HACKEZ-MOI CETTE APPLICATION

RMLL, 2010
Bordeaux, France, 7 juillet 2010

MENU DU JOUR

- Comment attaquer une application Web
  - Découverte
  - Code ouvert
  - Cas réels

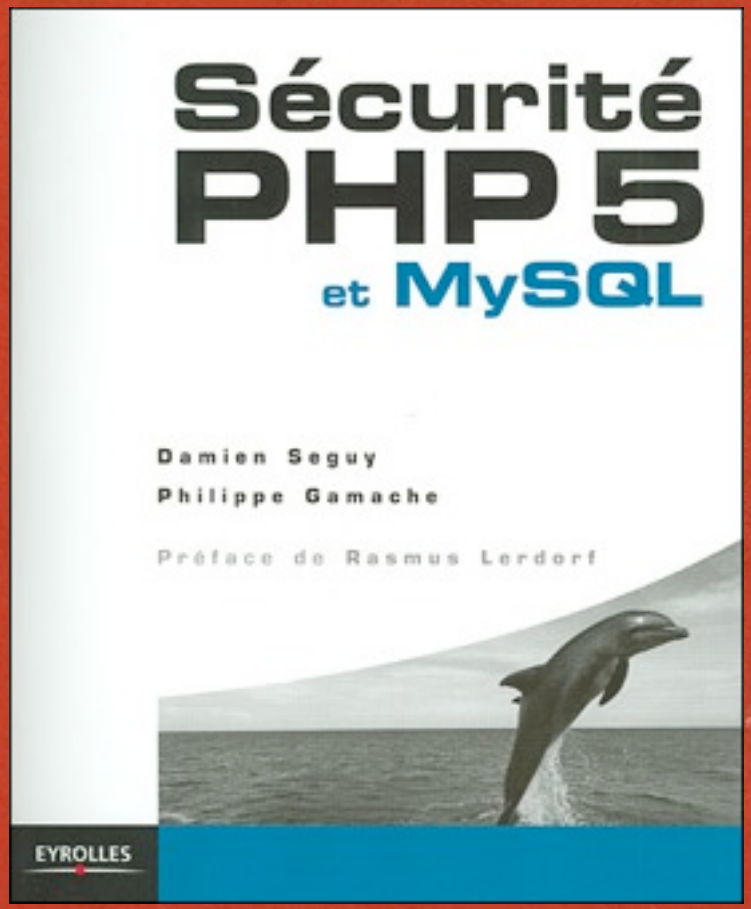
AFUP

- http://www.afup.org/

Alter Way
consulting

AYE' CAPTAIN

- Groupe Alter Way
- Damien Seguy
  - damien.seguy@alterway.fr
- Expertise PHP MySQL
- Livre blanc industrialisation

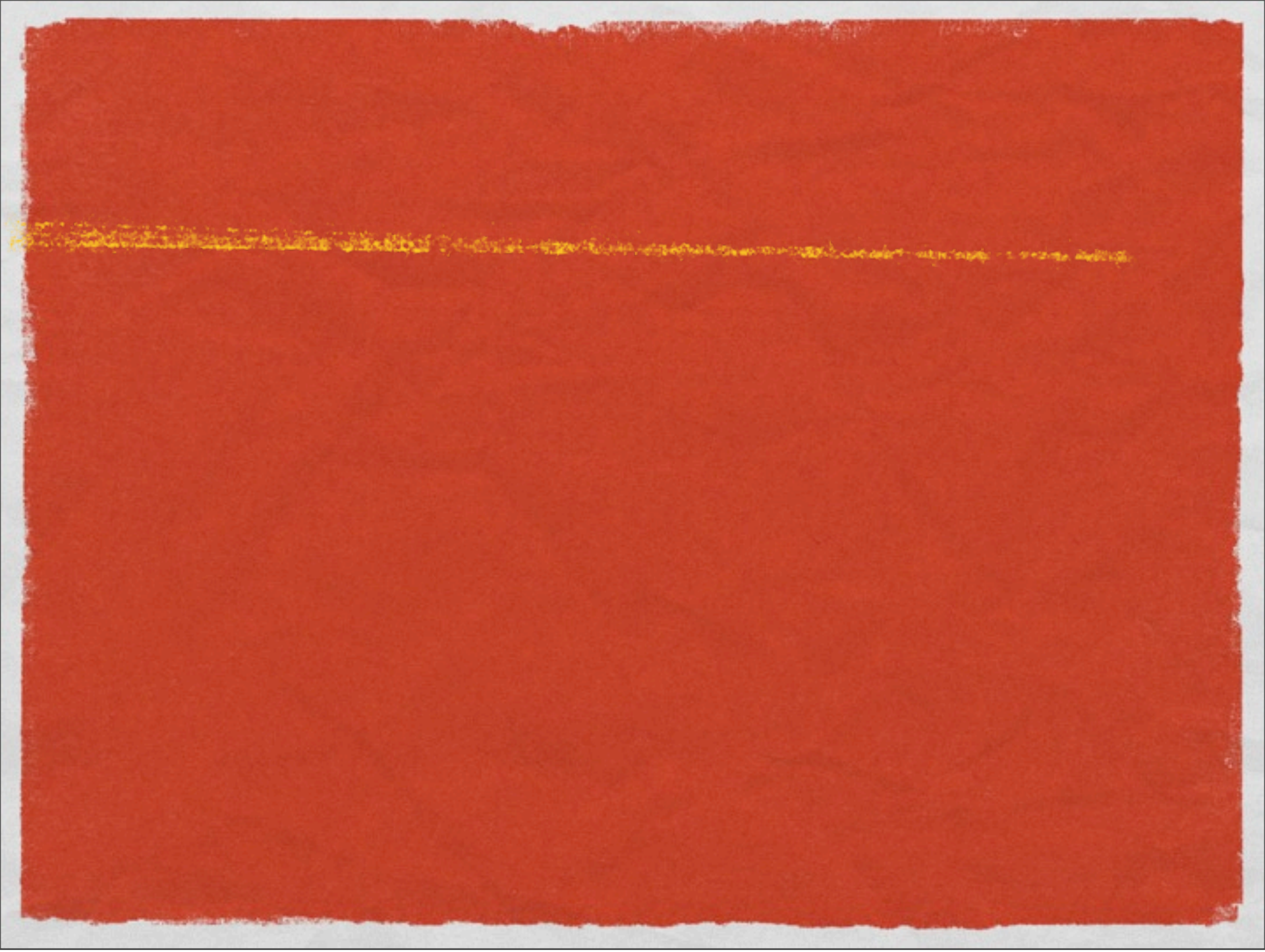


QUESTIONS?

RÉPONSES?

LA SÉCURITÉ?

- Protéger le compte root
- Abus de ressources
- Destruction de données
- Modification de données
- Lecture de données
- Simple ridicule...




http://www.saint-gobain.com/?=
Alter Way
Communauté
Outils
Actualité (7)
www.saint-gobain.com 120 × 67 ...
php


http://www.saint-
Alter Way
Communauté
Outils
www.saint-gobain.com 120 × 67 ...
php


http://www.essilor.com/?=
Alter Way
Communauté
Outils
Actualit
www.essilor.com 120 × 67 pixels
php


http://www.saint-
Alter Way
Communauté
Outils
www.saint-gobain.com 120 × 67 ...
php

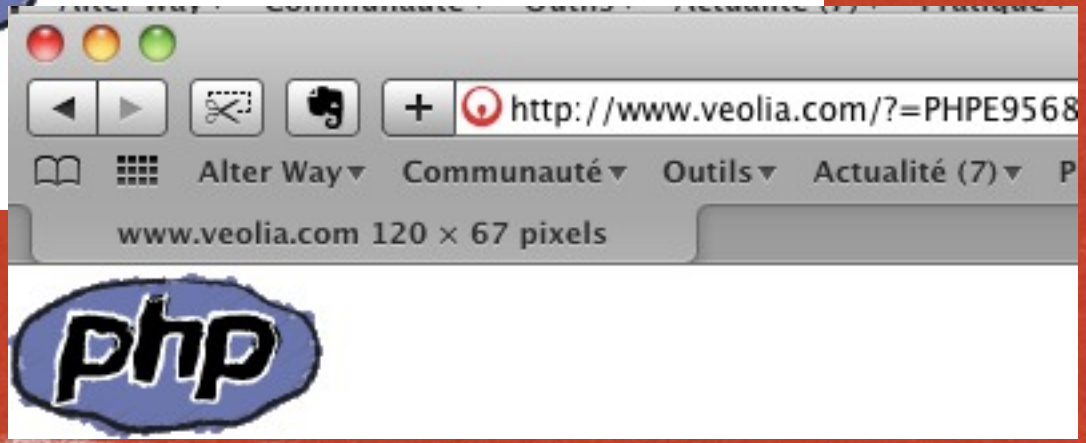

http://www.essilor.com/?=
Alter Way
Communauté
Outils
Actualit
www.essilor.com 120 × 67 pixels
php

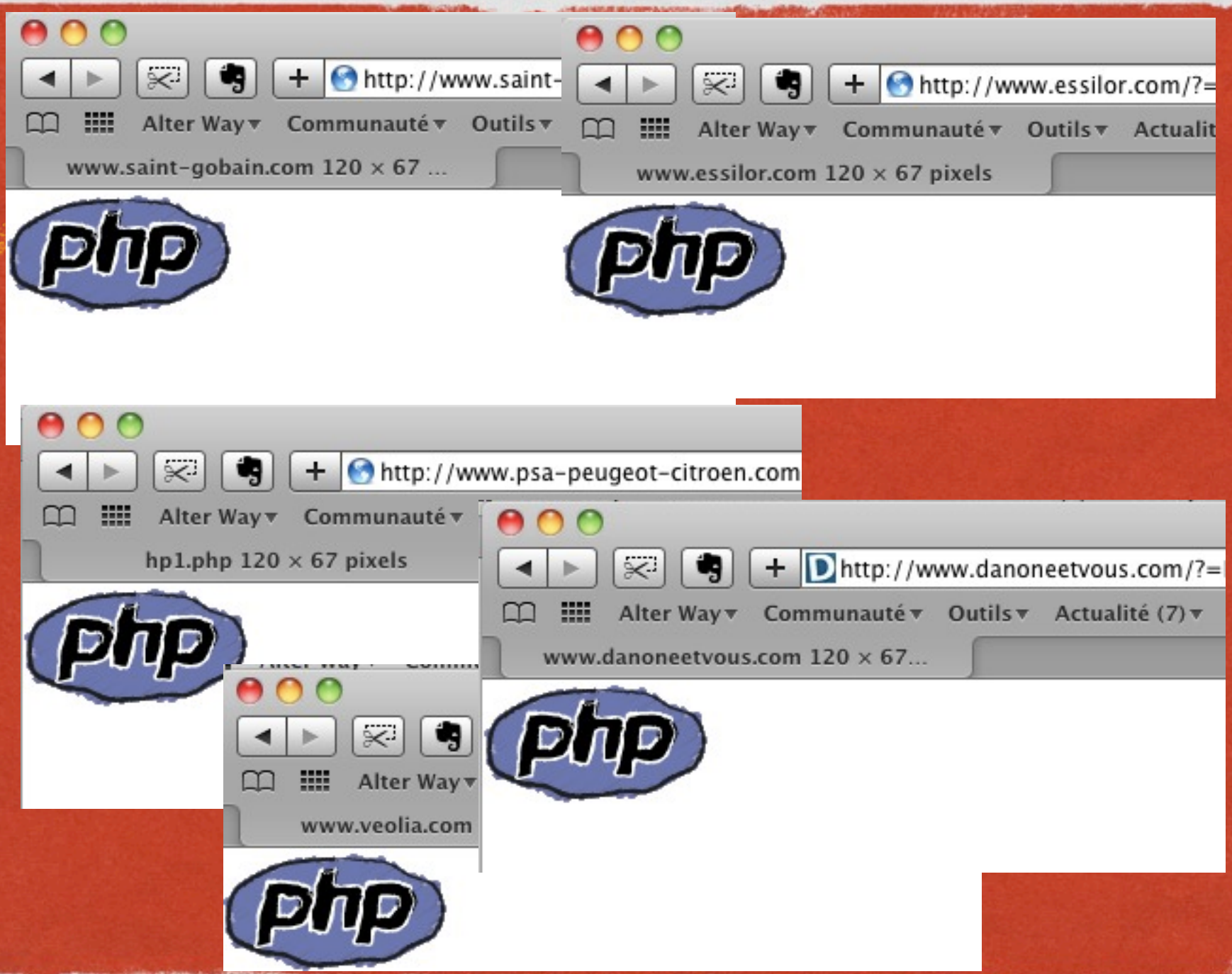

http://www.psa-peugeot-citroen.com
Alter Way
Communauté
Outils
Actualité (7)
Pra
hp1.php 120 × 67 pixels
php

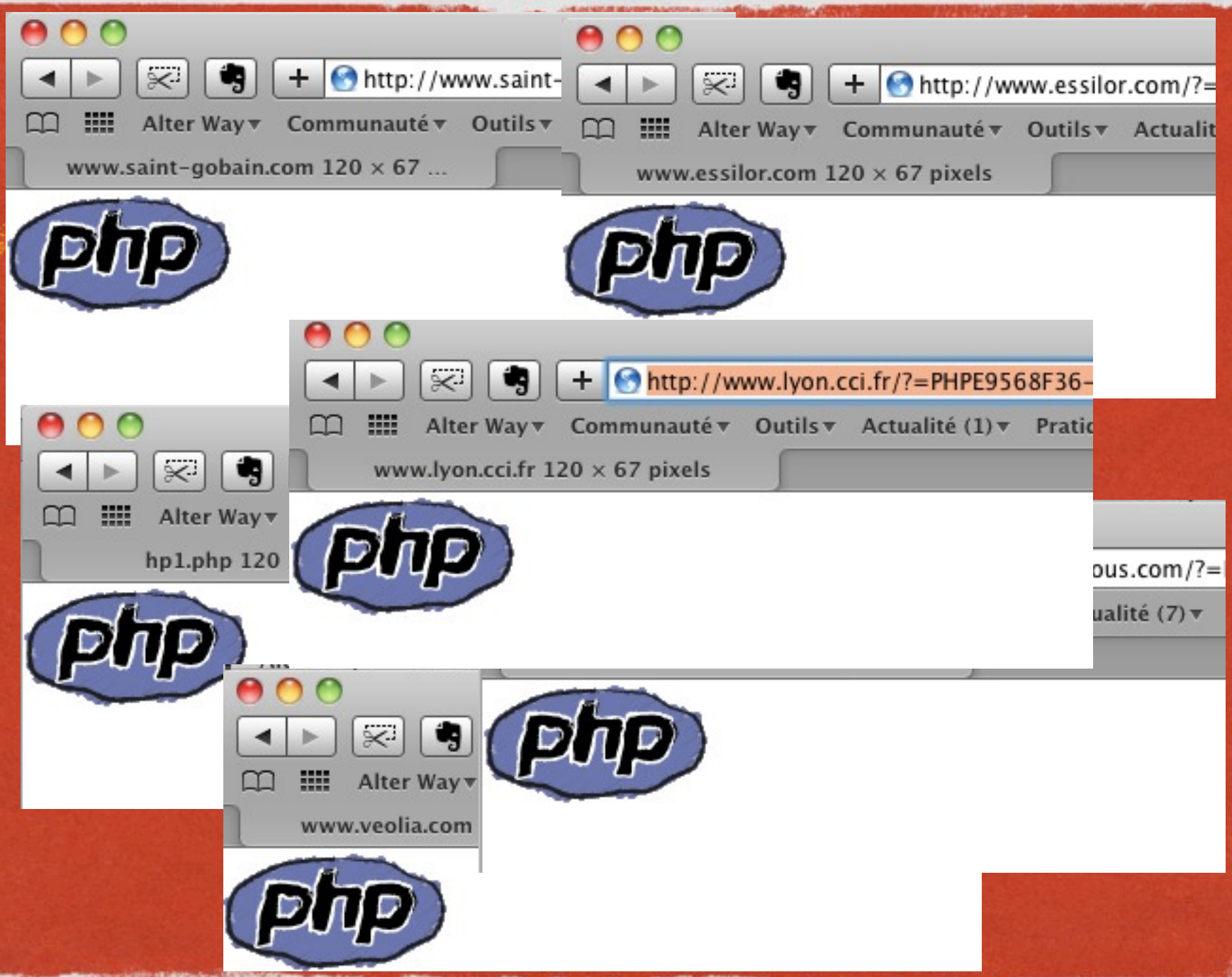

http://www.saint-
Alter Way
Communauté
Outils
www.saint-gobain.com 120 × 67 ...
php


http://www.essilor.com/?=
Alter Way
Communauté
Outils
Actualit
www.essilor.com 120 × 67 pixels
php

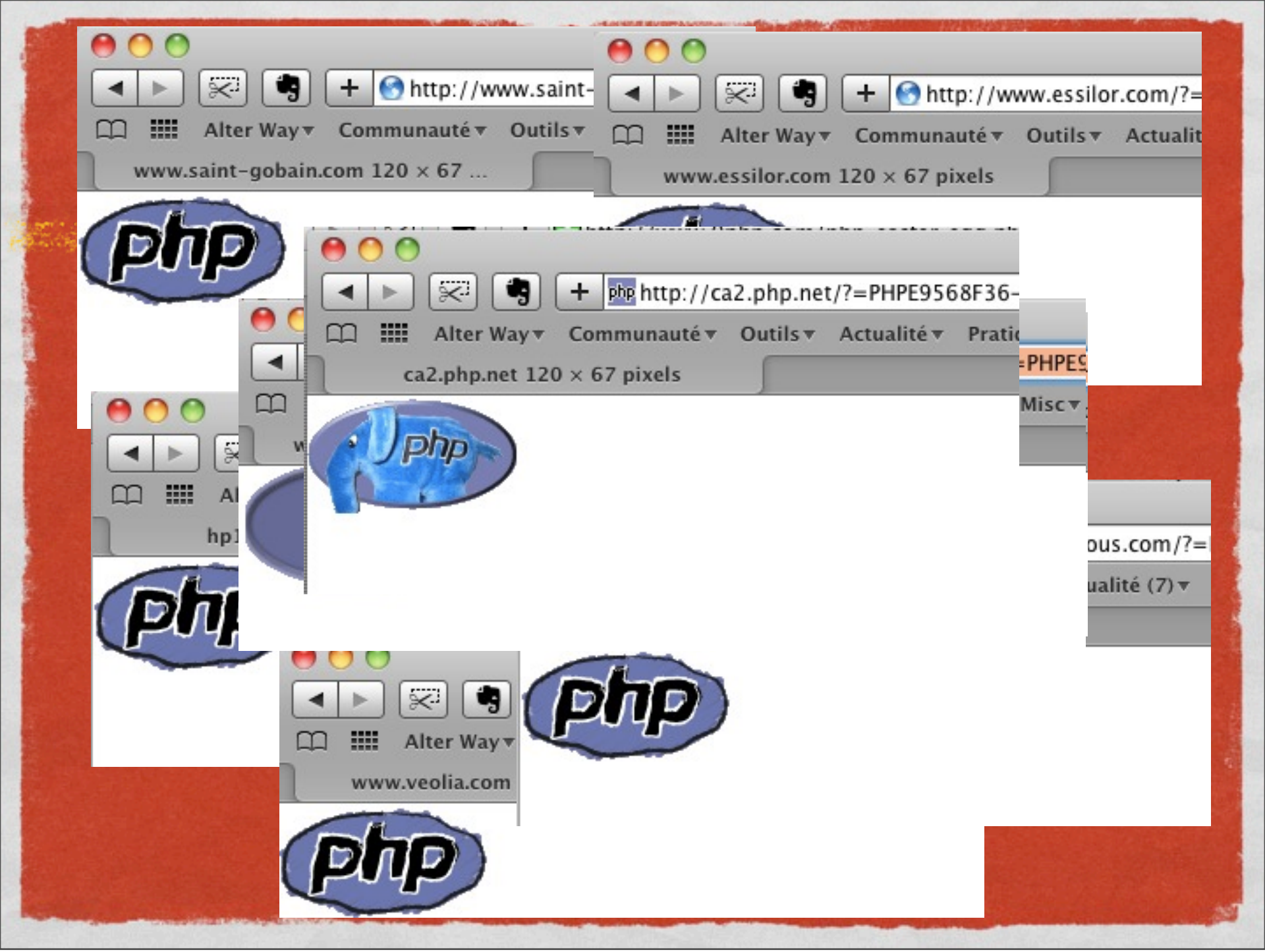

http://www.psa-peugeot-citroen.com
Alter Way
Communauté
Outils
Actualité (7)
hp1.php 120 × 67 pixels
php


http://www.veolia.com/?=PHPE9568
Alter Way
Communauté
Outils
Actualité (7)
www.veolia.com 120 × 67 pixels
php


http://www.saint-
Alter Way
Communauté
Outils
www.saint-gobain.com 120 × 67 ...
php
http://www.essilor.com/?=
Alter Way
Communauté
Outils
Actualit
www.essilor.com 120 × 67 pixels
php
http://www.psa-peugeot-citroen.com
Alter Way
Communauté
hp1.php 120 × 67 pixels
php
http://www.danoneetvous.com/?=
Alter Way
Communauté
Outils
Actualité (7)
www.danoneetvous.com 120 × 67...
php
Alter Way
www.veolia.com
php


http://www.saint-
Alter Way
Communauté
Outils
www.saint-gobain.com 120 × 67 ...
http://www.essilor.com/?=
Alter Way
Communauté
Outils
Actualit
www.essilor.com 120 × 67 pixels
http://www.lyon.cci.fr/?=PHPE9568F36-
Alter Way
Communauté
Outils
Actualité (1)
www.lyon.cci.fr 120 × 67 pixels
Alter Way
hp1.php 120
Alter Way
www.veolia.com
php


http://www.saint-
Alter Way
Communauté
Outils
www.saint-gobain.com 120 × 67 ...
http://www.essilor.com/?=
Alter Way
Communauté
Outils
Actualit
www.essilor.com 120 × 67 pixels
http://www.rpima1.terre.defense.gouv.fr/?=PHPE
Alter Way
Communauté
Outils
Actualité
Pratique
Misc
www.rpima1.terre.defense.gouv.fr...
Alter Way
www.veolia.com
php


http://www.saint-
Alter Way
Communauté
Outils
www.saint-gobain.com 120 × 67 ...
http://www.essilor.com/?=
Alter Way
Communauté
Outils
Actualit
www.essilor.com 120 × 67 pixels
php
http://ca2.php.net/?=PHPE9568F36-
Alter Way
Communauté
Outils
Actualité
ca2.php.net 120 × 67 pixels
Misc
Alter Way
www.veolia.com
php

VOCABULAIRE

- Découverte
  - En apprendre plus sur l'application
- Vulnérabilité
  - Une faille qui permet de perturber le système
- Attaque
  - Une vulnérabilité avec un objectif

MONTJOIE SAINT DENIS!

- Mettez-vous dans la peau d'un pirate
- Commencez par découvrir, puis affinez
  - Quels sont les points d'entrée accessibles?
  - Comment les exploiter?
- Comment puis-je détourner cette application?

A L'ABORDAGE

INFORMATIONS EN VRAC

- curl, wget, firefox
- HTTP headers reader

```
GET / HTTP/1.1
Host: www.pyrenees-orientales.pref.gouv.fr
User-Agent: Mozilla/5.0 (Macintosh; U; Inte
Referer: http://www.rexswain.com/httpview.h
Connection: close
```

Receiving Header:

```
HTTP/1.1·200·OK(CR)(LF)
Content-Type:·text/html(CR)(LF)
Server:·Microsoft-IIS/7.0(CR)(LF)
X-Powered-By:·PHP/5.2.8(CR)(LF)
X-Powered-By:·ASP.NET(CR)(LF)
Date:·Mon,·08·Feb·2010·16:15:57·GMT(CR)(LF)
Connection:·close(CR)(LF)
Content-Length:·4951(CR)(LF)
(CR)(LF)
```

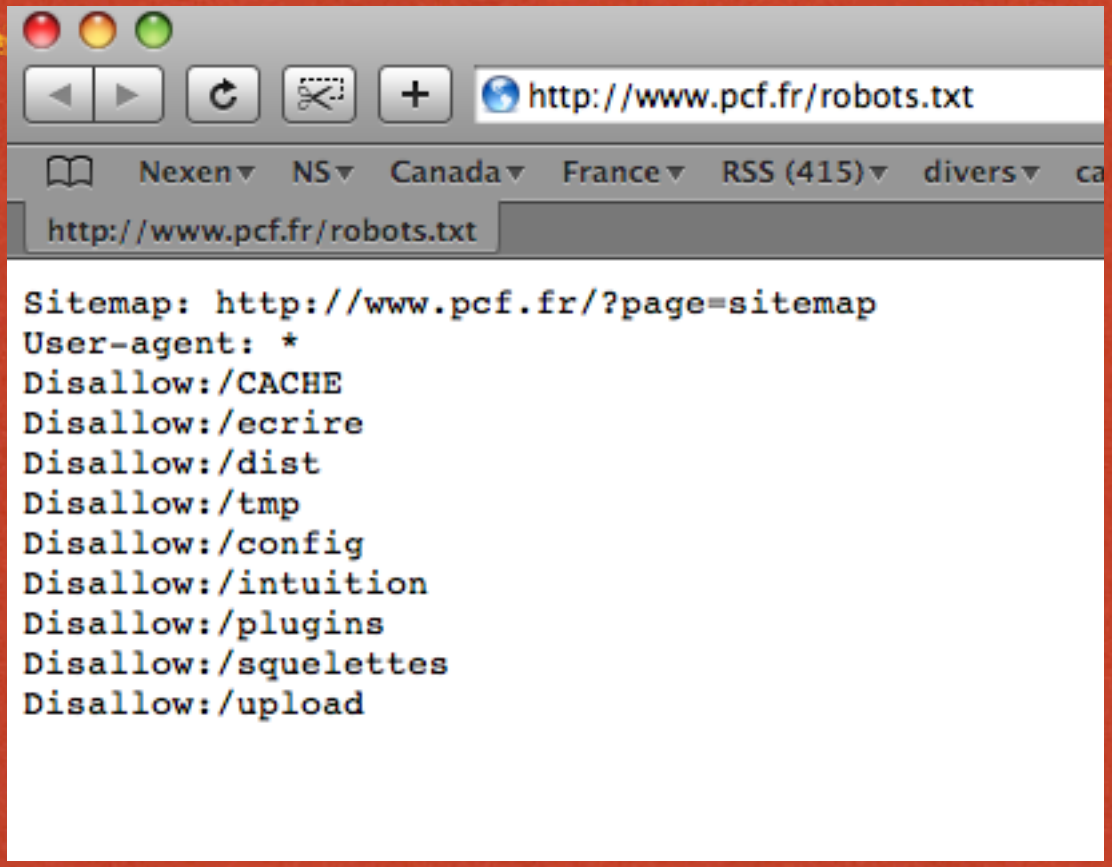

Surfez intelligent : les indispensables
http://www.surfez-intelligent.gouv.fr/spip.php?accueil=1
RSS
Alter Way
Communauté
Outils
Actualité (1)
Pratique
Misc
Immo
Surfez intelligent : les indispensables
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE
LES INDISPE
accuEil
pouRquoi cE sitE?
La Charte
pour la promotion
de l'authentification
Les dossiers
>> Qu'est-ce que le filoutage (Phishing) ?
>> Qu'est-ce que
Comme dans la vie de tous les jours, il y a des règles
sur Internet pour pouvoir en profiter pleinement. Ave
publics et privés- le Secrétariat d'Etat en charge
Développement de l'économie numérique vous pro
bonnes pratiques indispensables pour "surfer" en toute
Données personnelles, ordinateur et
Prenez les choses en main
Vos Données
soyez le maitre!
Votre messagerie
faites le tri!


Surfez intelligent : les indispensables
http://www.surfez-intelligent.gouv.fr/spip.php?accueil=1
Alter Way
Communauté
Outils
Actualité (1)
Pratique
Misc
Immo
Surfez intelligent : les indispensables
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE
LES INDISPE
accuEil
pouRquoi cE sitE?
Comme dans la vie de tous les jours, il y a des règles
>> Qu'est-ce que
Receiving Header:
HTTP/1.1 302 Found(CR)(LF)
Date: Mon, 08 Feb 2010 16:22:32 GMT(CR)(LF)
Server: Apache(CR)(LF)
X-Powered-By: PHP/4.4.1(CR)(LF)
Location: spip.php?accueil=1(CR)(LF)
Content-Length: 0(CR)(LF)
Connection: close(CR)(LF)
Content-Type: text/html(CR)(LF)
(CR)(LF)

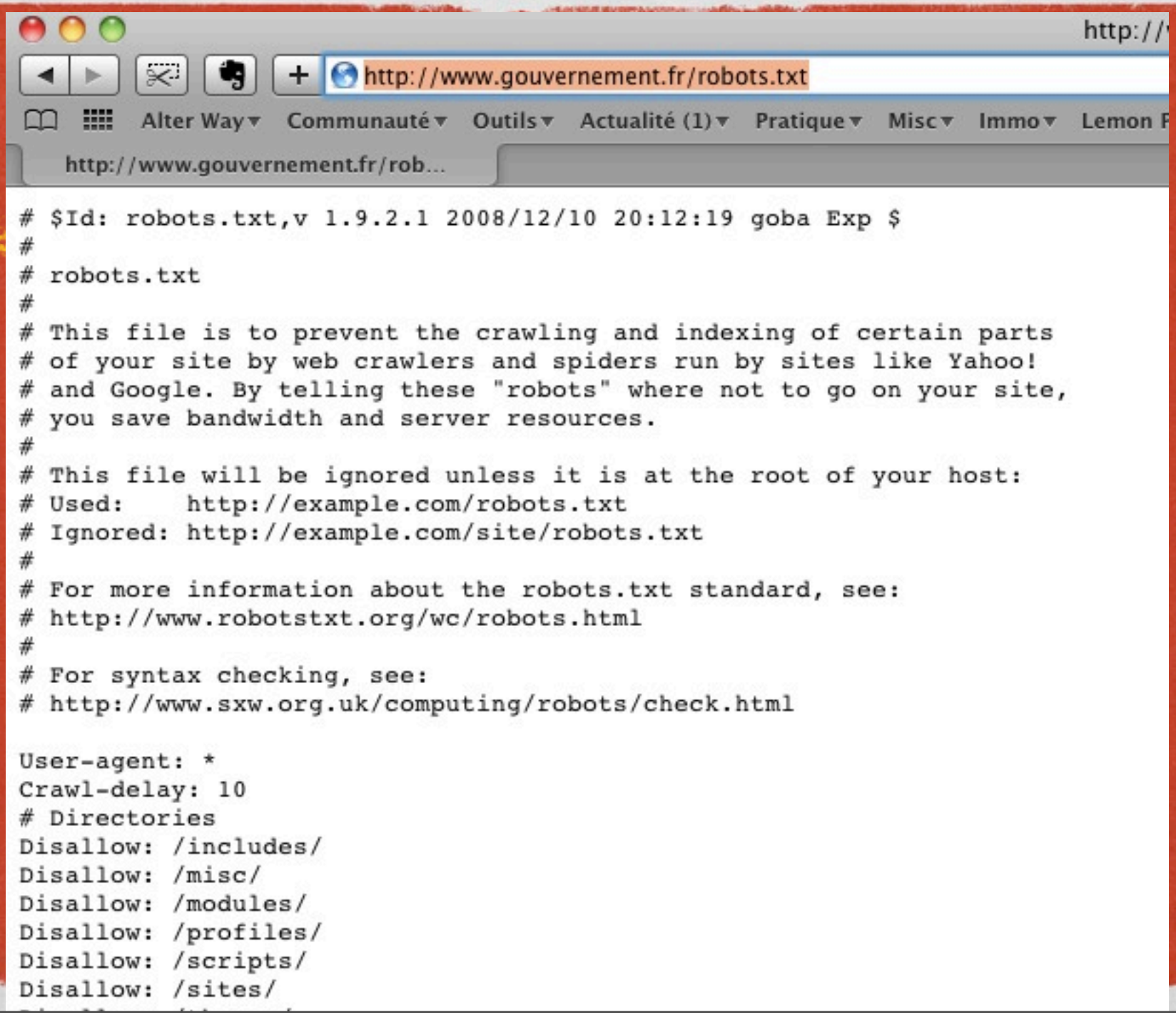

1er Régiment de Parachutistes d'Infanterie de
http://www.rpima1.terre.defense.gouv.fr/
Alter Way
Communauté
Outils
Actualité (1)
Pratique
Misc
1er Régiment de Parachutistes d'I...
MINISTÈRE DE LA DÉFENSE
1er Régiment de Parachutistes d'Infanterie de
EMA | DGA | SGA | Terre | Marine | Air | Gendarmerie | Santé
Presse
Vidéo
Cadres d'emploi
Sigles
Cercle mess
Découverte
Historique
Attributs
Fanfare
Implantation
Au cœur du régiment
Missions
Organisation
Personnel
Matériel
Témoignages
Votre espace
Contacts
>> Accueil /
Bienvenue
Bienvenue sur le site officiel du 1er Régiment de Parach
de Marine, régiment Forces Spéciales.


1er Régiment de Parachutistes d'Infanterie de
http://www.rpima1.terre.defense.gouv.fr/
Alter Way
Communauté
Outils
Actualité (1)
Pratique
Misc
1er Régiment de Parachutistes d'I...
MINISTÈRE DE LA DÉFENSE
1er Régiment de Parachutistes d'Infanterie de
EMA | DGA | SGA | Terre | Marine | Air | Gendarmerie | Santé
Presse
Vidéo
Cadres d'emploi
Sigles
Cercle mess
Découverte
Historique
Contacts
>> Accueil /
Bienvenue
Bienvenue sur le site officiel du 1er Régiment de Parach
Forces Spéciales.
Receiving Header:
HTTP/1.1 200 OK(CR)(LF)
Date: Mon, 08 Feb 2010 16:25:59 GMT(CR)(LF)
Server: Apache/1.3.41 (Unix)(CR)(LF)
X-Powered-By: PHP/4.1.2(CR)(LF)
Connection: close(CR)(LF)
Transfer-Encoding: chunked(CR)(LF)
Content-Type: text/html(CR)(LF)
(CR)(LF)

ROBOTS.TXT



- http://www.pcf.fr/robots.txt


http://www.gouvernement.fr/robots.txt
Alter Way
Communauté
Outils
Actualité (1)
Pratique
Misc
Immo
http://www.gouvernement.fr/rob...
$Id: robots.txt,v 1.9.2.1 2008/12/10 20:12:19 goba Exp $
#
robots.txt
#
This file is to prevent the crawling and indexing of certain parts
of your site by web crawlers and spiders run by sites like Yahoo!
and Google. By telling these "robots" where not to go on your site,
you save bandwidth and server resources.
#
This file will be ignored unless it is at the root of your host:
Used: http://example.com/robots.txt
Ignored: http://example.com/site/robots.txt
#
For more information about the robots.txt standard, see:
http://www.robotstxt.org/wc/robots.html
#
For syntax checking, see:
http://www.sxw.org.uk/computing/robots/check.html
User-agent: *
Crawl-delay: 10
Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /sites/

ROBOTS.TXT

- Empoisonnez les données
  - Ne mettez pas seulement les dossiers à protéger
  - Mettez des dossiers qui n'existent pas
  - Notez les IP qui s'y connectent
- Vérifiez en ligne les URLs de votre site

Sleepin'bed Camp 2P(140) gris Quechua F

http://store.quechua.com/quechua_supporte_les_reumeuleuleu-id_8129329.html

Alter Way ▾ Communauté ▾ Outils ▾ Actualité (5) ▾ Pratique ▾ Misc ▾ Immo ▾ PHP100 CodeIgniter ...P

Sleepin'bed Camp 2P(140) gris Q...

Quechua

Mon compte Mon panier Aide

Nos sports | Nos produits | Soldes

Accueil / Sleepin'bed Camp 2P(140) gris

SAC DE COUCHAGE ; DUV

Sleepin'bed C

Ref : 8129329

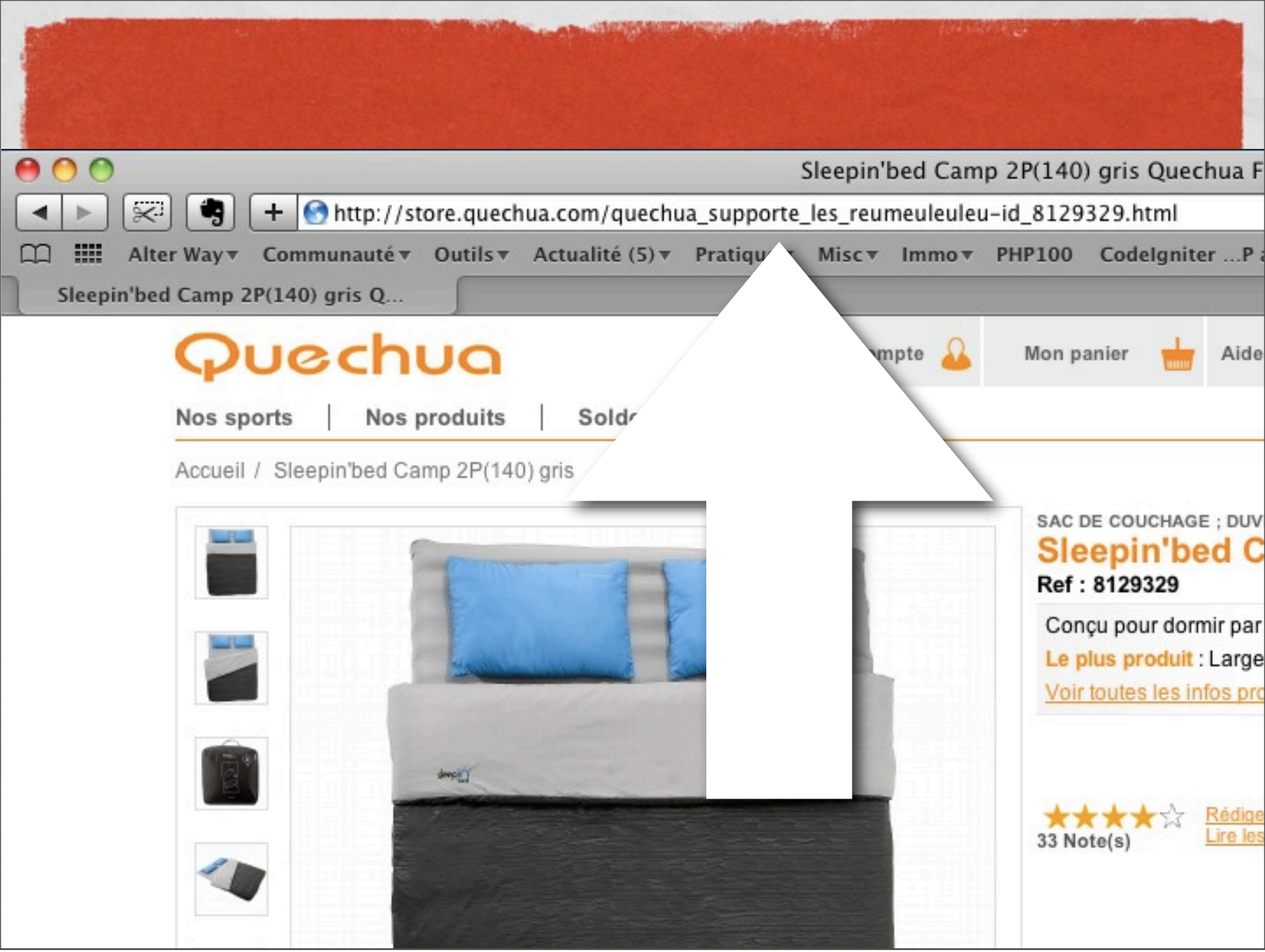
Conçu pour dormir par

Le plus produit : Large

Voir toutes les infos pro

★★★★☆ Rédige

33 Note(s) Lire les


Sleepin'bed Camp 2P(140) gris Quechua F
http://store.quechua.com/quechua_supporte_les_reumeuleuleu-id_8129329.html
Alter Way
Communauté
Outils
Actualité (5)
Misc
Immo
PHP100
CodeIgniter
Sleepin'bed Camp 2P(140) gris Q...
Quechua
Mon panier
Nos sports
Nos produits
Accueil / Sleepin'bed Camp 2P(140) gris
SAC DE COUCHAGE ; DUV
Sleepin'bed C
Ref : 8129329
Conçu pour dormir par
Le plus produit : Large
Voir toutes les infos pro
33 Note(s)

STEGANOGRAPHIE

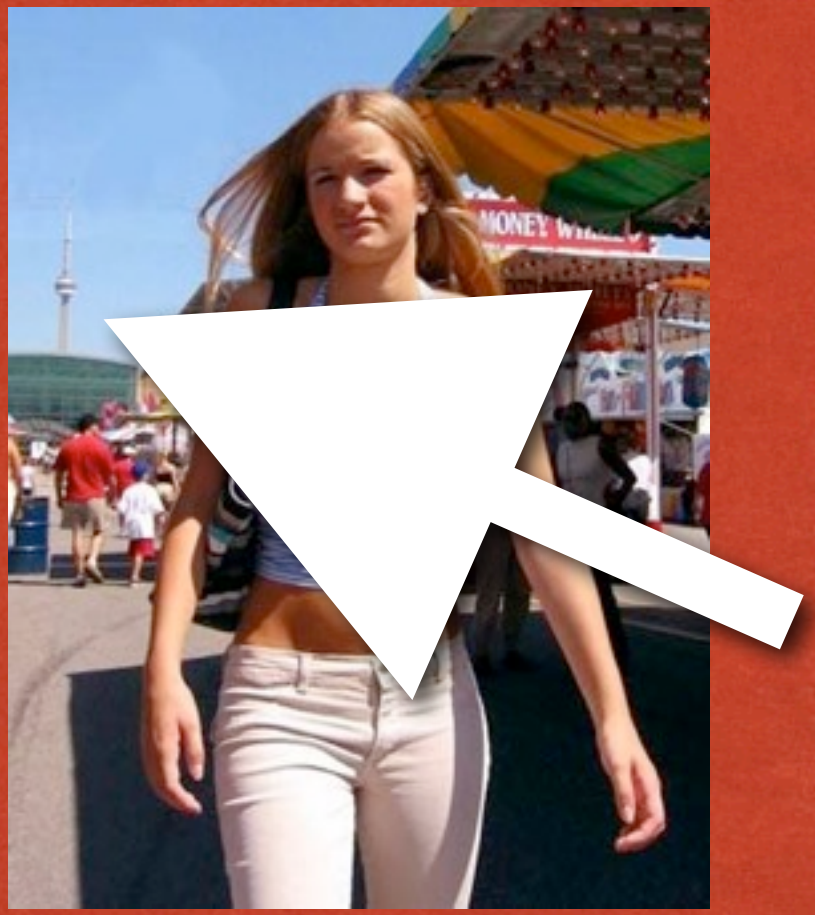
- L'art de cacher les choses à la vue de tous
- Trouvez la tour la plus haute du monde dans l'image suivante

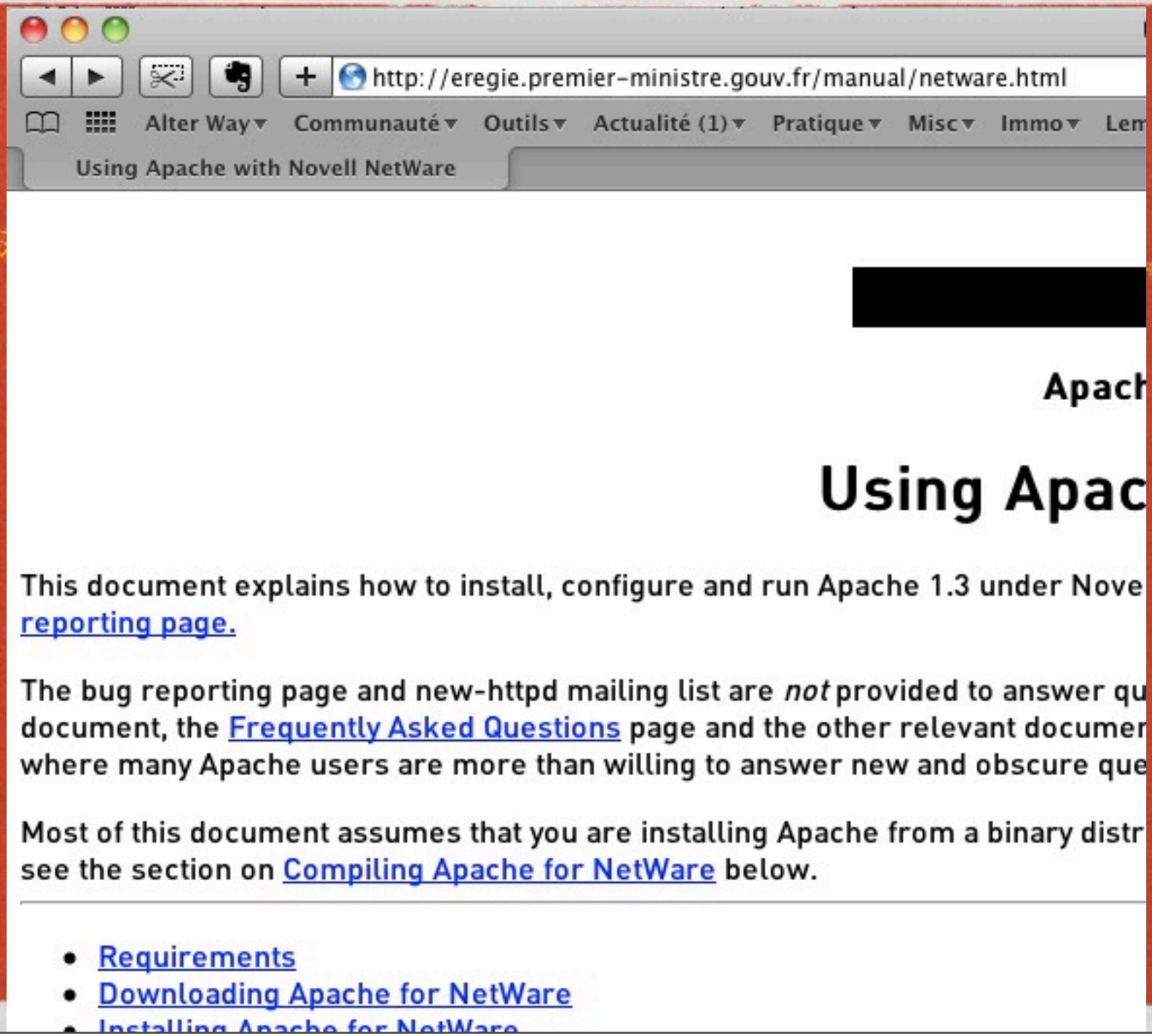
STEGANOGRAPHIE

- L'art de cacher les choses à la vue de tous
- Trouvez la tour la plus haute du monde dans l'image suivante

STEGANOGRAPHIE

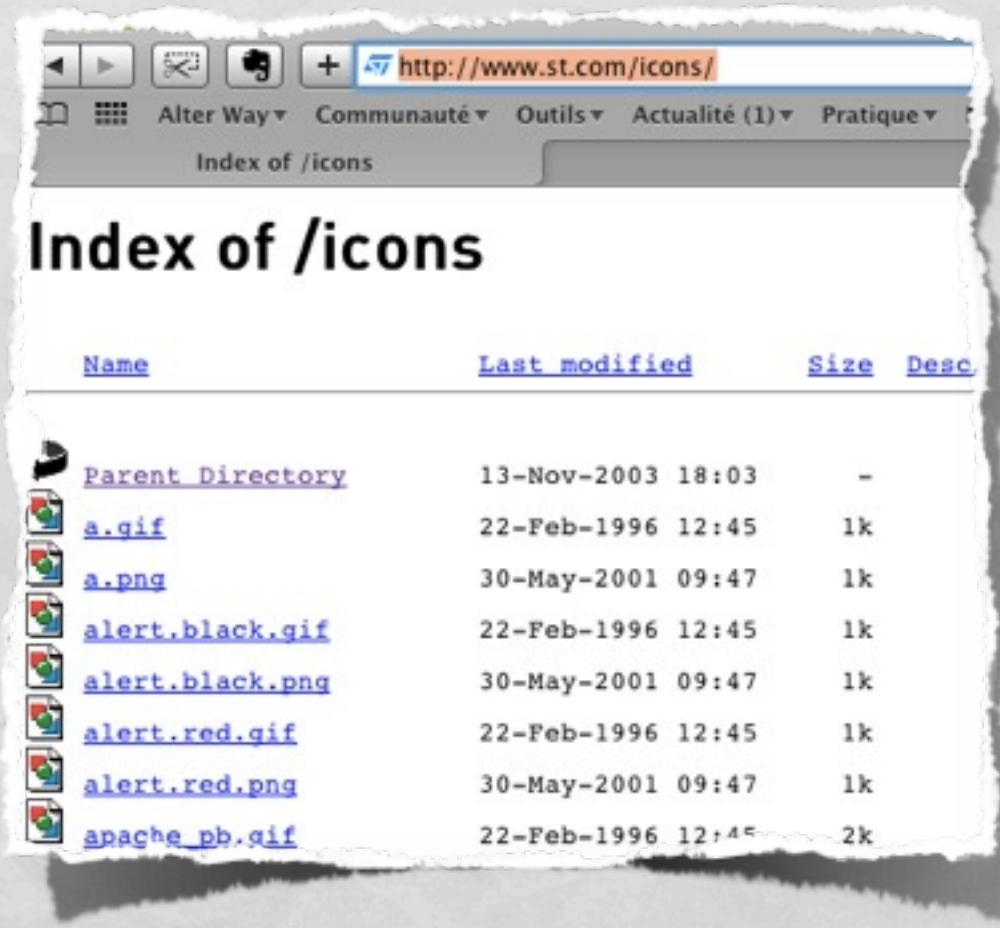
- L'art de cacher les choses à la vue de tous
- Trouvez la tour la plus haute du monde dans l'image suivante




http://eregie.premier-ministre.gouv.fr/manual/netware.html
Alter Way
Communauté
Outils
Actualité (1)
Pratique
Misc
Immo
Using Apache with Novell NetWare
Apach
Using Apac
This document explains how to install, configure and run Apache 1.3 under Nove
reporting page.
The bug reporting page and new-httpd mailing list are *not* provided to answer qu
document, the Frequently Asked Questions page and the other relevant documer
where many Apache users are more than willing to answer new and obscure que
Most of this document assumes that you are installing Apache from a binary distr
see the section on Compiling Apache for NetWare below.
Requirements
Downloading Apache for NetWare

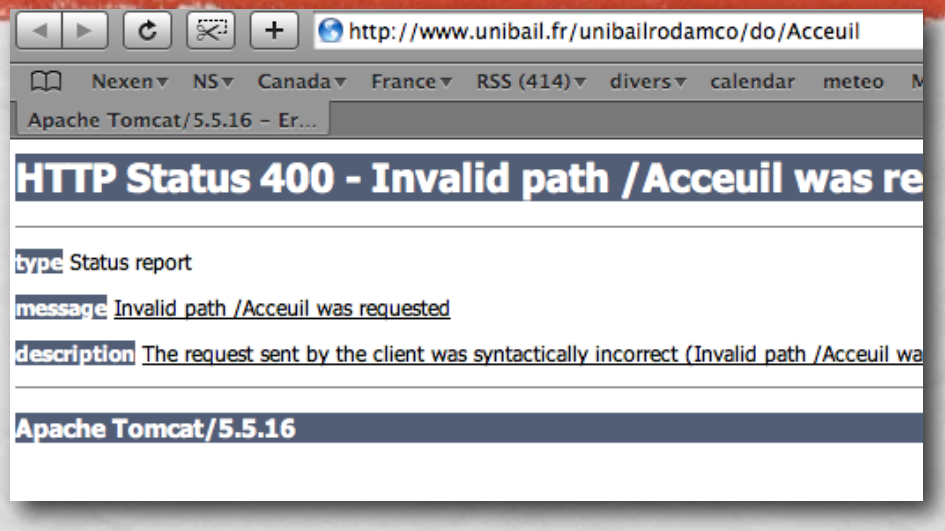
PAR DÉFAUT

- Signatures dans les entêtes HTTP
- Alias apache : /icons/
- Le listage de dossiers est mauvais



DONNÉES CACHÉES

- La page 404
- https
- Dossiers communs
  - includes, inc, lib, etc, ini, config,
  - hidden, protected, archives, bills, factures
  - admin, adm, admnistrateur, administrator, erreurs, classes



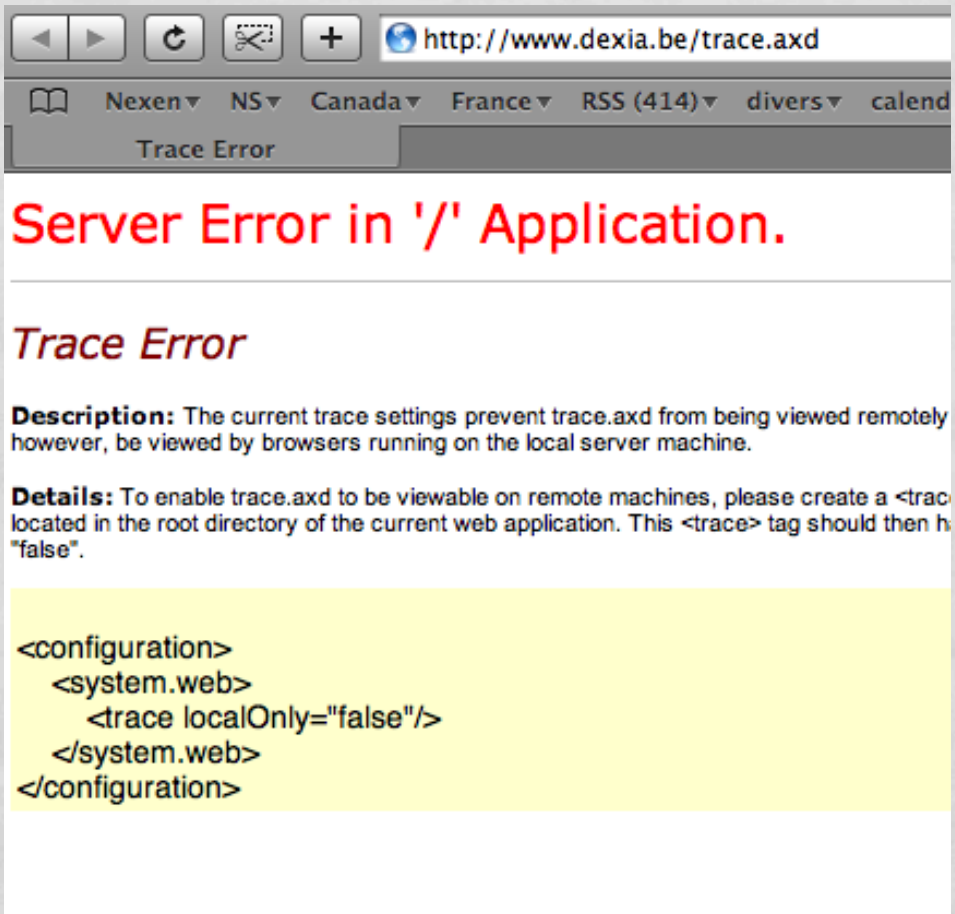
ACCÈS CODE SOURCE

- Tous les fichiers innocents
  - .ini, .yaml, .xml, .log, INSTALL.txt, zip, doc, odt,
- Dossiers assistants :
  - .svn, CVS, .ssh, .git, .bazaar, .bash_history...
- Fichiers :
  - phpinfo.php, trace.axd

NE PAS FAIRE!


http://eregie.premier-ministre.gouv.fr/
Alter Way
Communauté
Outils
Actualité (1)
Pratique
Misc
Im
http://eregie.premier-ministre.go...
<html><body>
<? //phpinfo(); ?>
</body></html>

MÊME EN ASP

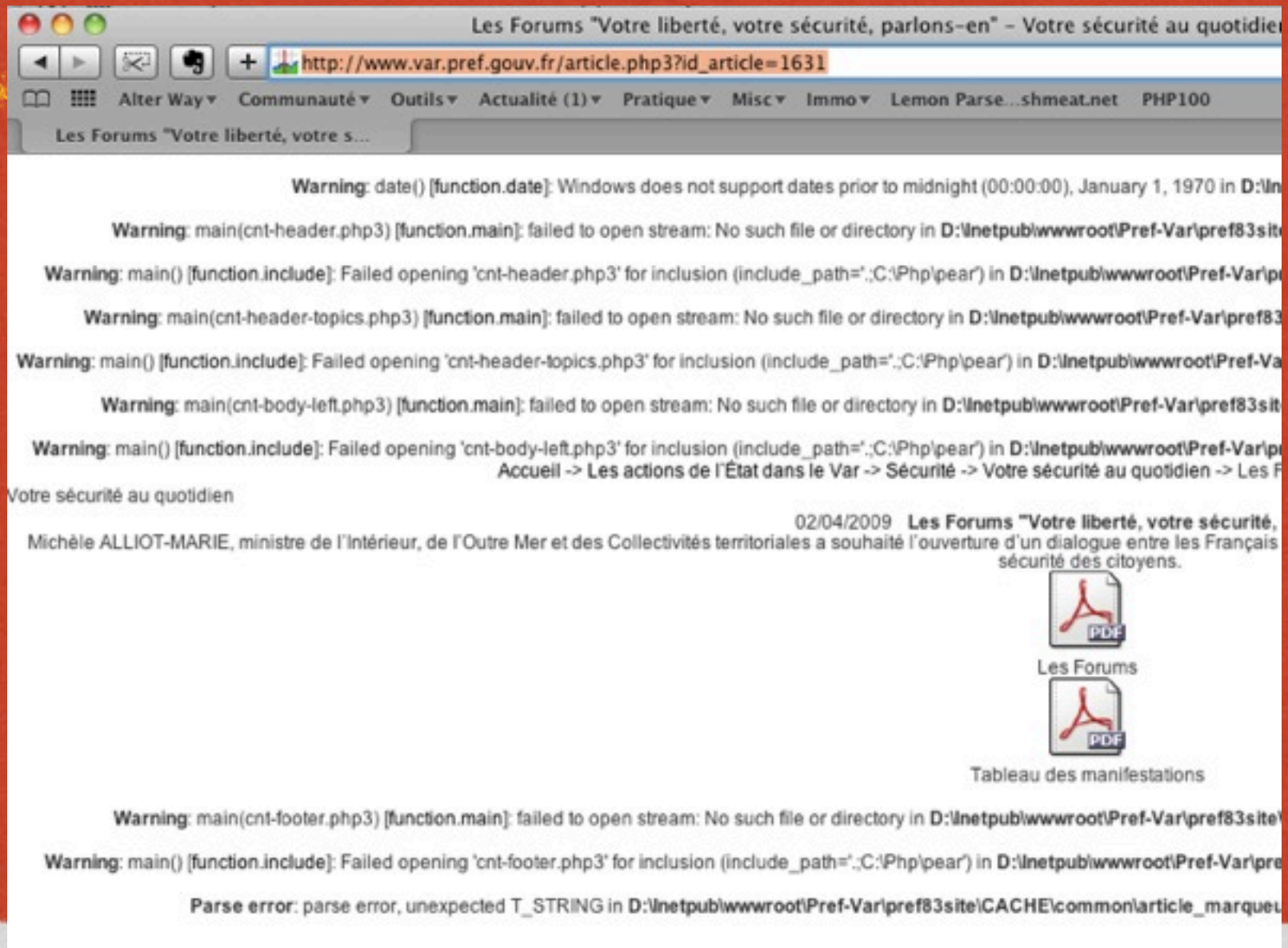

http://www.dexia.be/trace.axd
Nexen NS Canada France RSS (414) divers calend
Trace Error
Server Error in '/' Application.
Trace Error
Description: The current trace settings prevent trace.axd from being viewed remotely
however, be viewed by browsers running on the local server machine.
Details: To enable trace.axd to be viewable on remote machines, please create a <trac
located in the root directory of the current web application. This <trace> tag should then h
"false".
<configuration>
<system.web>
<trace localOnly="false"/>
</system.web>
</configuration>

MÊME EN ASP

BONNES PRATIQUES

- Utilisez un dossier hors Web
- Utilisez de préférences des directives du serveur Web
- Relisez régulièrement votre dossier Web

AFFICHAGE D'ERREURS



AFFICHAGE D'ERREURS

- Erreurs PHP
  - display_errors = off
  - error_reporting = E_ALL & ~E_NOTICE
- Erreurs de base de données
  - print mssql_get_last_error()
  - || die mssql_get_last_error() ou page blanche
- Essayez les assertions
  - beaucoup mieux que var_dump et echo

VICIEUX ?


http://www.travailler-mieux.gouv.fr/?page[]=recher
http://www.travailler-mieux.gouv.fr/?page[]=recherche
Alter Way
Communauté
Outils
Actualité (1)
Pratique
Misc
Immo
http://www.travailler-mieux.gouv...
Warning: preg_match() expects parameter 2 to be string, array given in
/home/stresstravail/public_html/travailler-mieux/ecrire/public/styli

TESTS

- Listez tous les fichiers de votre application
- Accédez directement aux fichiers (sans variables) et dossiers
- Transformez les variables en tableaux
  - url.php?x[]=0 ou url.php?x[][][]=0
- Recherchez du code PHP, SQL dans la page de résultat
- Ajoutez des variables courantes (debug, admin)
- Combinez GET, POST et COOKIES

FUZZING

- Ces tests sont longs et pénibles
  - Automatisez les!
- Construisez des dictionnaires de valeurs
- Testez les combinaisons
- Souvent
- Automatiquement

COTÉ CODE SOURCE

MORT À REGISTER_GLOBALS

- register_globals = 0ff

MORT À REGISTER_GLOBALS

Il y a pas moins de

méthodes pour émuler register globals

MORT À REGISTER_GLOBALS

Il y a pas moins de

5

méthodes pour émuler register globals

MORT À REGISTER_GLOBALS

MORT À REGISTER_GLOBALS

- import_request_vars('P')

MORT À REGISTER_GLOBALS

- import_request_vars('P')
- extract($_GET)

MORT À REGISTER_GLOBALS

- import_request_vars('P')
- extract($_GET)
- foreach ($_POST as $k => $v)
  { $$k = $v; }

MORT À REGISTER_GLOBALS

- import_request_vars('P')
- extract($_GET)
- foreach ($_POST as $k => $v)
  { $$k = $v; }
- $GLOBALS[]

MORT À REGISTER_GLOBALS

- import_request_vars('P')
- extract($_GET)
- foreach ($_POST as $k => $v)
  { $$k = $v; }
- $GLOBALS[]
- parse_str()

MORT À REGISTER_GLOBALS

- Pire que l'original
- Toujours impossible de savoir
  si une variable est propre ou pas!
- Transférez les données dans un tableau $_CLEAN

			
Fichiers	4073	2086	4543
$_GET	149	17	318
$_POST	252	20	481
$_REQUEST	46	3	8098

DOS PAR $_REQUEST

- $_REQUEST : $_GET, $_POST et COOKIES!
- Si l'état peut être modifié via $_REQUEST, il peut être figé par COOKIE!
- Exemple : déconnexion par logoff = ON :
  - Les utilisateurs sont bloqués hors de l'application
  - Même les administrateurs
  - Il faut retirer les cookies du navigateur pour retrouver l'accès

MANTRA DE SÉCURITÉ

- Validez en entrée
- Protégez en sortie

PREG_DANGERS()

```php
$id = $_GET['id'];
if (!preg_match('/^\d+$/', $id))
{
  header('Location: ../index.php');
  die();
}

$requete = "SELECT * FROM user WHERE id = " . $_GET['id'];
```

PREG_DANGERS()

- Les REGEX ne vérifie que des chaînes de caractères
  - Aucune sémantique
- /^\d+$/ n'est pas un nombre!
  - C'est une chaîne de chiffres, sur une ligne
  - Attentions aux cas particuliers $
    - "100\nEt encore autre chose!"

TESTEZ VOS FILTRES

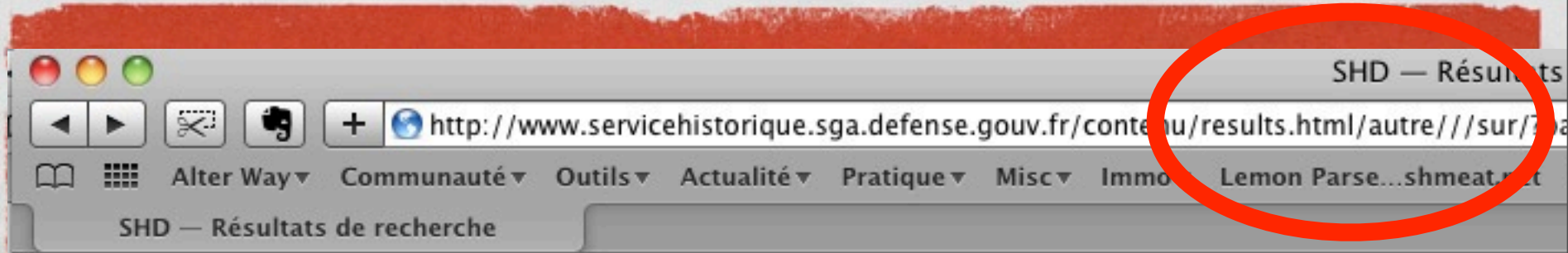
- Isolez-les
- Ajoutez une série de tests unitaires pour voir leur réaction
  - Un peu de fuzzing, aléatoire
  - Un gros dictionnaire de données maison
- Vérifiez-les souvent

ATTAQUE PAR PHP_SELF

- PHP_SELF est produit par le navigateur
- Apache le traite
- PHP le traite autrement


SHD — Résultat
http://www.servicehistorique.sga.defense.gouv.fr/contenu/results.html?base=ead&ba
Alter Way
Communauté
Outils
Actualité
Pratique
Misc
Immo
Lemon Parse...shmeat.net
SHD — Résultats de recherche
Collecter Conserver Communiquer
MINISTÈRE DE LA DÉFENSE
service historique de la Défense
Consulter en ligne - Accueil
>> Accueil / Ressources et publications / Consulter en ligne
Recherche simple :
Recherche avancée
Toutes les ressources
Fonds d'archives
Collections des bibliothèques
Résultats de recherche
Votre requête : Texte intégral : asdf
0 résultat dans 0 instrument de recherche.
Copyright Ministè
SGA
Secrétariat général pour l'administration


SHD — Résultats
http://www.servicehistorique.sga.defense.gouv.fr/contenu/results.html/autre///sur/?ba
Alter Way
Communauté
Outils
Actualité
Pratique
Misc
Immo
Lemon Parse...shmeat.net
SHD — Résultats de recherche
Site Internet www.defense.gouv.fr
Site internet du service historique de la Défense
→→ Accueil / Ressources et publications / Consulter en ligne
Consulter en ligne - Accueil
Recherche simple :
Lancer la recherche
Recherche avancée
Toutes les ressources
Fonds d'archives
Collections des bibliothèques
Site internet du Secrétariat général pour l'administration
Résultats de recherche
Votre requête : Texte intégral : asdf
0 résultat dans 0 instrument de recherche



[Site Internet www.defense.gouv.fr](#)
[Site internet du service historique de la Défense](#)

→→ [Accueil](#) / Ressources et publications / Consulter en ligne

[Consulter en ligne - Accueil](#)

- Recherche simple :
  - Lancer la recherche
- [Recherche avancée](#)
- [Toutes les ressources](#)
- [Fonds d'archives](#)
- [Collections des bibliothèques](#)

[Site internet du Secrétariat général pour l'administration](#)

Résultats de recherche

Votre requête : Texte intégral : asdf

0 résultat dans 0 instrument de recherche

NE PAS FAIRE CONFIANCE

- http://site.com/chemin/fichier.php/<XSS>?yo
  - Apache : /chemin/fichier.php
  - PHP : /chemin/fichier.php/<XSS>
- Valable pour PHP_SELF, HTTP_*, HTTP_REFERER, etc.
- Toujours valider et protéger
  les données $_SERVER avant de les utiliser

INJECTION PAR GIF

- Prenez une image GIF, ajoutez phpinfo()
- Envoyez la sur le site
- Si tous les fichiers sont traités par PHP...

ATTENTION AUX UPLOADS

- Stockez les fichiers hors Web, avec VOS noms et extensions
  - Stockez les noms de fichiers en base
  - Protégez-les noms de fichiers
- Attention à la modération!
- Double attention aux fichiers PHP

afup

Alter Way

consulting

- DAMIEN.SEGUY@ALTERWAY.FR