACF435286256BFA0063D15A" noteid="7DC2" siblings="4">
- <entrydata 6ACF435286256BFA0063D15A" name">
  <text>Ca
</entrydata
- <entrydata
  <text/>
</entrydata
</viewentry>
- <viewentry p 3E52B3E86256BFB00602A1E" noteid="BE96" siblings="4">
- <entrydata 3E52B3E86256BFB00602A1E" name">
  <text>Ca
</entrydata
- <entrydata
  <text/>
</entrydata
</viewentry>
- <viewentry p 719E1C3386256BFC001FD3CE" noteid="DB3A" siblings="4">
- <entrydata 719E1C3386256BFC001FD3CE" name">
  <text>Ca
</entrydata
- <entrydata
  <text/>
</entrydata
</viewentry>
- <viewentry p children="3" descendants="3" siblings="6152">
- <entrydata " category="true">
  <text>1f
</entrydata
- <entrydata
  <number
</entrydata
```

www.kitetoa.com - we will hack  
your pizzas for free



# Classique ou Hippie?

---

- n En matière de tests d'intrusion, vous êtes plutôt classique ou hippie?
- n Le concept de hacking de pizzas
- n Comment est-il possible que Kitettoa.com existe...
- n Alors que nous n'avons pas de capacités techniques particulières...



# So what?

---

- n Que faire?
- n Existe-t-il un moyen de sécuriser un réseau, une application web, etc.?
- n La responsabilité des directions générales.
- n La conclusion à laquelle les hackers de pizzas sont arrivés...