SÉCURITÉ DES SERVEURS ET DES APPLICATIONS

Conseils de paramétrage Apache/PHP

M. Contensin

02/04/2015

7ème journée du réseau ARAMIS – Lyon

Introduction

Collecte : recherche d'informations pour cibler l'attaque

OS

Introduction

Collecte : recherche d'informations pour cibler l'attaque

GWS

Apache HTTP SERVER PROJECT

node

IIS

NGINX

serveur HTTP

ubuntu

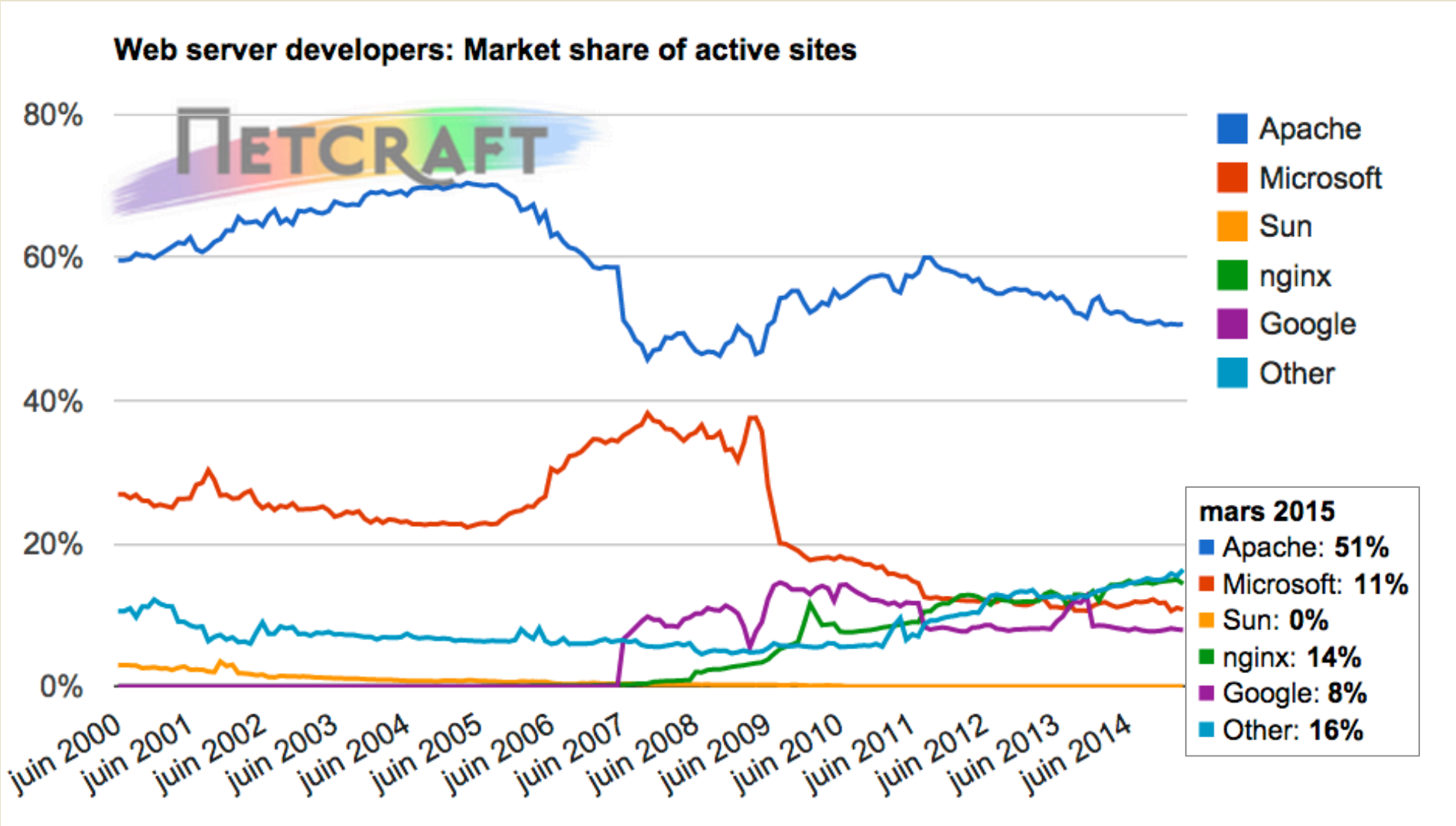
debian

CentOS

Microsoft

OS

Introduction



http://news.netcraft.com/archives/2015/03/19/march-2015-web-server-survey.html

Introduction

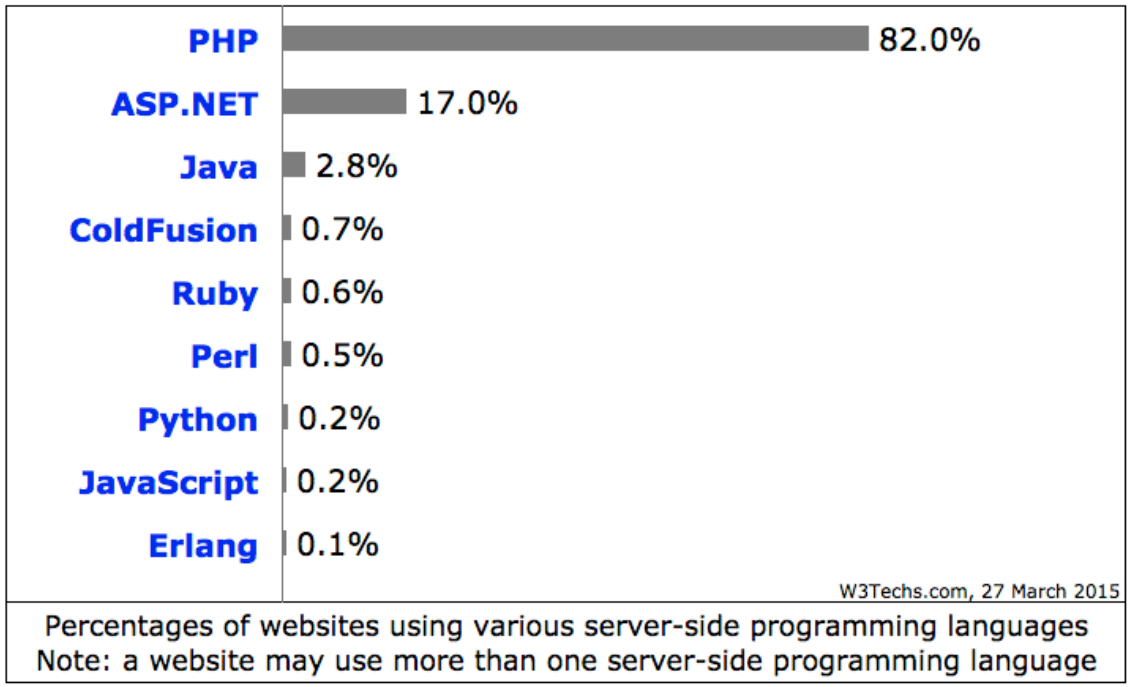
Collecte : recherche d'informations pour cibler l'attaque

Introduction

Usage of server-side programming languages for websites

This diagram shows the percentages of websites using various server-side programming languages. See technologies overview for explanations on the methodologies used in the surveys. Our reports are updated daily.

How to read the diagram:
PHP is used by 82.0% of all the websites whose server-side programming language we know.

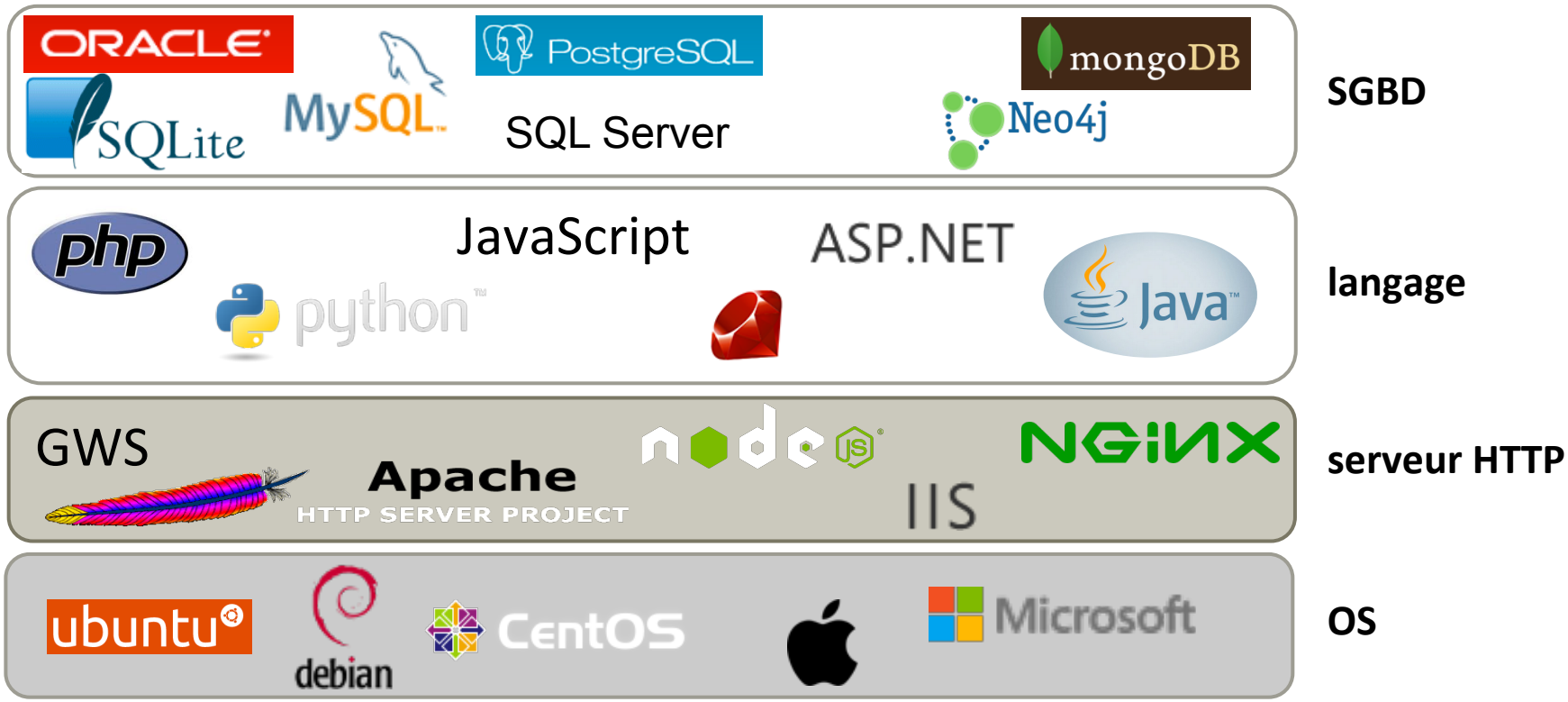


Percentages of websites using various server-side programming languages
Note: a website may use more than one server-side programming language

Source : http://w3techs.com/technologies/overview/programming_language/all

Introduction

Collecte : recherche d'informations pour cibler l'attaque



Introduction

Collecte : recherche d'informations pour cibler l'attaque

Application + points d'entrée

SGBD

langage

serveur HTTP

OS

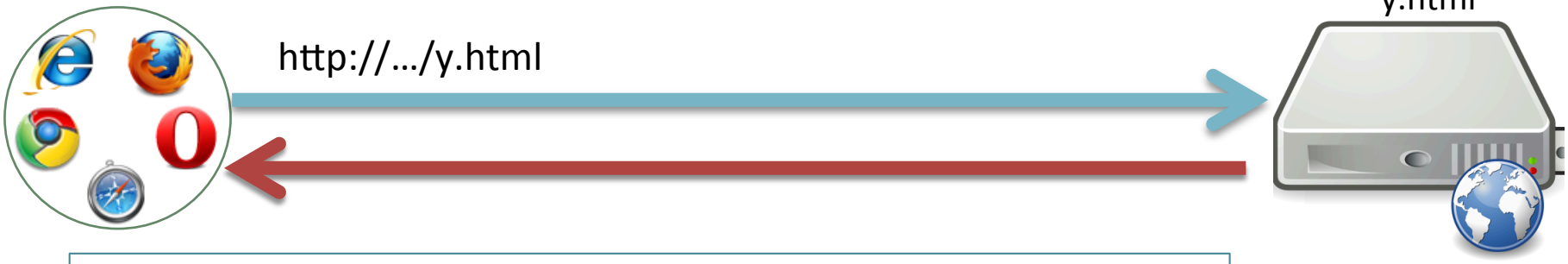
Introduction

Plan

1. Limiter les informations sur Apache
2. Limiter les informations sur le langage
3. Masquer les fichiers sensibles
4. Interdire la surcharge de configuration
5. Protéger les sessions
6. Champs d'en-tête HTTP de sécurité

1. Limiter les informations sur Apache

- Signature : page d'erreur, listing de répertoire



Not Found

The requested URL /y.html was not found on this server.

Apache/2.4.12 (Unix) OpenSSL/1.0.1j PHP/5.6.6 Server at www.monsite.fr Port 80

ServerSignature

On

Not Found

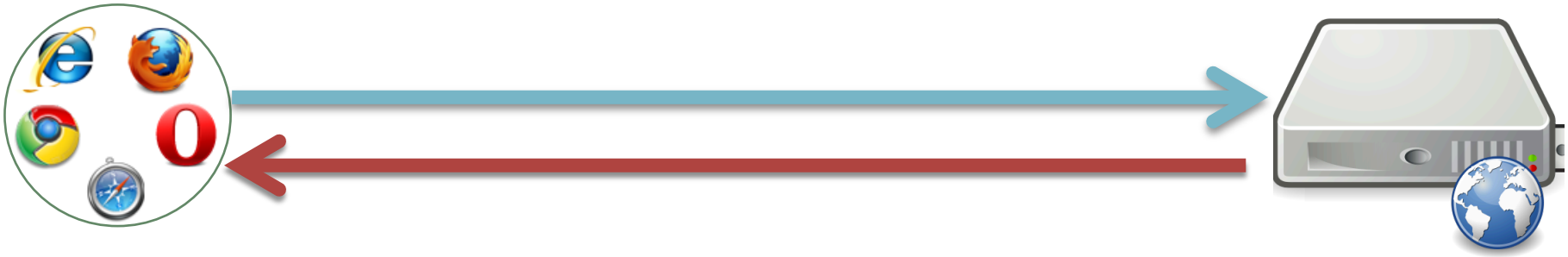
The requested URL /y.html was not found on this server.

Off

(défaut)

1. Limiter les informations sur Apache

- En-tête de la réponse HTTP : champ `Server`



HTTP/1.1 200 OK
Date: Fri, 27 Feb 2015 20:40:02 GMT
Server: Apache/2.4.12 (Unix) PHP/5.6.6 Python/2.7.9 OpenSSL/1.0.1j
Content-Length: 1289
Content-Type: text/html;charset=UTF-8

HTTP/1.1 200 OK
Date: Fri, 27 Feb 2015 20:42:17 GMT
Server: Apache
Content-Length: 1289
Content-Type: text/html;charset=UTF-8

ServerTokens

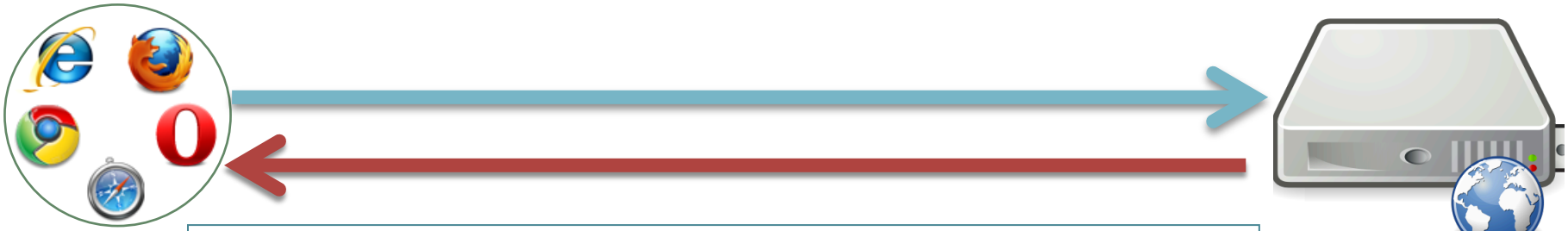
Full

(défaut)

Prod

1. Limiter les informations sur Apache

- En-tête de la réponse HTTP : modifier les champs



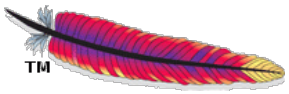
HTTP/1.1 200 OK
Date: Fri, 27 Feb 2015 21:03:41 GMT
Server: Apache
X-Powered-By: PHP/5.6.6
Composed-By: SPIP 2.1.23 @ www.spip.net + images(1.0.1), porte_plume(1.7.9), safehtml(1.3.7), vertebres(1.0.0)
…

LoadModule **headers_module** modules/mod_headers.so

```
<IfModule headers_module>
    Header set Author "MCKP"
    Header unset X-Powered-By
    Header unset Composed-By
</IfModule>
```

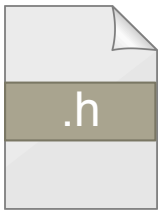
HTTP/1.1 200 OK
Date: Fri, 27 Feb 2015 21:09:34 GMT
Server: Apache
Author: MCKP
…

1. Limiter les informations sur Apache



- Modifier le nom et la version du serveur
  - Modifier les Sources (Apache 2.x)

```
#define AP_SERVER_BASEVENDOR "Apache Software Foundation"
#define AP_SERVER_BASEPRODUCT "Apache"
#define AP_SERVER_MAJORVERSION_NUMBER 2
#define AP_SERVER_MINORVERSION_NUMBER 4
#define AP_SERVER_PATCHLEVEL_NUMBER   12
```



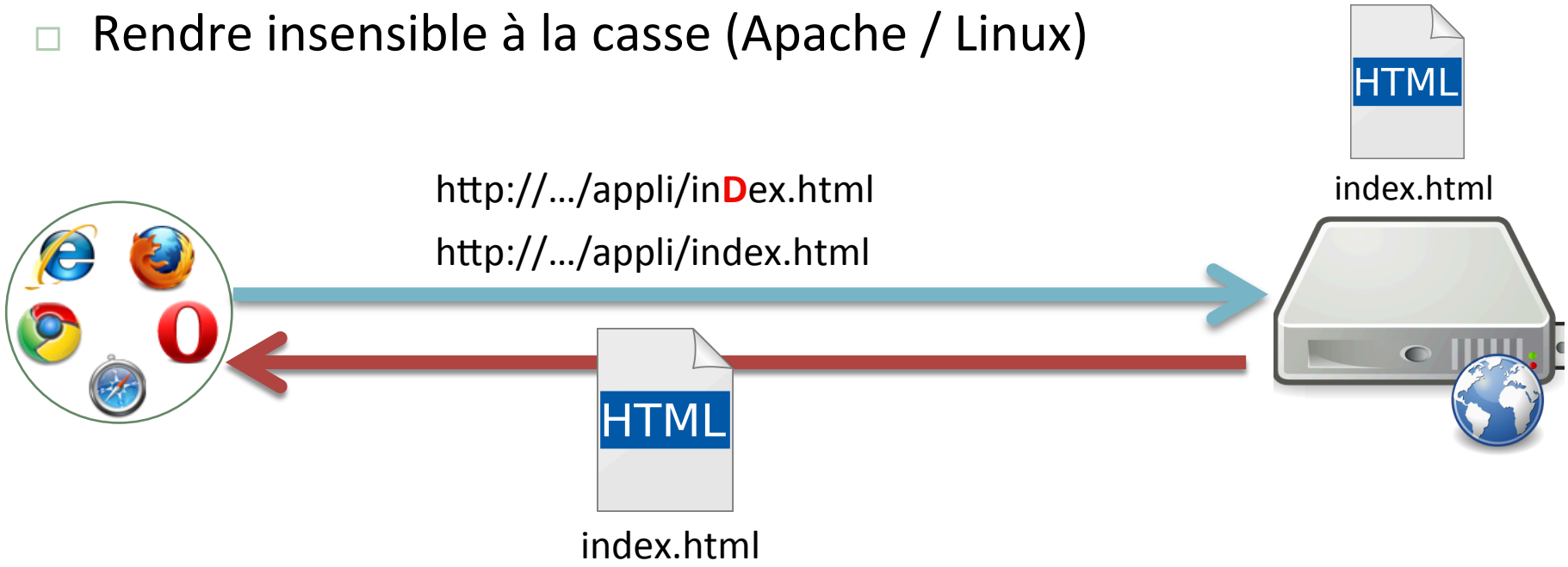
ap_release.h

  - Utiliser mod_security

```
SecServerSignature "Unknown Server"
```

1. Limiter les informations sur Apache

- Rendre insensible à la casse (Apache / Linux)

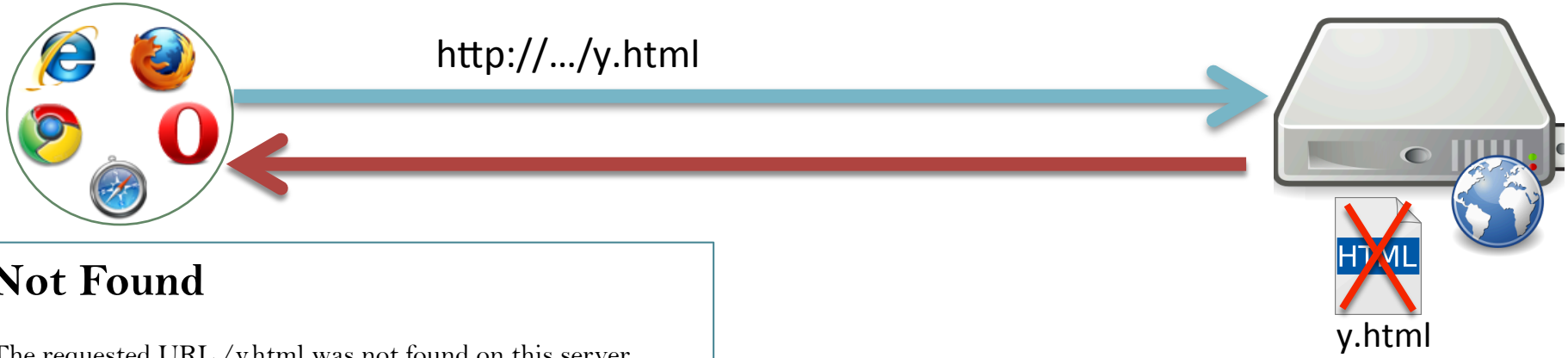


LoadModule speling_module modules/mod_speling.so

```
<Directory /appli>
   CheckSpelling    On
   CheckCaseOnly  On
</Directory>
```

1. Limiter les informations sur Apache

- Personnaliser les pages d'erreurs (HTTP 400 à 417 et 500 à 505)



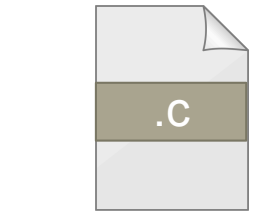
Not Found

The requested URL /y.html was not found on this server.

file not found!

ErrorDocument 404 "file not found!"
ErrorDocument 500 /error/serv_error.html

- Personnaliser les codes d'erreurs



http_protocol.c

```
#define LEVEL_400 39
    "400 Bad Request",
    "401 Unauthorized",
    "402 Payment Required",
    "403 Forbidden",
    "404 Not Found",
    "405 Method Not Allowed",
    "406 Not Acceptable",
    "407 Proxy Authentication Required",
    "408 Request Timeout",
    "409 Conflict",
    "410 Gone",
```

2. Limiter les informations sur le langage

- Configurer tout ce qui pourrait donner indirectement de l'information sur le langage utilisé
  - extension (.jsp, .asp, .php)
  - cookie de session (PHPSESSID, JSESSIONID, ASPSESSIONID)
  - messages d'erreurs
  - informations données par PHP

Dans certains cas masquer le langage est inutile

- briques logicielles spécifiques
- distribution d'application web avec infos sur la configuration requise
- le pirate a un compte sur le serveur

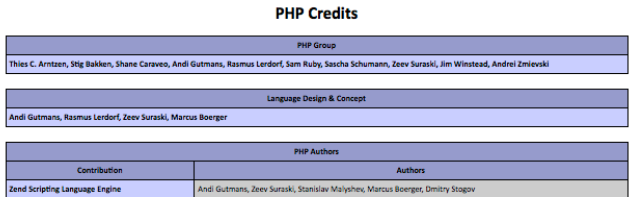
2. Limiter les informations sur le langage

- Informations données par PHP
  - Réponse HTTP

```
HTTP/1.1 200 OK
Date: Fri, 27 Feb 2015 23:16:41 GMT
Server: Apache
X-Powered-By: PHP/5.3.3
...
```

→ **expose_php = Off**

  - Crédits ?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000 PHP < 5.5



PHP Credits

PHP Group
Thies C. Arntzen, Stig Bakken, Shane Caraveo, Andi Gutmans, Rasmus Lerdorf, Sam Ruby, Sascha Schumann, Zeev Suraski, Jim Winstead, Andrei Zmievski

Language Design & Concept
Andi Gutmans, Rasmus Lerdorf, Zeev Suraski, Marcus Boerger

PHP Authors	
Contribution	Authors
Zend Scripting Language Engine	Andi Gutmans, Zeev Suraski, Stanislav Malyshev, Marcus Boerger, Dmitry Stogov

  - Images PHP < 5.5

?=PHPE9568F34-D428-11d2-A769-00AA001ACF42
?=PHPE9568F35-D428-11d2-A769-00AA001ACF42
?=PHPE9568F36-D428-11d2-A769-00AA001ACF42

2. Limiter les informations sur le langage

- Informations données par PHP

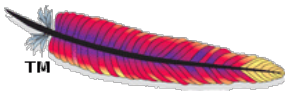
```
<?php
   phpinfo();
```

PHP Version 5.6.6RC1

System	Darwin macmag 11.4.2 Darwin Kernel Version 11.4.2: Thu Aug 23 16:25:48 PDT 2012; root:xnu-1699.32.7~1/RELEASE_X86_64 x86_64
Build Date	Feb 27 2010 12:28:52
Configure Command	'./configure' '--prefix=/Applications/XAMPP/xamppfiles' '--program-suffix=-5.3.1' '--libdir=/Applications/XAMPP/xamppfiles/lib/php/php-5.3.1' '--includedir=/Applications/XAMPP/xamppfiles/include/php/php-5.3.1' '--with-apxs2=/Applications/XAMPP/xamppfiles/bin/apxs' '--with-config-file-path=/Applications/XAMPP/xamppfiles/etc' '--with-mysql=/Applications/XAMPP/xamppfiles' '--disable-debug' '--enable-cli' '--enable-cgi' '--enable-bcmath' '--enable-calendar' '--enable-ctype' '--enable-discard-path' '--enable-filepro' '--enable-filter' '--enable-force-cgi-redirect' '--enable-fastcgi' '--enable-ftp' '--enable-hash' '--enable-ipv6' '--enable-json' '--enable-odbc' '--enable-path-info-check' '--enable-gd-imgstrttf' '--enable-gd-native-ttf' '--with-ttf' '--enable-magic-quotes' '--enable-memory-limit' '--enable-safe-mode' '--enable-shmop' '--enable-sysvsem' '--enable-sysvshm' '--enable-track-vars' '--enable-trans-sid' '--enable-reflection' '--enable-session' '--enable-spl' '--enable-tokenizer' '--enable-wddx' '--enable-yp' '--enable-xmlreader' '--enable-xmlwriter' '--enable-zlib' '--enable-zts' '--with-simplexml' '--with-iconv' '--with-libxml' '--with-wddx' '--with-xml' '--with-ftp' '--with-ncurses=/Applications/XAMPP/xamppfiles' '--with-gdbm=/Applications/XAMPP/xamppfiles' '--with-jpeg-dir=/Applications/XAMPP/xamppfiles' '--with-png-dir=/Applications/XAMPP/xamppfiles' '--with-freetype-dir=/Applications/XAMPP/xamppfiles' '--without-xpm' '--with-zlib=shared' '--with-zlib-dir=/Applications/XAMPP/xamppfiles' '--with-openssl=/Applications/XAMPP/xamppfiles' '--with-expat-dir=/Applications/XAMPP/xamppfiles' '--enable-xslt=shared,/Applications/XAMPP/xamppfiles' '--with-xsl=shared,/Applications/XAMPP/xamppfiles' '--with-dom=shared,/Applications/XAMPP/xamppfiles' '--with-ldap=shared,/Applications/XAMPP/xamppfiles' '--with-gd=shared' '--with-mysql-sock=/Applications/XAMPP/xamppfiles/var/mysql/mysql.sock' '--with-mcrypt=/Applications/XAMPP/xamppfiles' '--with-mhash=/Applications/XAMPP/xamppfiles' '--enable-sockets' '--enable-zend-multibyte' '--with-libxml-dir=/Applications/XAMPP/xamppfiles' '--enable-pcntl' '--enable-dbx=shared' '--with-mysqli=shared,/Applications/XAMPP/xamppfiles/bin/mysql_config' '--with-pear=/Applications/XAMPP/xamppfiles/lib/php/pear' '--with-mssql=/Applications/XAMPP/xamppfiles' '--with-imap-dir=/Applications/XAMPP/xamppfiles' '--with-imap=shared,/Applications/XAMPP/xamppfiles' '--enable-mbstring=shared,all' '--with-pgsql=shared,/Applications/XAMPP/xamppfiles' '--with-gettext=/Applications/XAMPP/xamppfiles' '--enable-apache2-2filter=shared' '--enable-apache2-2handler=shared' '--with-bz2=shared' '--with-curl=shared' '--with-dba=shared' '--enable-dbase=shared' '--with-fdf=shared' '--enable-mbregex' '--enable-mbregex-backtrack' '--with-mime-magic=shared' '--with-mysql=shared,/Applications/XAMPP/xamppfiles' '--enable-shmop=shared' '--with-snmp=shared' '--enable-sockets=shared' '--enable-pdo' '--with-sqlite=shared' '--enable-zip=shared,/Applications/XAMPP/xamppfiles' '--enable-exif=shared' '--with-pdo-mssql=shared,/Applications/XAMPP/xamppfiles' '--with-pdo-mysql=shared,/Applications/XAMPP/xamppfiles/bin/mysql_config' '--with-pdo-pgsql=shared,/Applications/XAMPP/xamppfiles' '--with-pdo-sqlite=shared' '--with-pdo-sqlite-external=shared' '--enable-soap=shared' '--with-xmlrpc=shared' '--with-oracle=shared' '--with-pdf=shared' '--with-sqlite3=shared,/Applications/XAMPP/xamppfiles'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/Applications/XAMPP/xamppfiles/etc
Loaded Configuration File	/Applications/XAMPP/xamppfiles/etc/php.ini

disable_functions = "phpinfo, phpcredits, phpversion, php_uname"

2. Limiter les informations sur le langage



- Informations données par l'extension .php
  - Associer une autre extension

    AddType application/x-httpd-php .jsp .htm .html

  - Réécriture

    LoadModule rewrite_module modules/mod_rewrite.so

    RewriteEngine on

    RewriteRule (.+)\.html$ $1.php

  - Forcer le type (appliqué à tous les fichiers du répertoire, quel que soit leur type de média)

    ForceType application/x-httpd-php

2. Limiter les informations sur le langage

- Cookie de session

Name	Value	Domain	Path	Expires / Max-Age	Size	HTTP	Secure
▶ Request Cookies					52		
▼ Response Cookies					44		
PHPSESSID	ltmq9bhu4iveajgo743tl0its7		/	Session	44		

session.name = *sessionid*

Name	Value	Domain	Path	Expires / Max-Age	Size	HTTP	Secure
▶ Request Cookies					90		
▼ Response Cookies					44		
sessionid	o74acs8vqb6c2b6kusmql5...		/	Session	44		

2. Limiter les informations sur le langage

- Informations données par les erreurs
  - Exceptions : ne pas utiliser la méthode getMessage() en production

    SQLSTATE[28000] [1045] Access denied for user **'root'@'localhost'** (using password: YES)

  - Messages d'alerte et d'erreur

```
select * from theme_news where id=
Mysql Error:You have an error in your SQL syntax. Check the manual that corresponds to your MySQL server version for the right syntax to use near '' at line 1
```

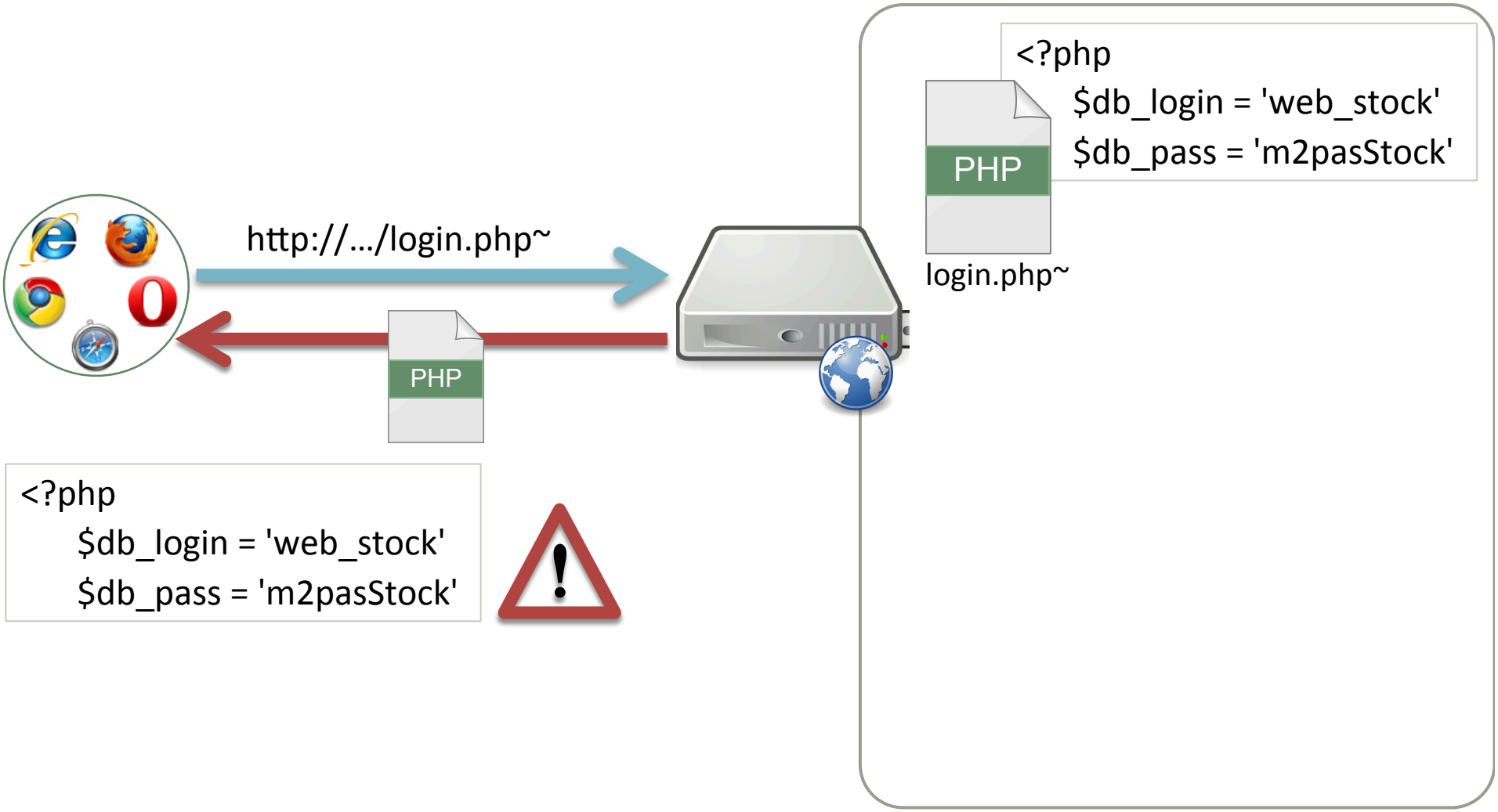
display_errors = Off

log_errors = On

error_log = *chemin_fichier_logs*

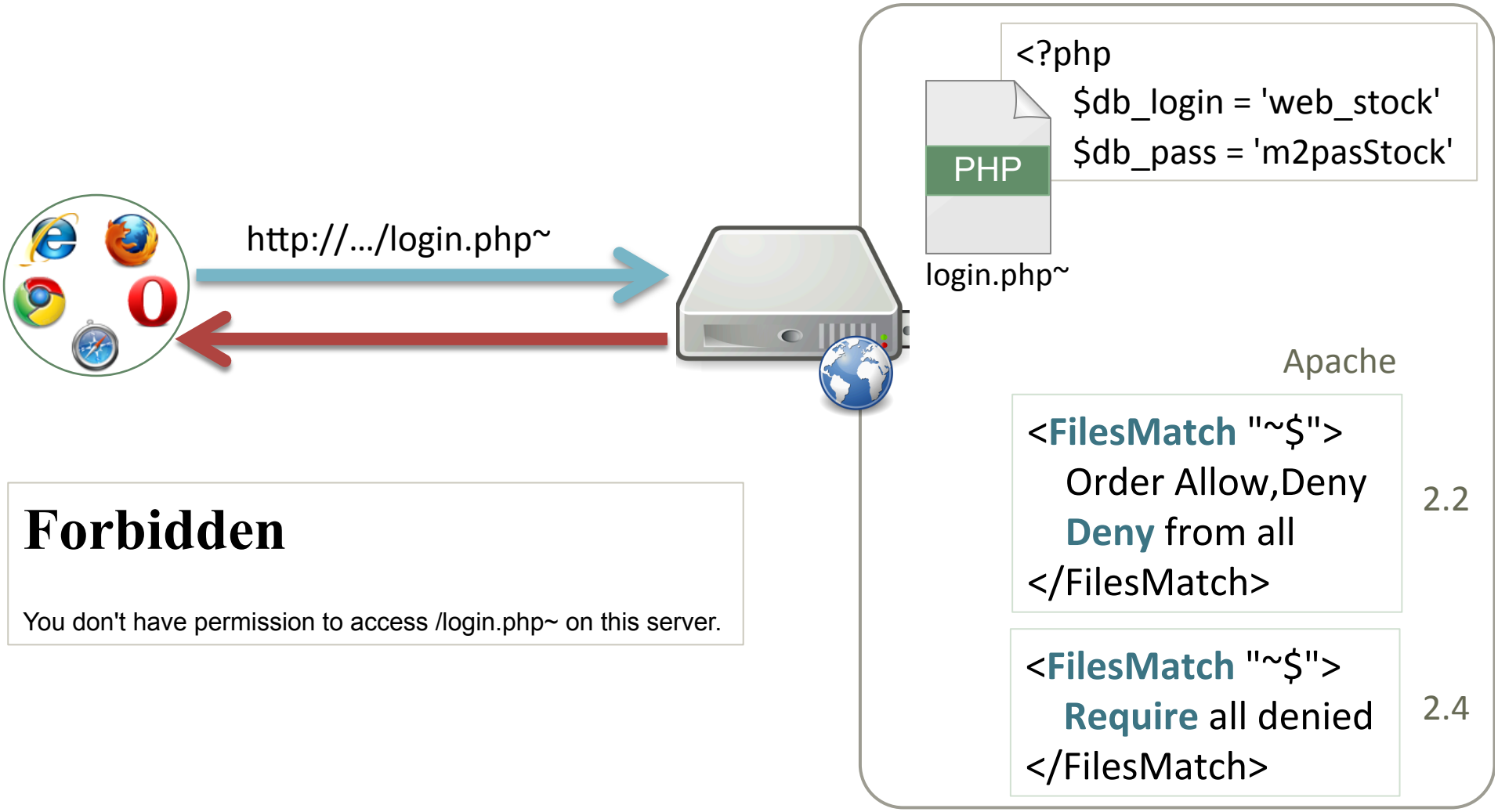
3. Masquer les fichiers sensibles

- Fichiers de sauvegardes (~, .old, .bak, .sav, …) et de configuration (.inc)



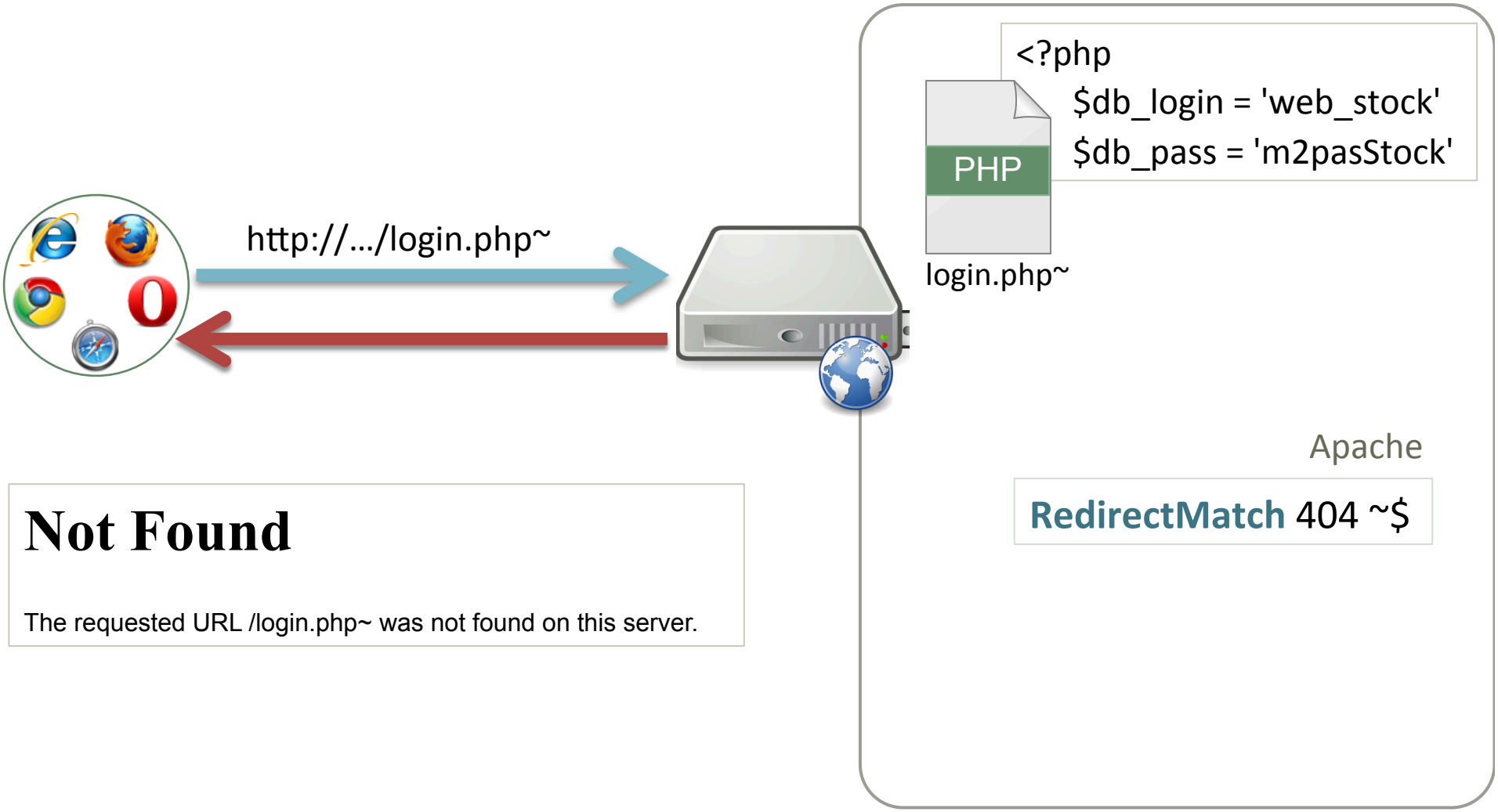
3. Masquer les fichiers sensibles

- Fichiers de sauvegardes (~, .old, .bak, .sav, …) et de configuration (.inc)



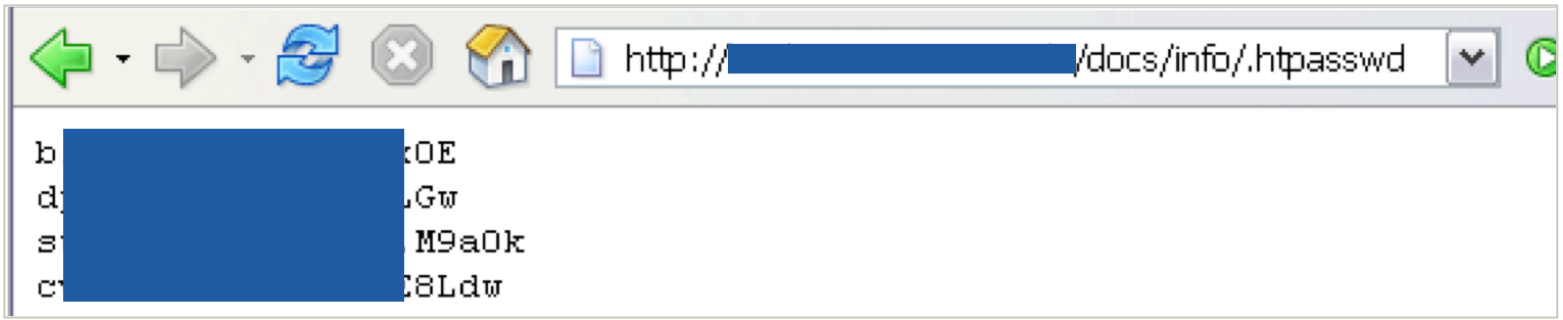
3. Masquer les fichiers sensibles

- Fichiers de sauvegardes (~, .old, .bak, .sav, …) et de configuration (.inc)



3. Masquer les fichiers sensibles

- Fichiers d'authentification



Forbidden

You don't have permission to access /.htaccess on this server.

```
<FilesMatch "^\.ht">
    Require all denied
</FilesMatch>
```

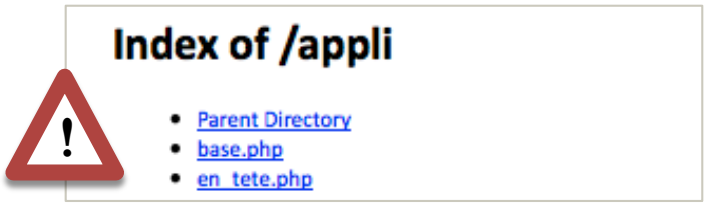
(défaut)

3. Masquer les fichiers sensibles

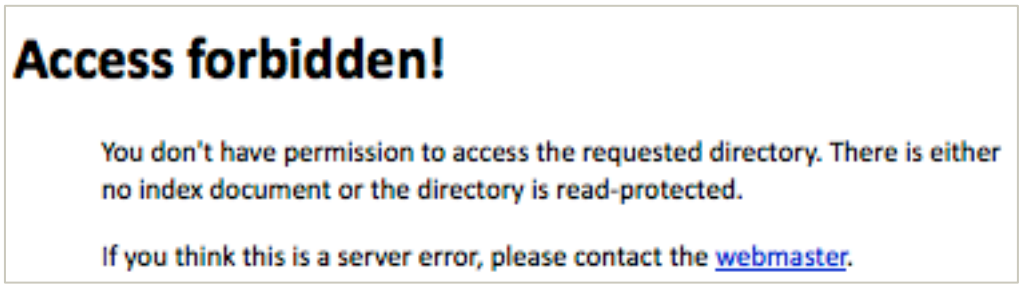
- Listing de répertoire

LoadModule autoindex_module modules/mod_autoindex.so

(défaut)



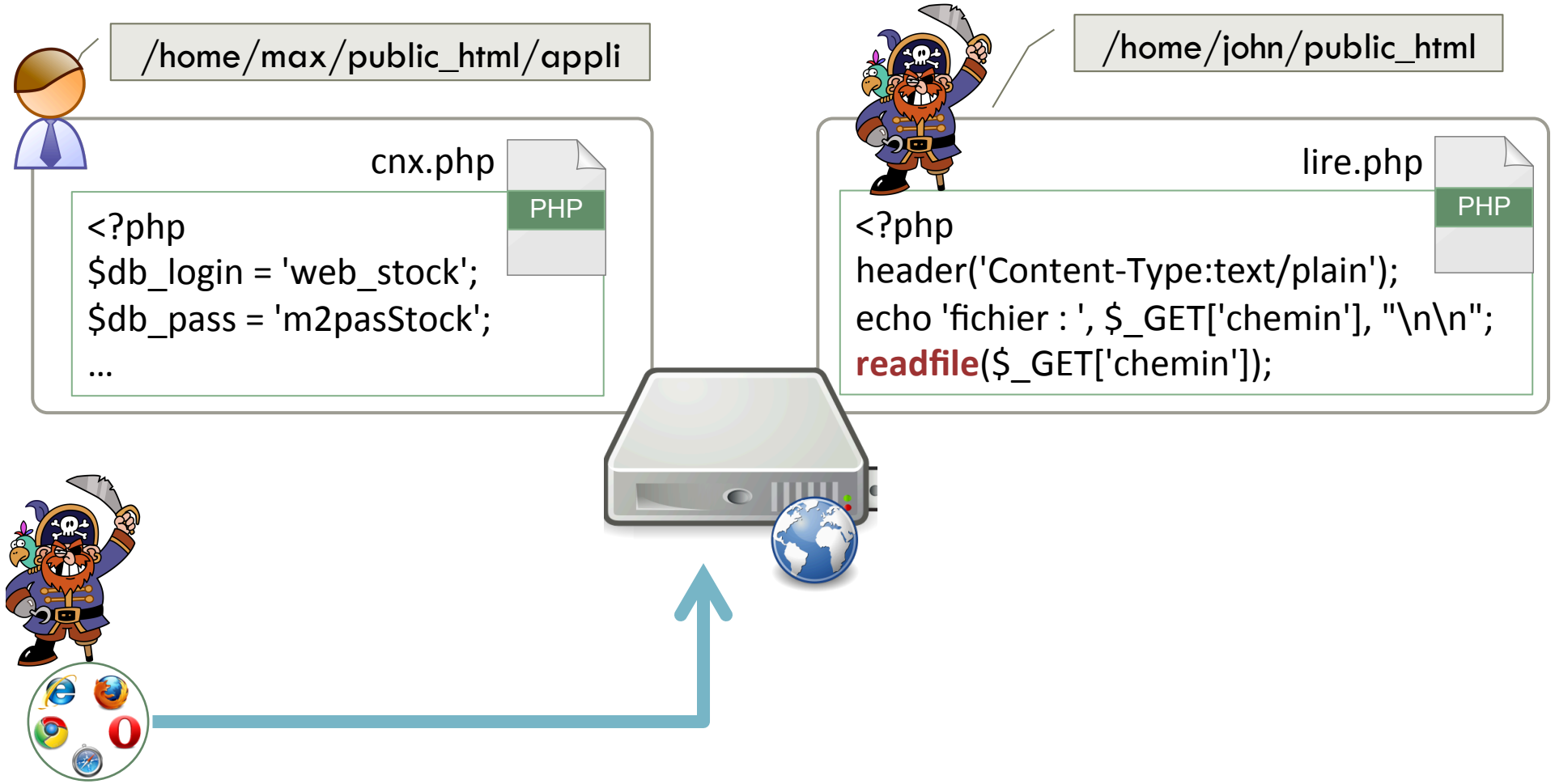

```
<Directory "…/appli">
        Options +Indexes
</Directory>
```




```
<Directory "…/appli">
        Options -Indexes
</Directory>
```

3. Masquer les fichiers sensibles

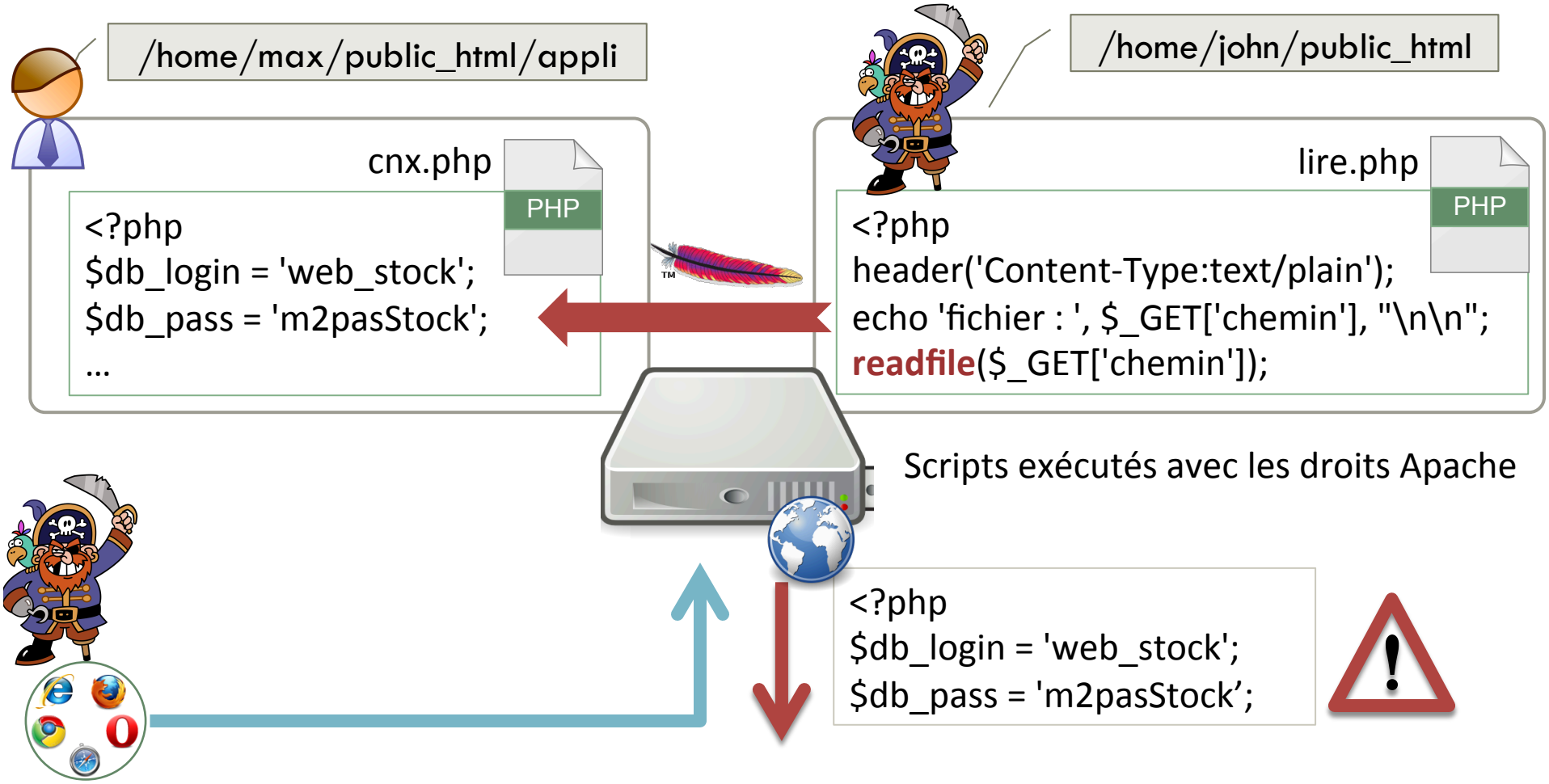
- Informations de connexion à la base de données (mod_php)



http://.../~john/lire.php?chemin=/home/max/public_html/appli/cnx.php

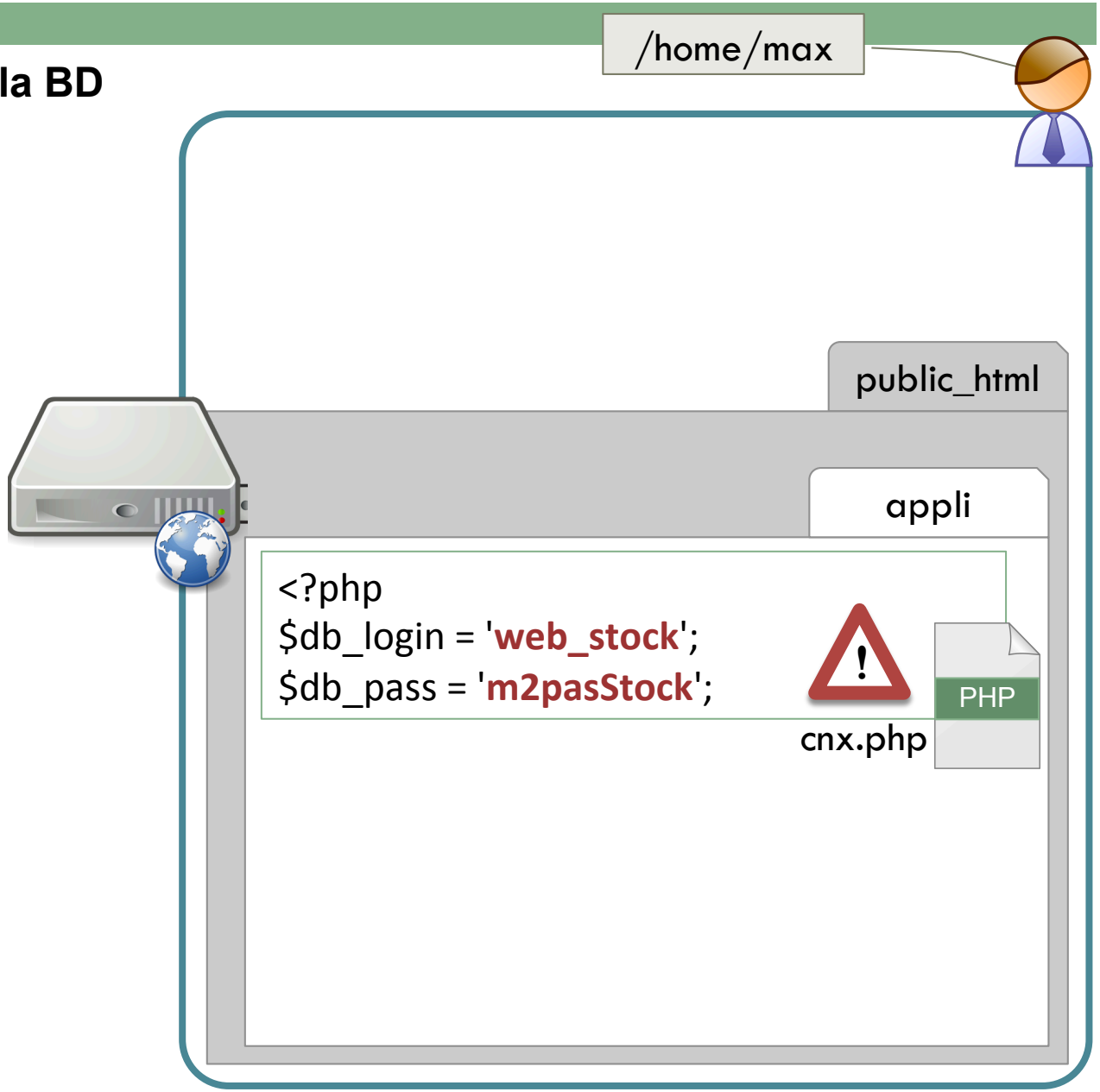
3. Masquer les fichiers sensibles

- Informations de connexion à la base de données (mod_php)



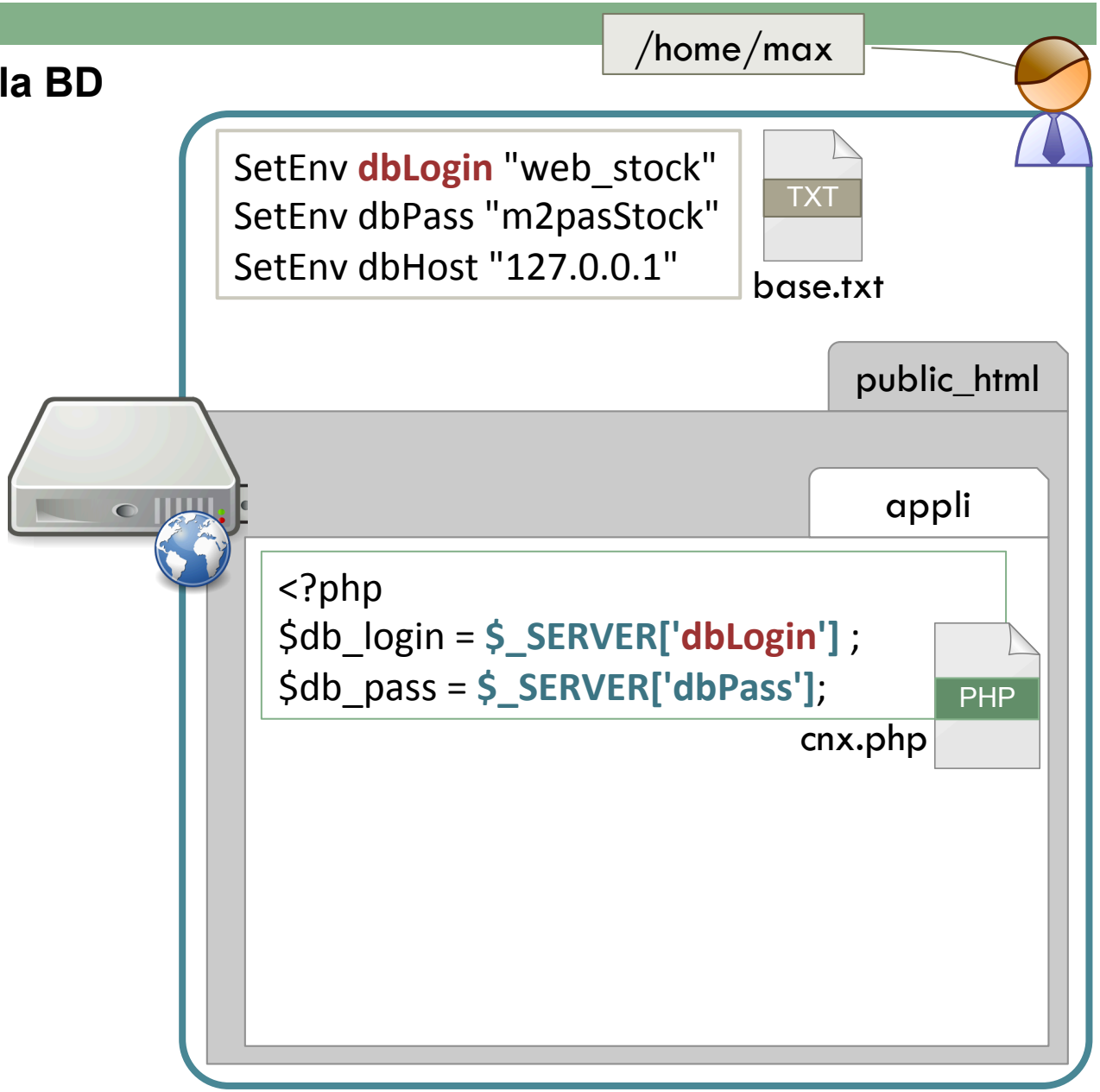
3. Masquer les fichiers sensibles

Protéger les identifiants de la BD



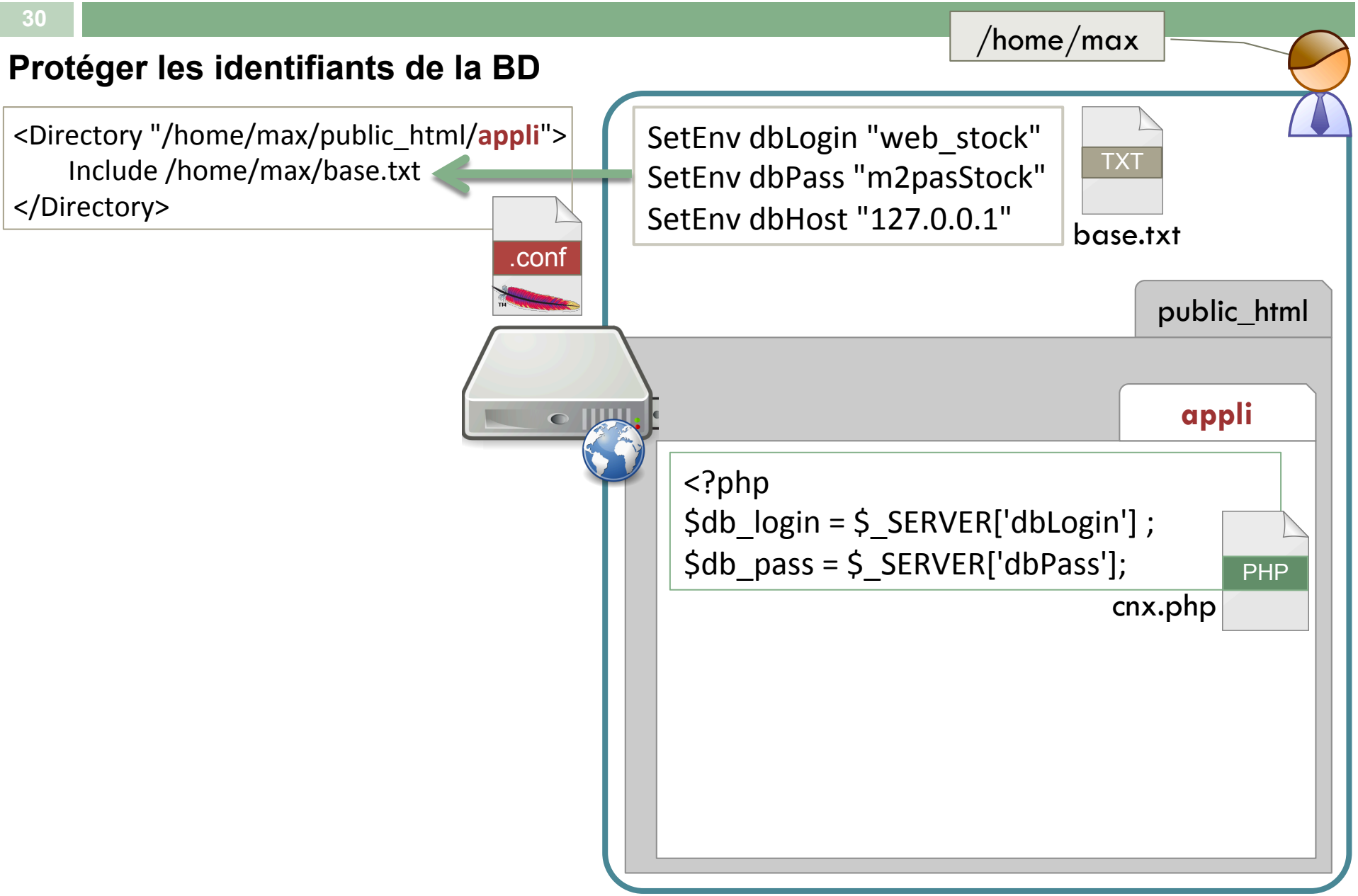
3. Masquer les fichiers sensibles

Protéger les identifiants de la BD



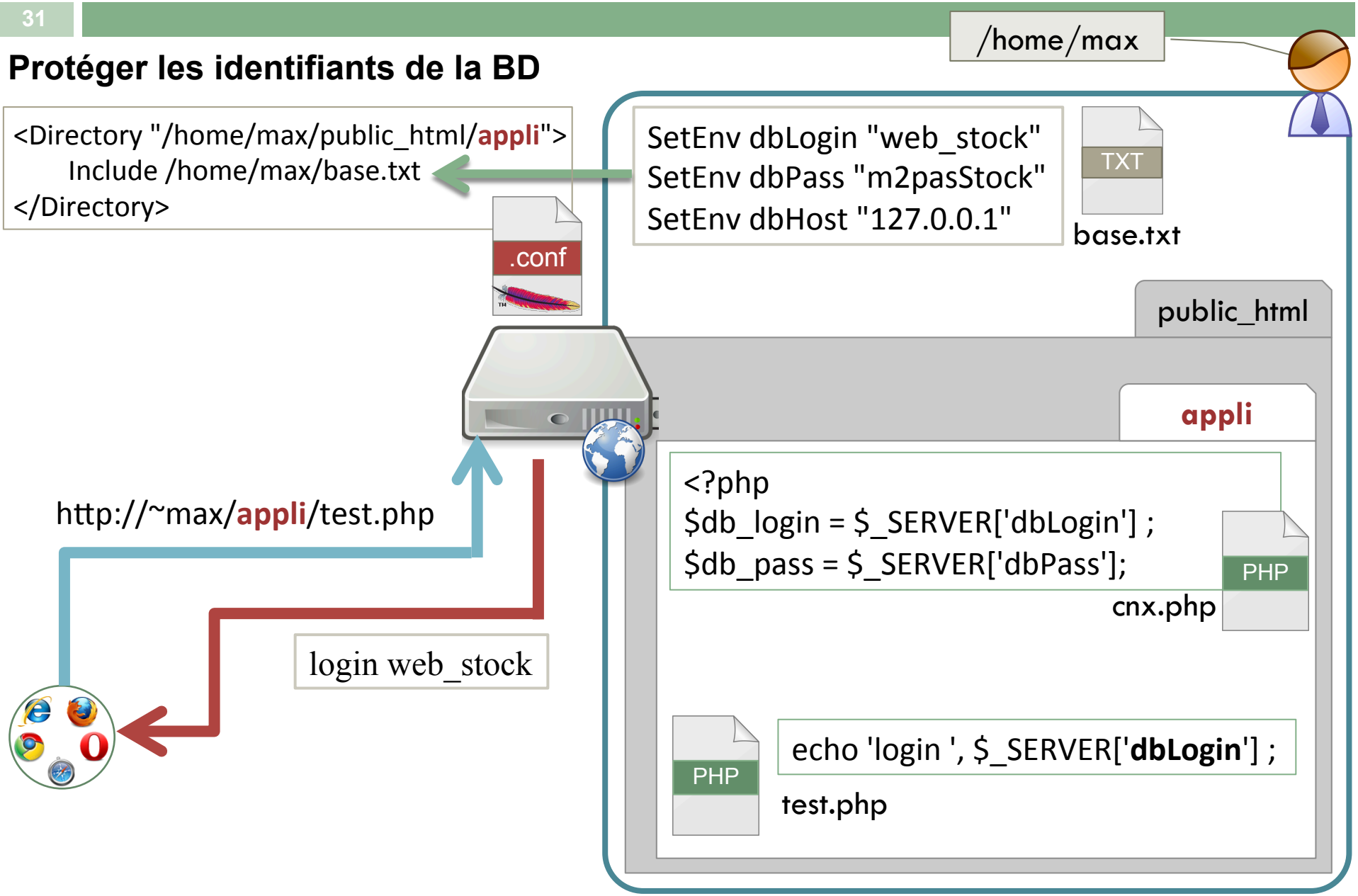
3. Masquer les fichiers sensibles

Protéger les identifiants de la BD



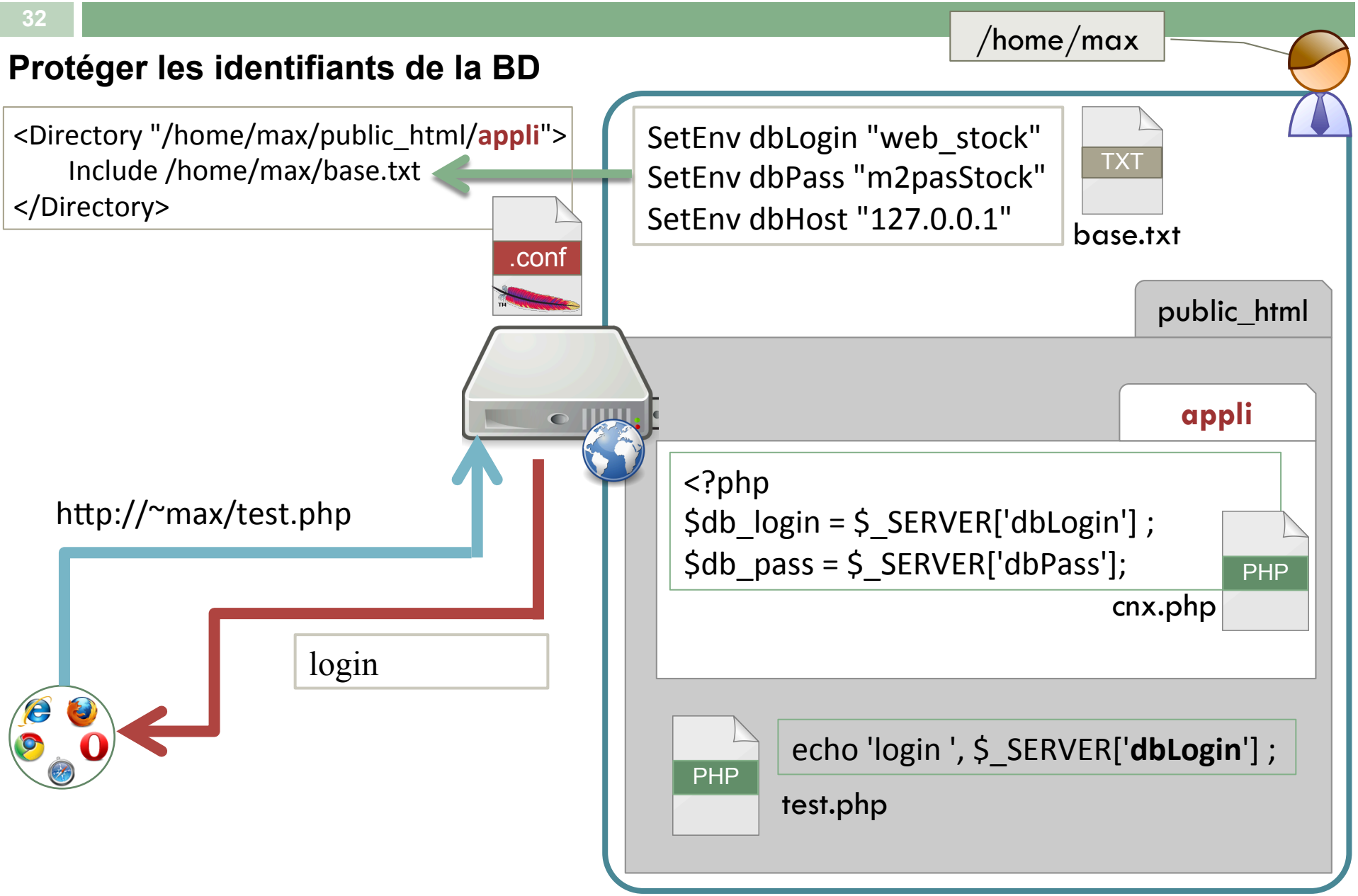
3. Masquer les fichiers sensibles

Protéger les identifiants de la BD



3. Masquer les fichiers sensibles

Protéger les identifiants de la BD



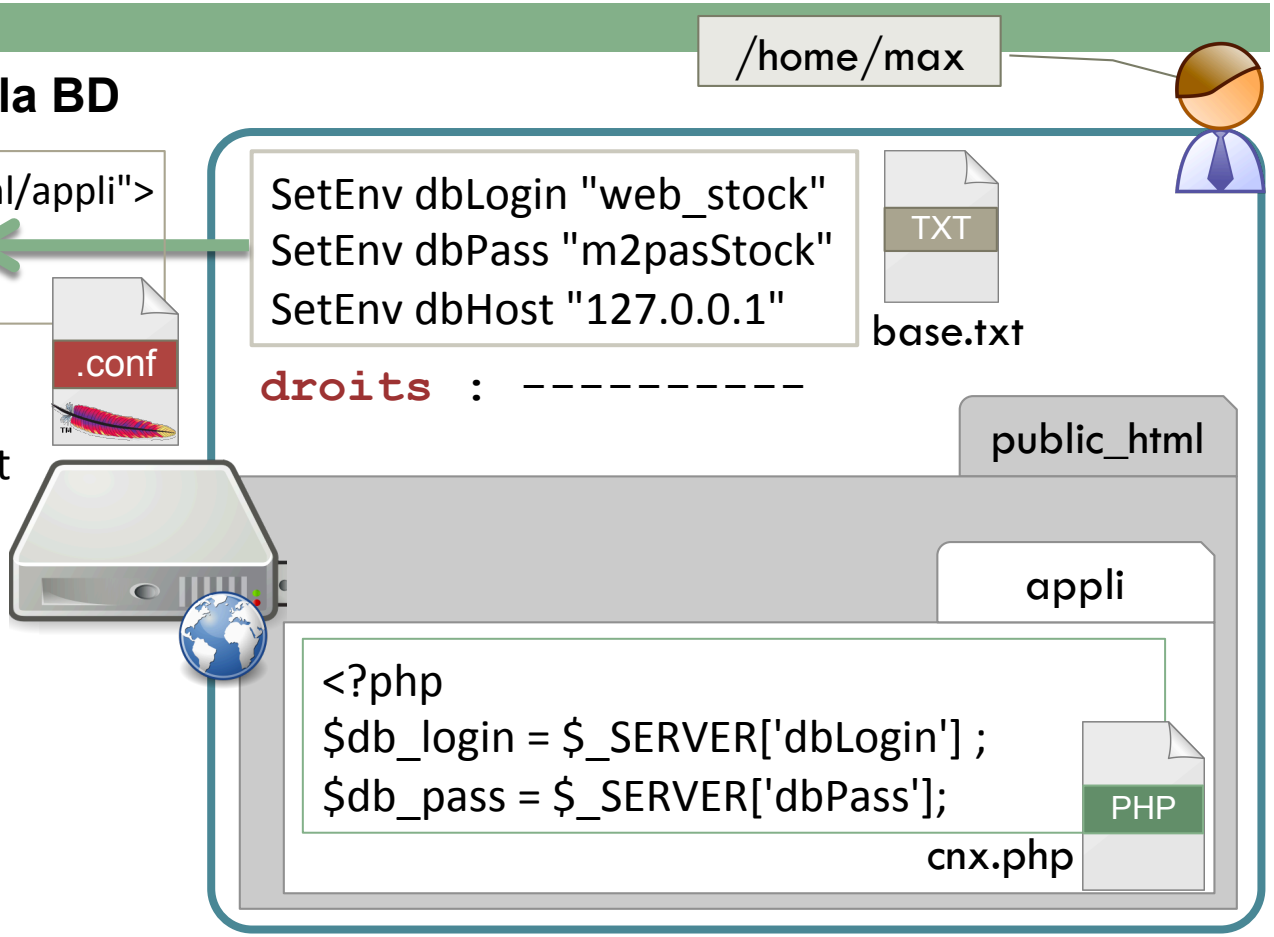
3. Masquer les fichiers sensibles

Protéger les identifiants de la BD

```
<Directory "/home/max/public_html/appli">
      Include /home/max/base.txt
</Directory>
```

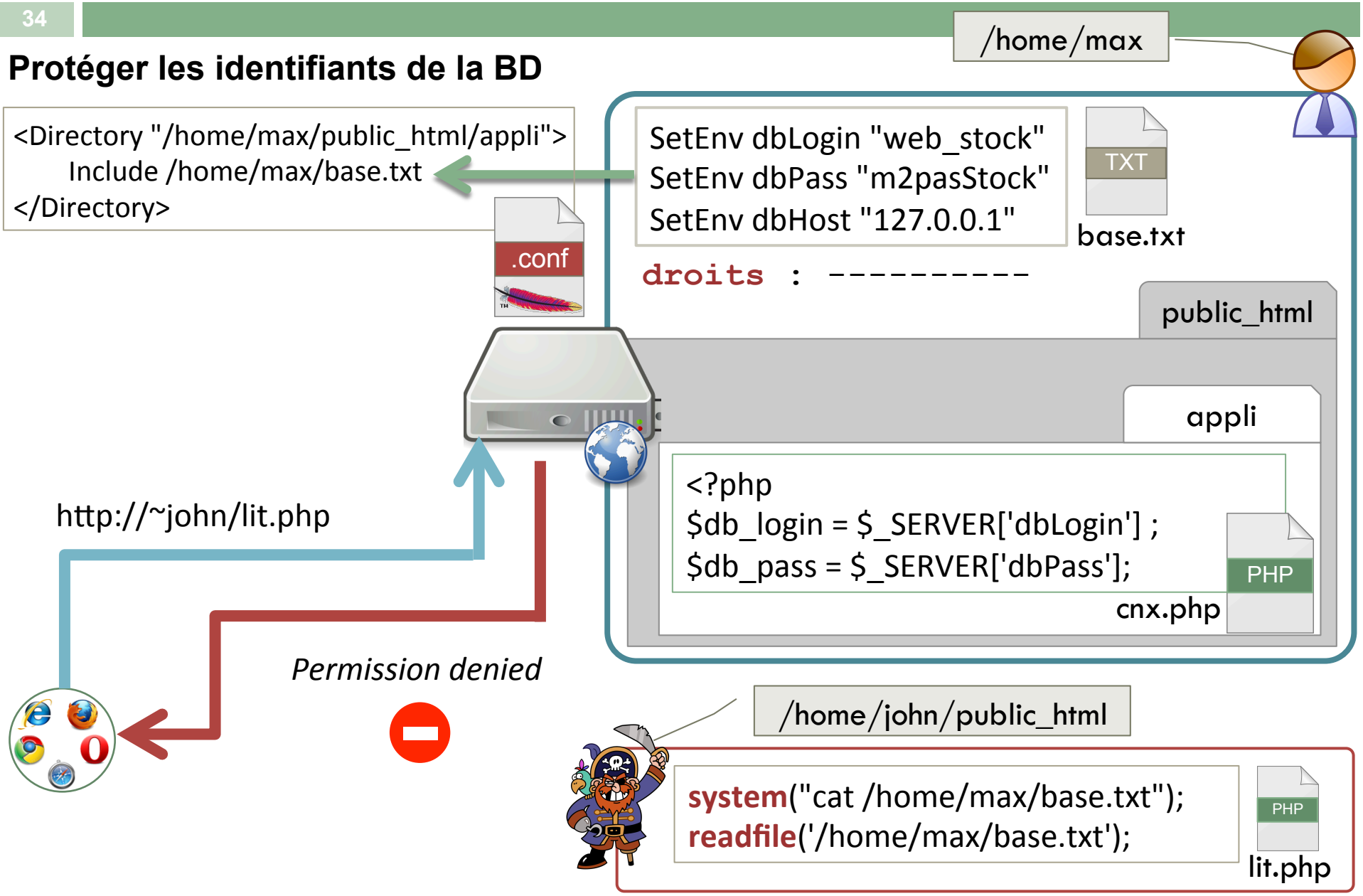
.conf

chmod 000 /home/max/base.txt



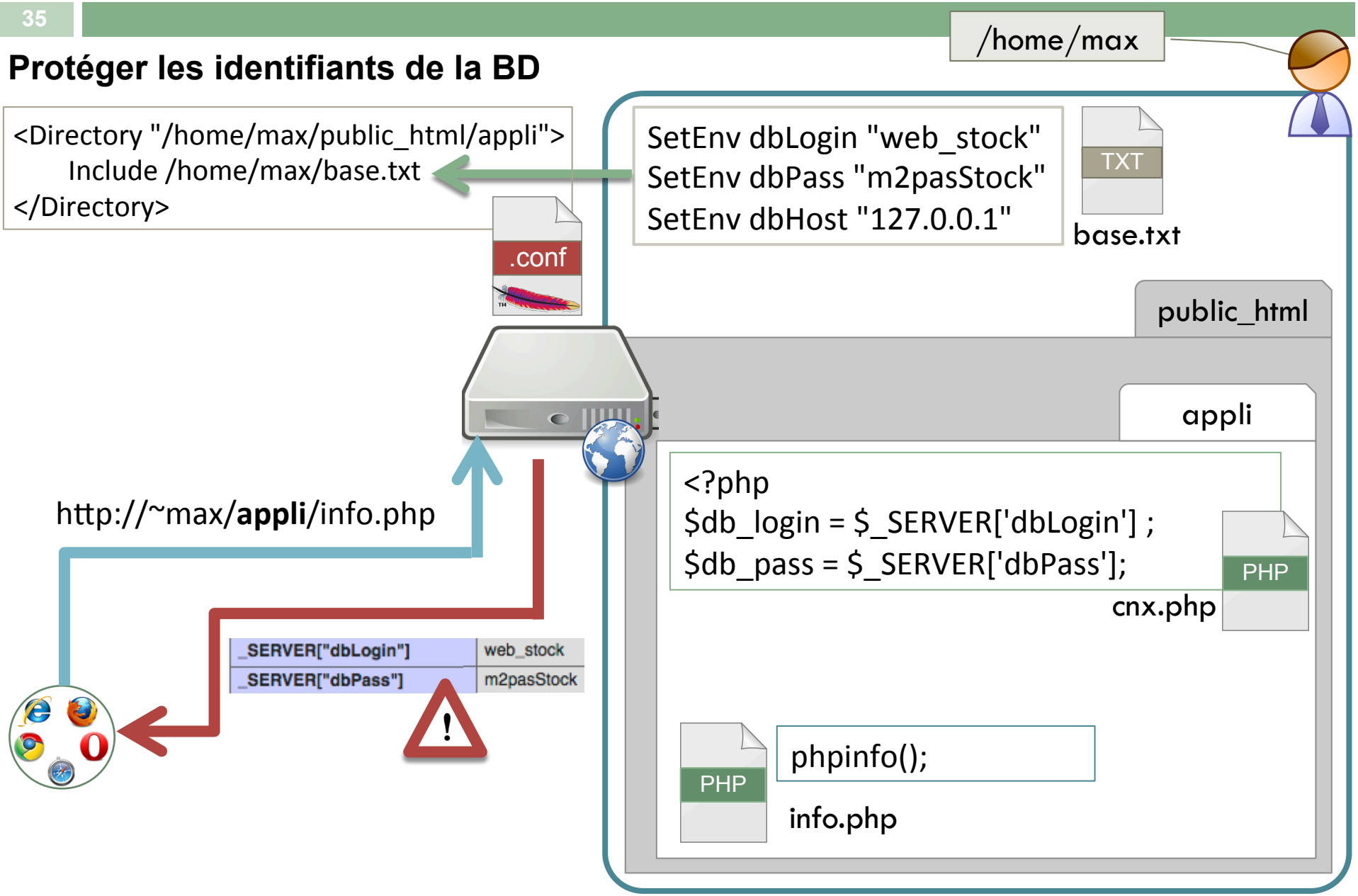
3. Masquer les fichiers sensibles

Protéger les identifiants de la BD



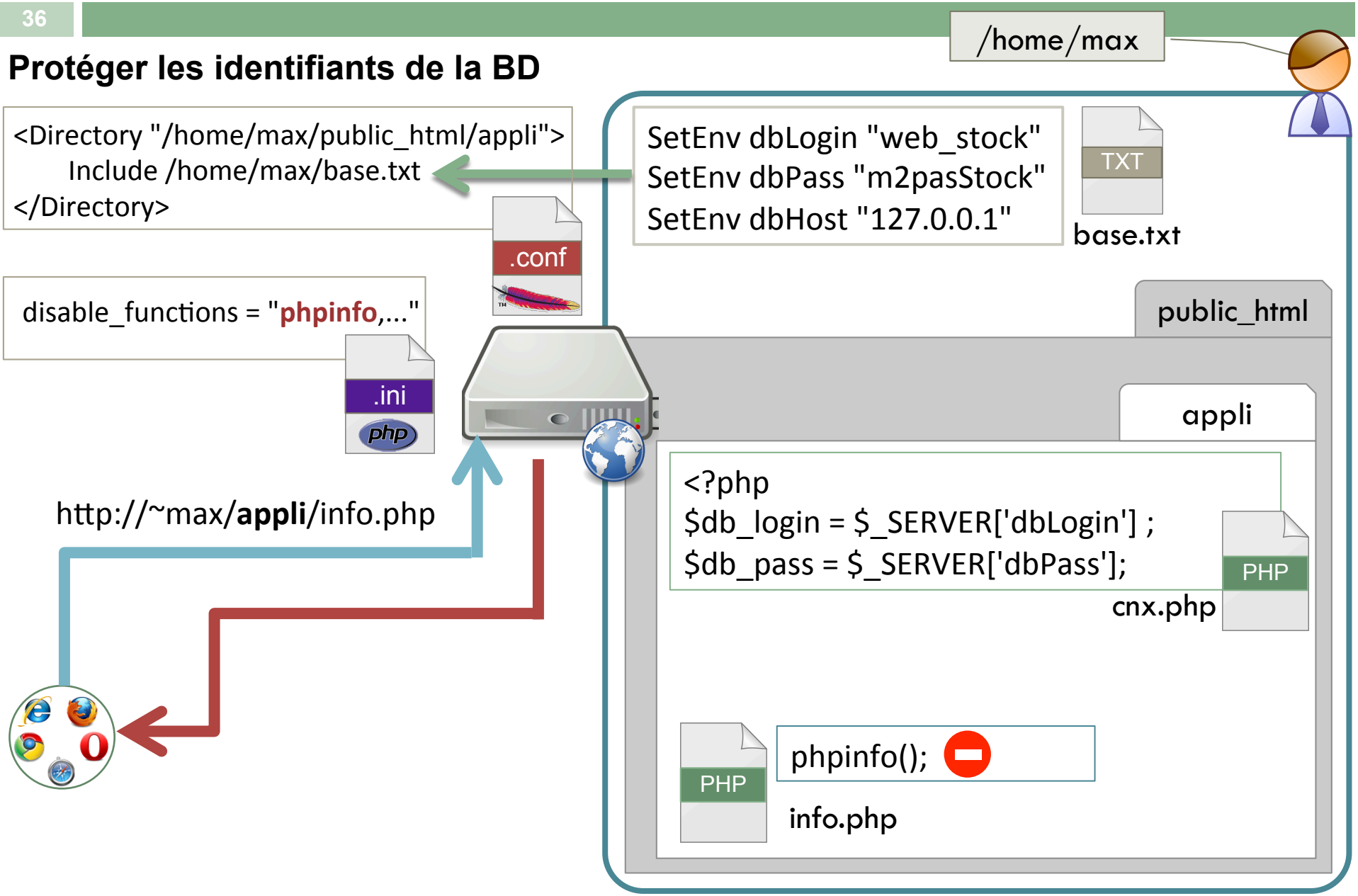
3. Masquer les fichiers sensibles

Protéger les identifiants de la BD

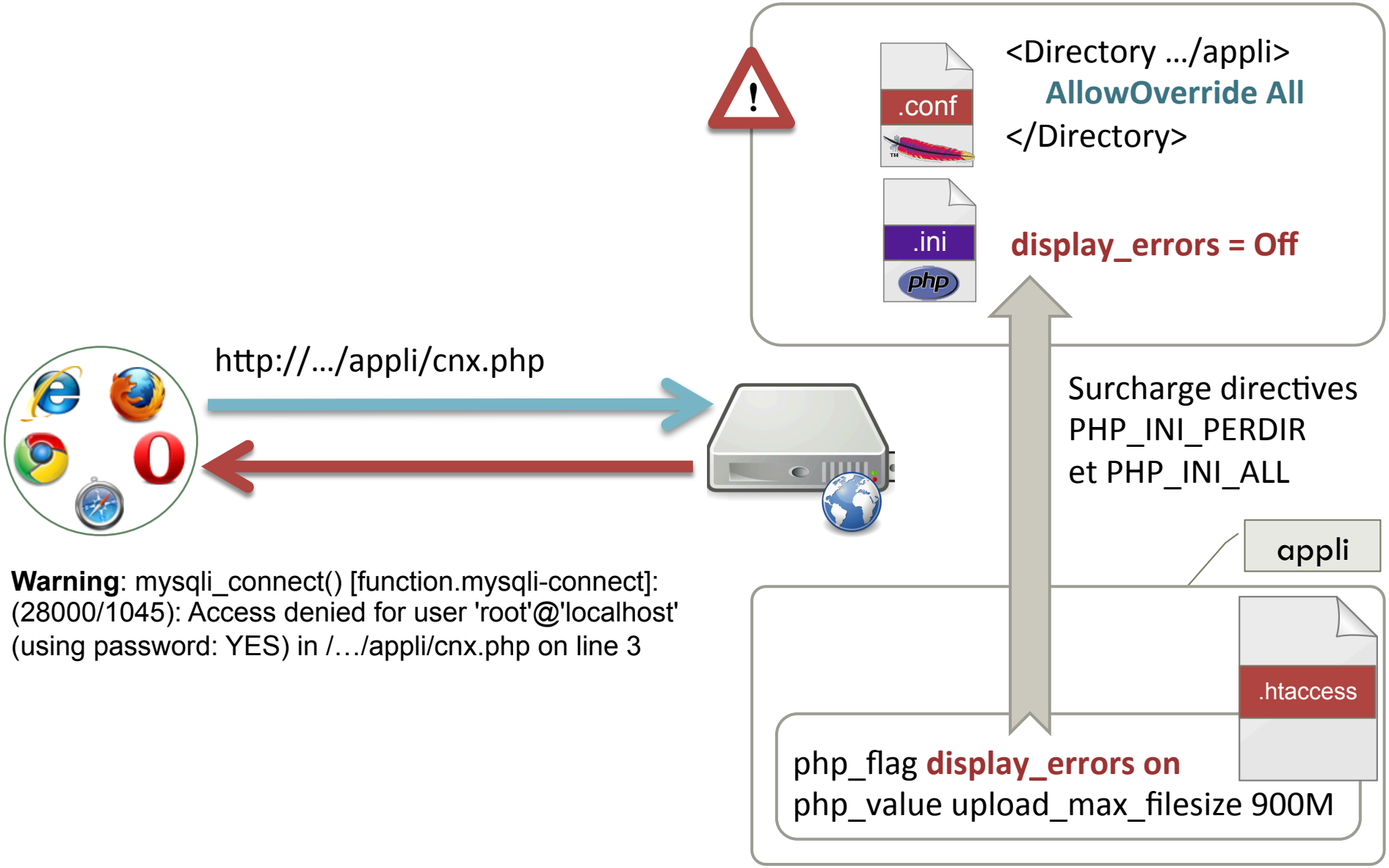


3. Masquer les fichiers sensibles

Protéger les identifiants de la BD

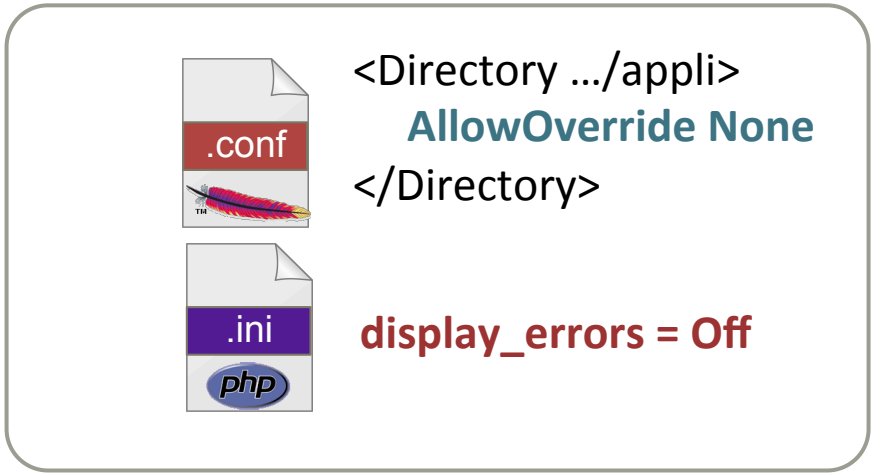


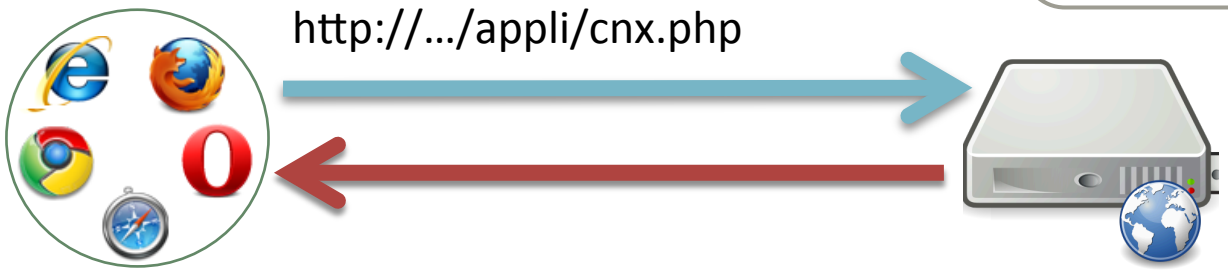
4. Interdire la surcharge de configuration



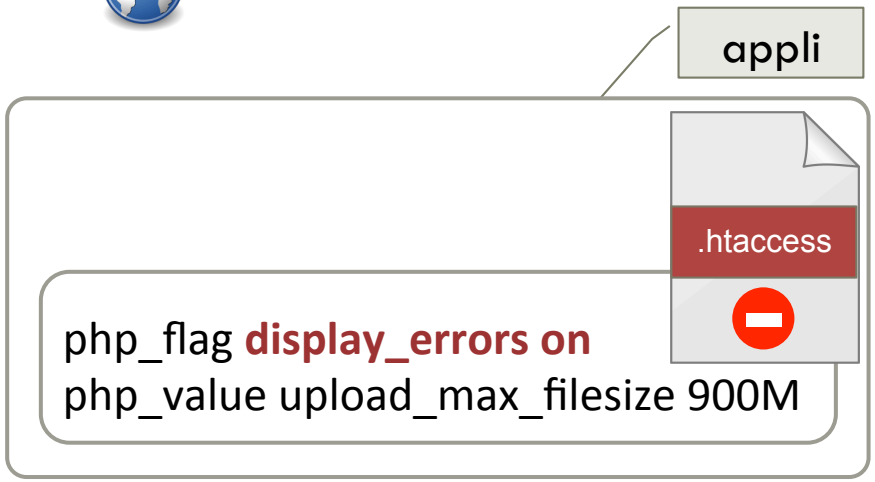
4. Interdire la surcharge de configuration

Interdire l'utilisation de .htaccess





Warning: mysqli_connect() [function.mysqli-connect]: (28000/1045): Access denied for user 'root'@'localhost' (using password: YES) in /…/appli/cnx.php on line 3

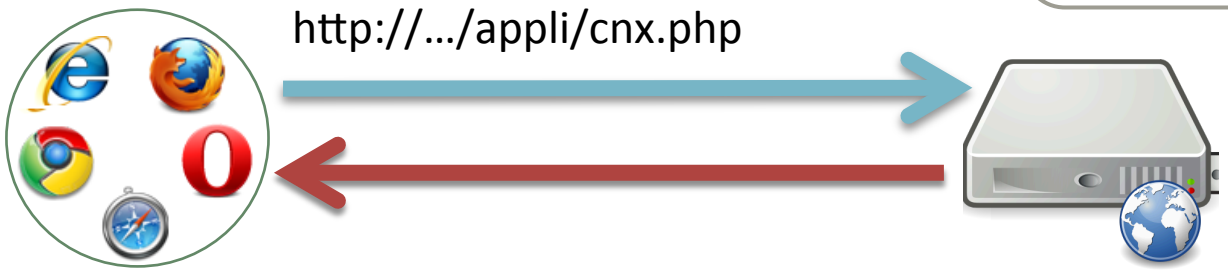


4. Interdire la surcharge de configuration

Interdire la modification des directives

```
<Directory />
    AllowOverride None
    php_admin_flag display_errors off
    php_admin_value upload_max_filesize 15M
</Directory>
<Directory …/appli>
    AllowOverride All
</Directory>
```

.conf



Warning: mysqli_connect() [function.mysqli-connect]: (28000/1045): Access denied for user 'root'@'localhost' (using password: YES) in /…/appli/cnx.php on line 3

appli

.htaccess

```
php_flag display_errors on
php_value upload_max_filesize 900M
```

5. Protéger les sessions

- Protéger le jeton

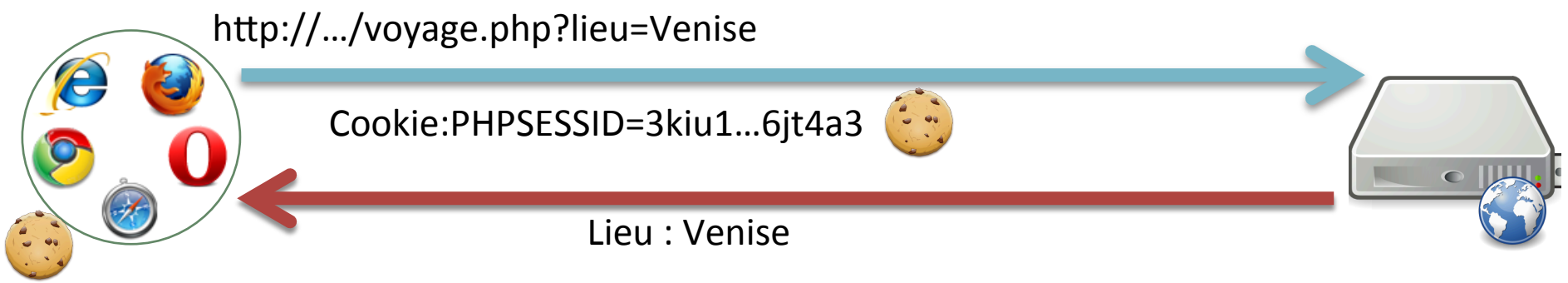
session.use_only_cookies = On

Transmission du jeton par cookie

5. Protéger les sessions

- Protéger le jeton


```
session.use_only_cookies = On
session.use_strict_mode = On
# Si HTTPS
session.cookie_secure = On
```

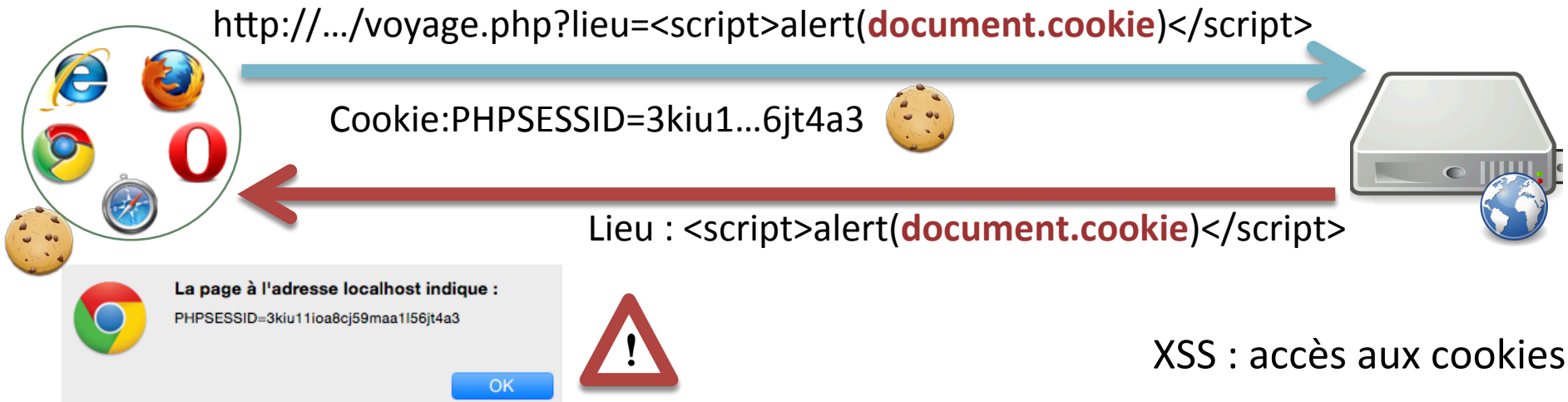


Transmission du jeton par cookie

5. Protéger les sessions

- Protéger le jeton

session.use_only_cookies = On
session.use_strict_mode = On

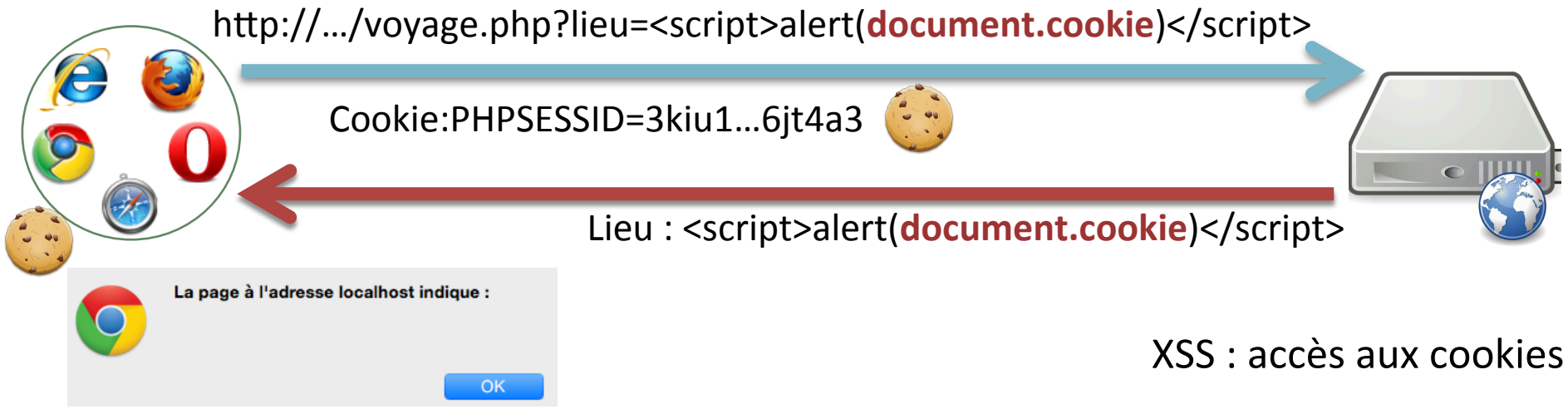


XSS : accès aux cookies

5. Protéger les sessions

- Protéger le jeton

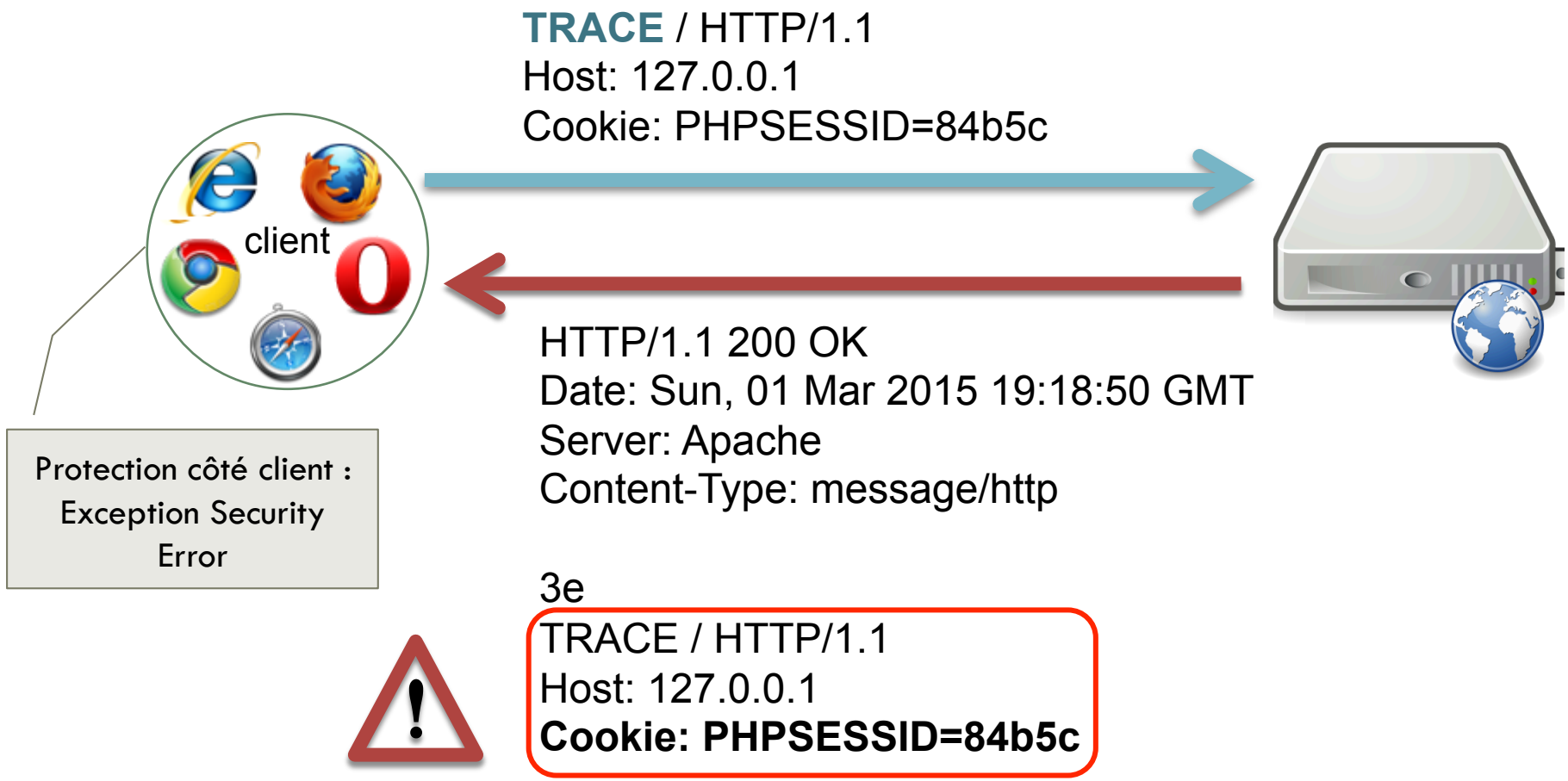
session.use_only_cookies = On
session.use_strict_mode = On
session.**cookie_httponly** = On



XSS : accès aux cookies

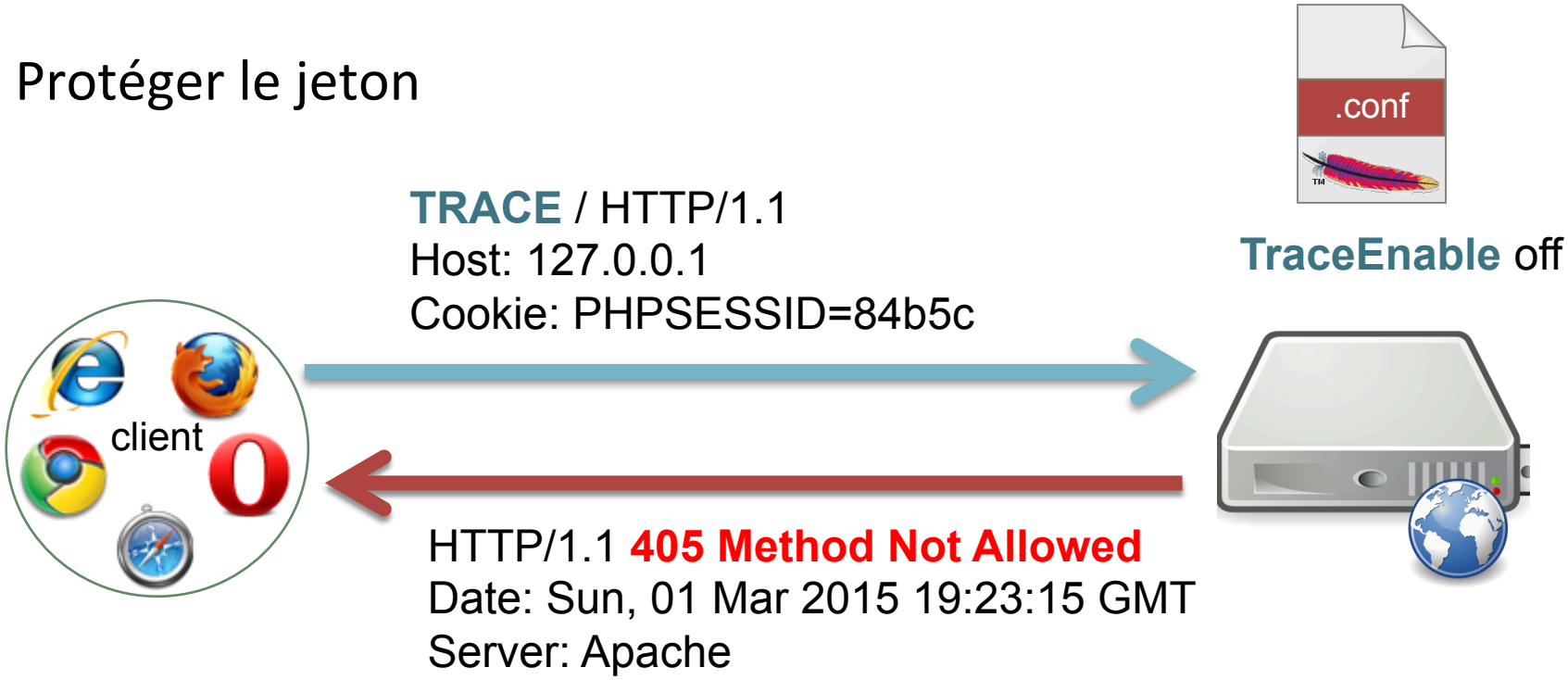
5. Protéger les sessions

- Protéger le jeton



5. Protéger les sessions

- Protéger le jeton



5. Protéger les sessions

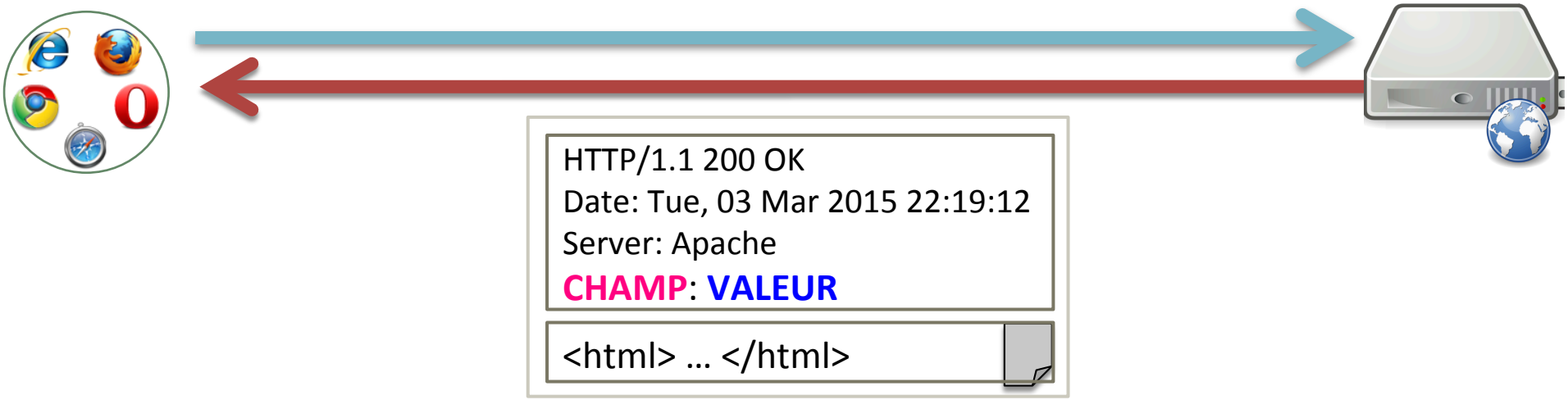
- Protéger les informations en session

session.save_handler = file
session.save_path = /var/php/session

Possibilité de stocker les informations dans une **base de données**

6. Champs d'en-tête HTTP de sécurité

- Ajouter des champs dans l'en-tête de la réponse HTTP



header("Content-Security-Policy: img-src 'self'");

Header set Content-Security-Policy "script-src 'self' "

Script PHP

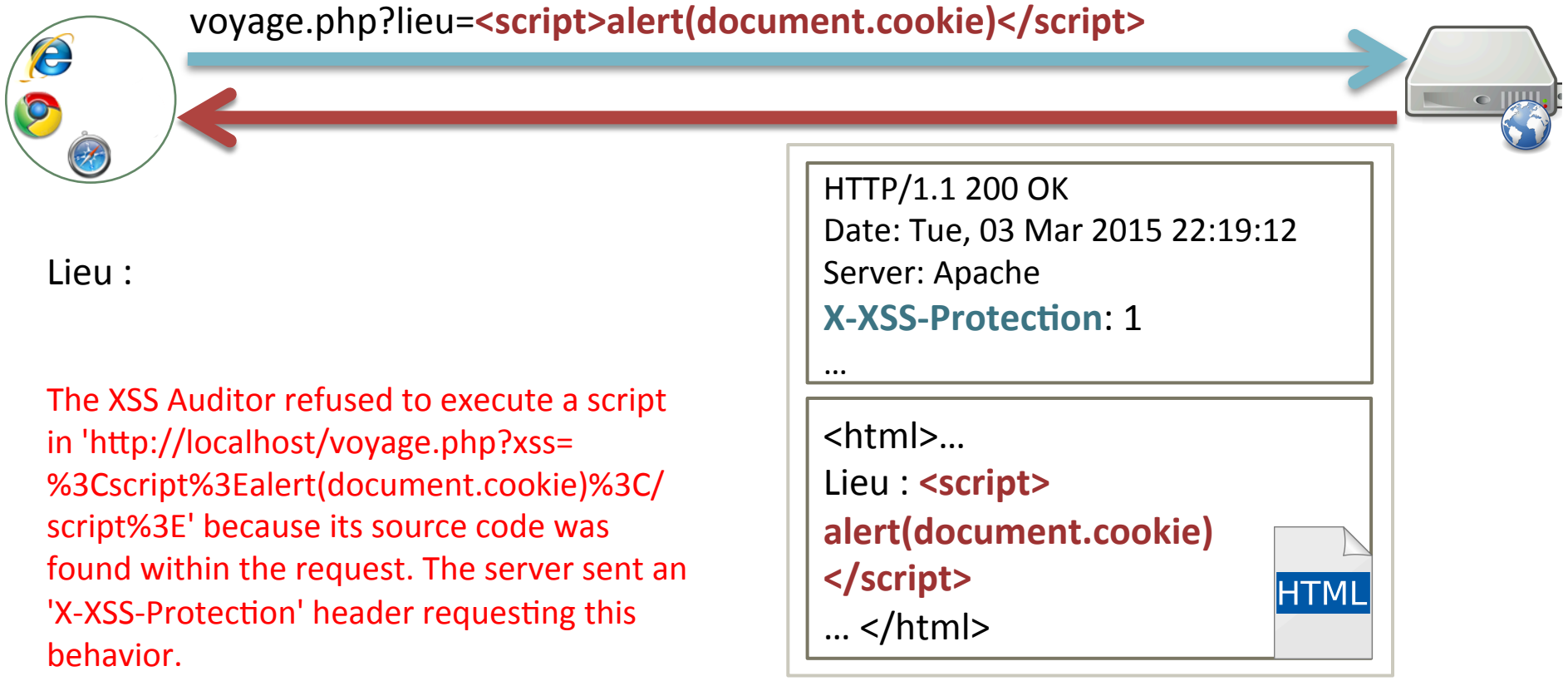
```
header("CHAMP:VALEUR");
```

Mod_header (.conf, .htaccess)

```
Header set CHAMP VALEUR
ou
Header append CHAMP VALEUR
```

6. Champs d'en-tête HTTP de sécurité

- En-tête HTTP X-XSS-Protection 0|1 Activation du filtre XSS



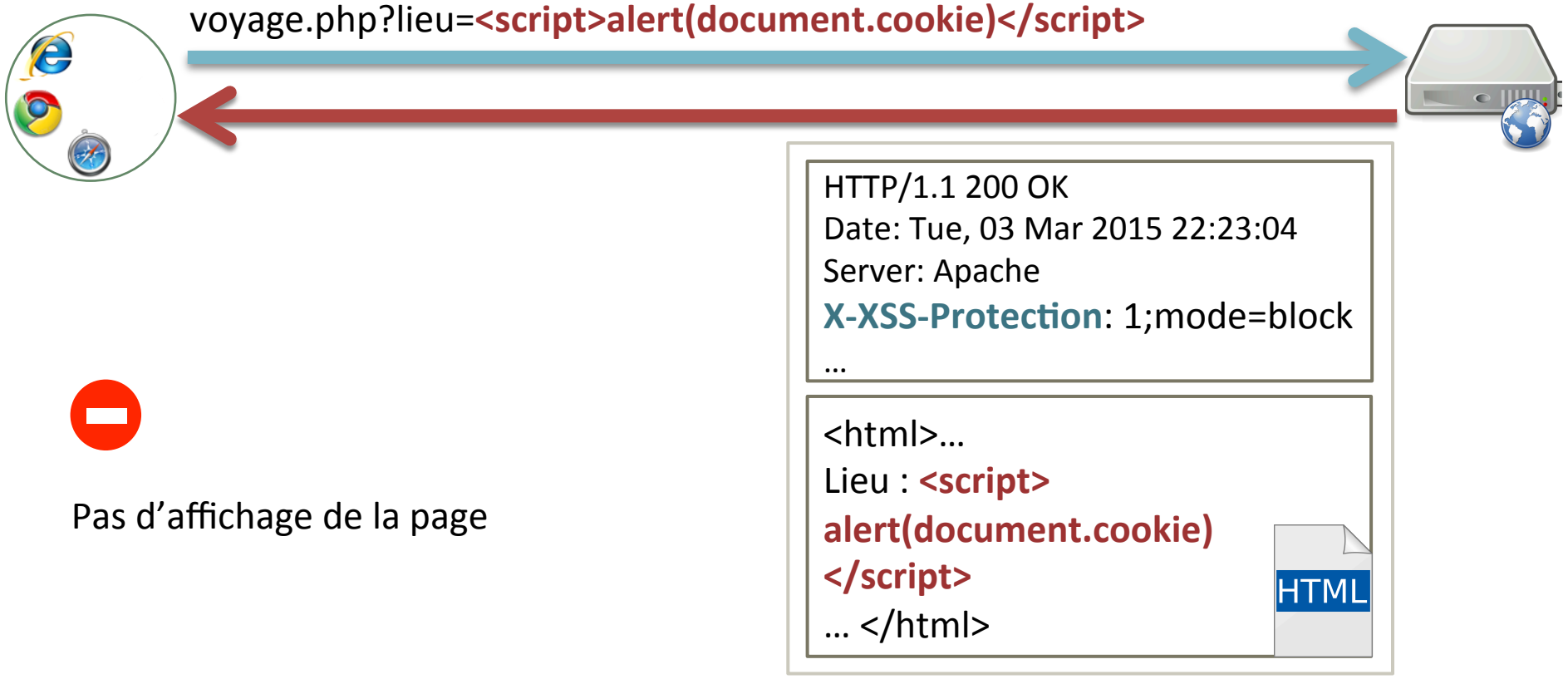
Lieu :

The XSS Auditor refused to execute a script in 'http://localhost/voyage.php?xss=%3Cscript%3Ealert(document.cookie)%3C/script%3E' because its source code was found within the request. The server sent an 'X-XSS-Protection' header requesting this behavior.

Page affichée, XSS non exécuté

6. Champs d'en-tête HTTP de sécurité

- En-tête HTTP X-XSS-Protection 0|1 Activation du filtre XSS



Google	Twitter
1; mode=block	1; mode=block

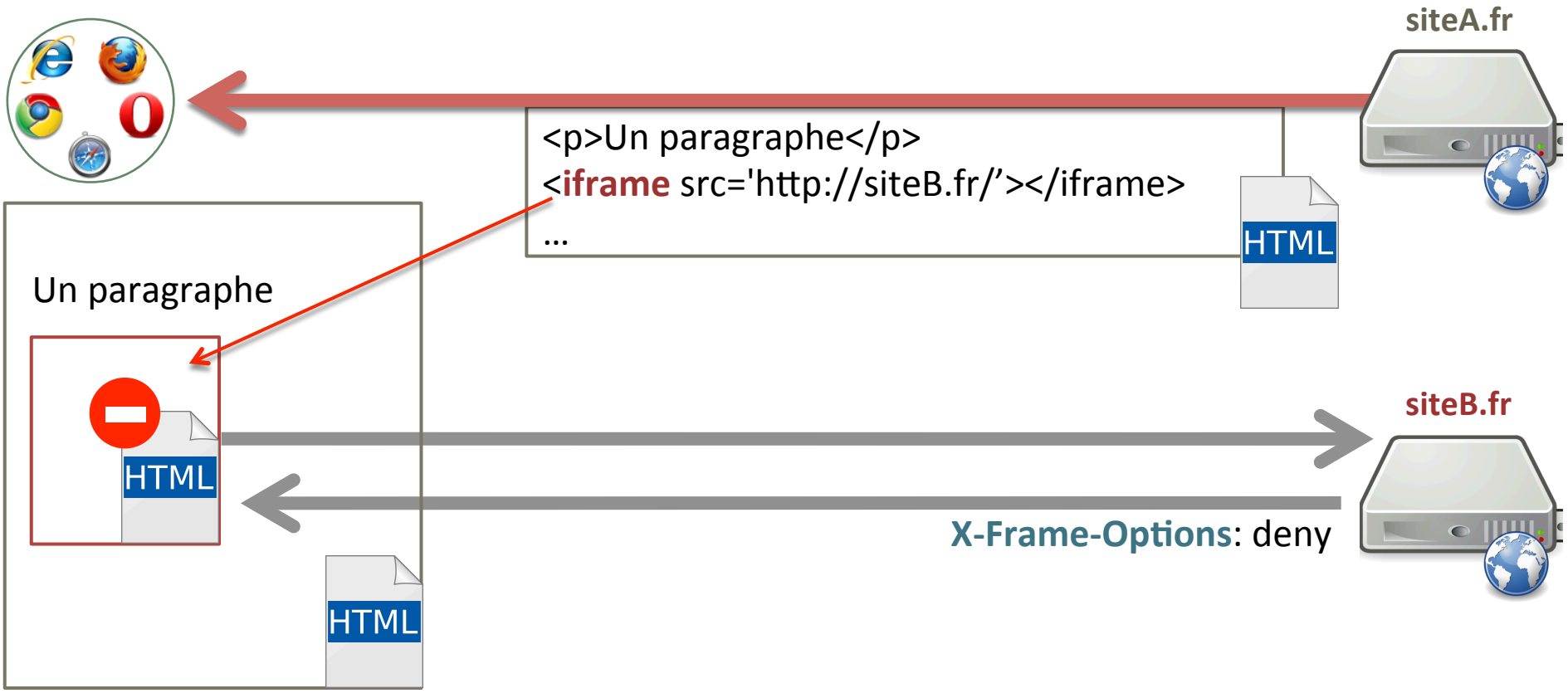
6. Champs d'en-tête HTTP de sécurité

- En-tête HTTP X-Frame-Options deny|sameorigin|allow-from *URL*

Cadre flottant = inclusion d'une page HTML dans un cadre de la page HTML

6. Champs d'en-tête HTTP de sécurité

- En-tête HTTP X-Frame-Options deny|sameorigin|allow-from *URL*



Refused to display 'http://siteB.fr' in a frame because it set 'X-Frame-Options' to 'deny'.

Google	Twitter	Facebook
SAMEORIGIN	SAMEORIGIN	DENY

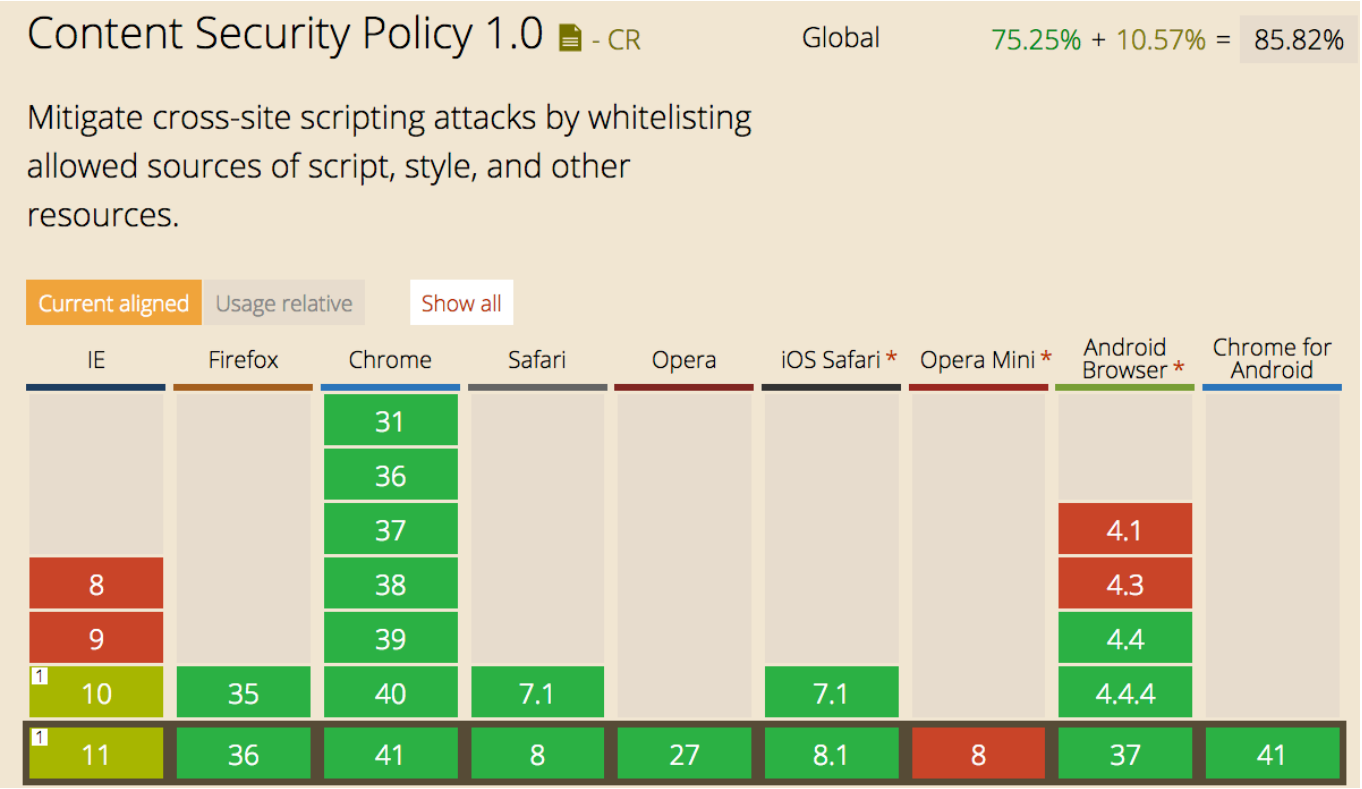
6. Champs d'en-tête HTTP de sécurité

- CSP (Content Security Policy – W3C) : en-tête HTTP Content-Security-Policy

  Politique : liste blanche de sources de confiance pour un type de ressources

  But : lutter contre le XSS et l'usurpation de contenu

  Version : 2.0 W3C Candidate Recommandation 19 janvier 2015



Support en mars 2015 - Source : http://caniuse.com/#feat=contentsecuritypolicy

6. Champs d'en-tête HTTP de sécurité

CSP : Scripts JS de **même domaine**

```
HTTP/1.1 200 OK
Date: Mon, 02 Mar 2015 23:14:06
Server: Apache
Content-Security-Policy: script-src 'self'
...
```

```
<html>
...
</html>
```

Content-Security-Policy: script-src 'self'

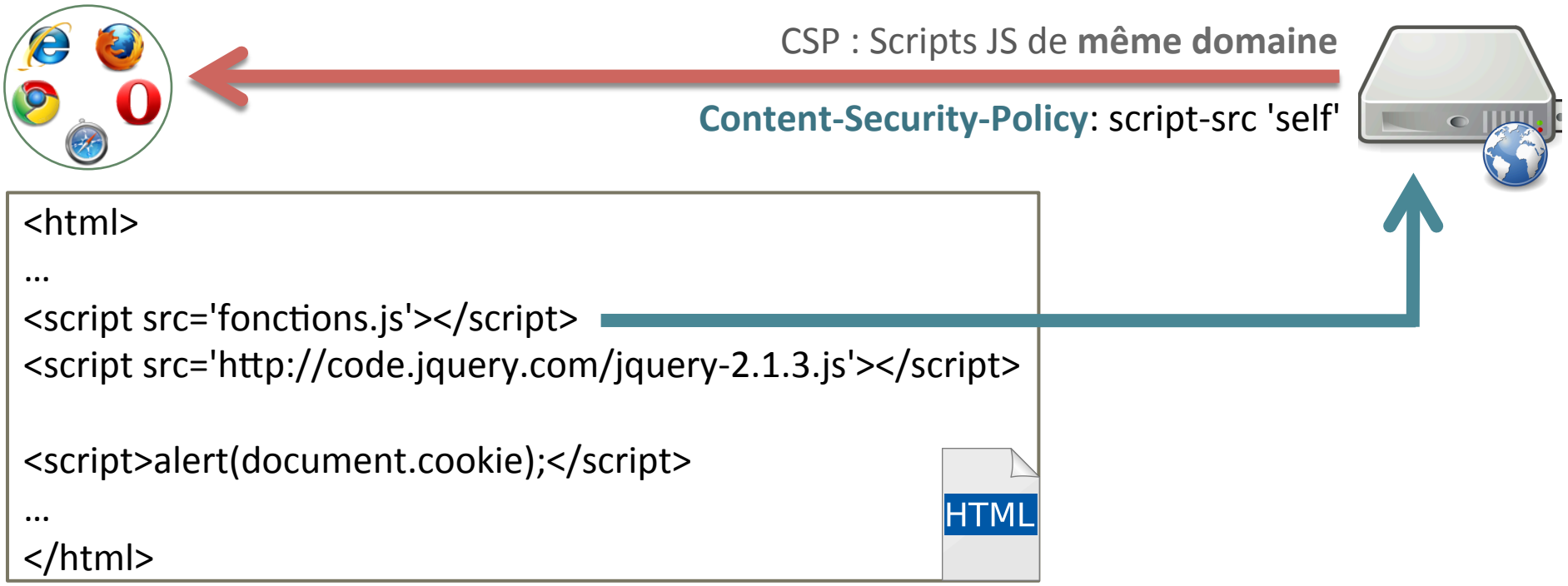
directive CSP

mot clé (self, none)

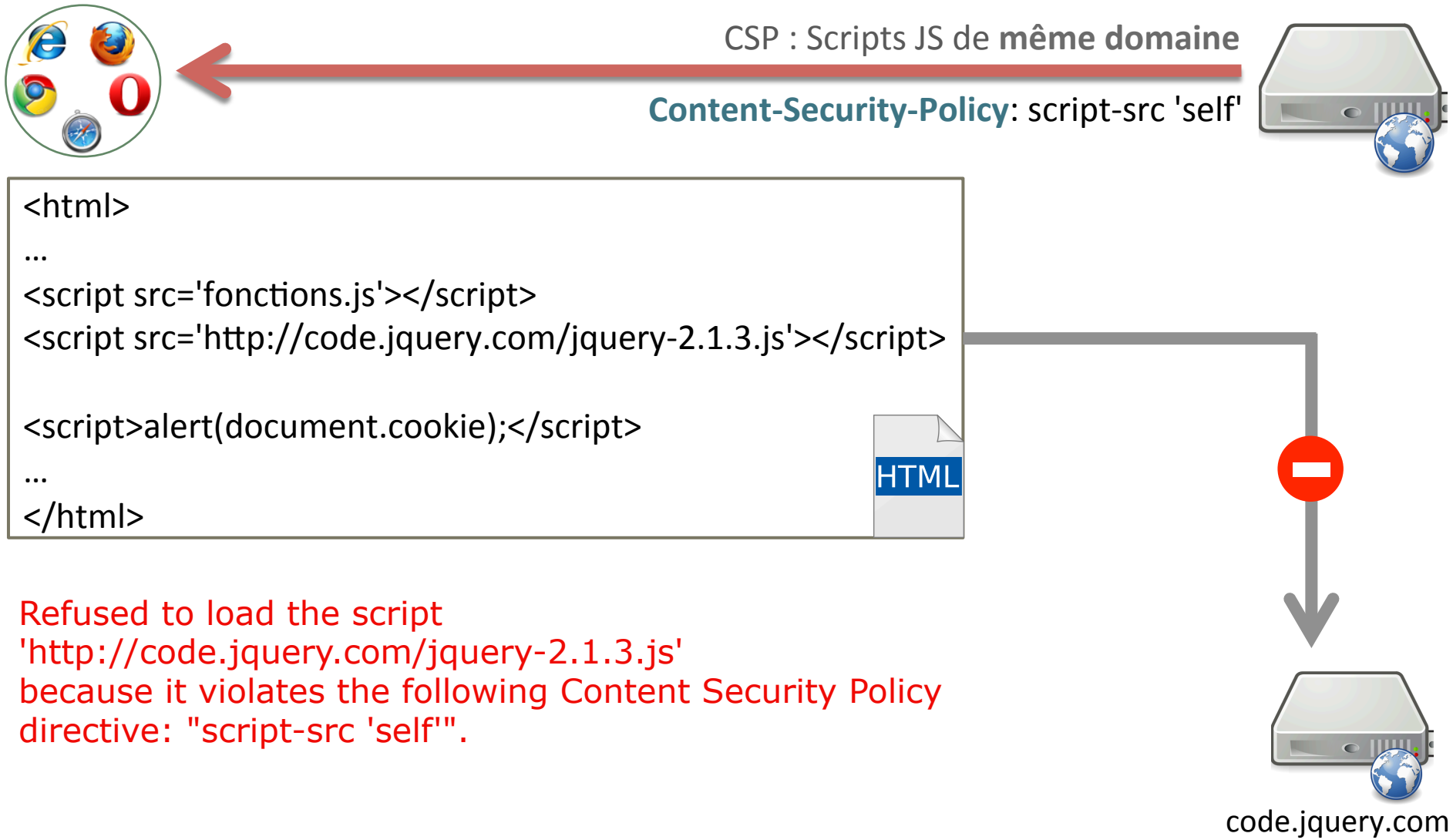
En-tête :

- Content-Security-Policy (W3C)
- X-Content-Security-Policy (Firefox 4-22, IE10)
- X-WebKit-CSP (Chrome < 25)

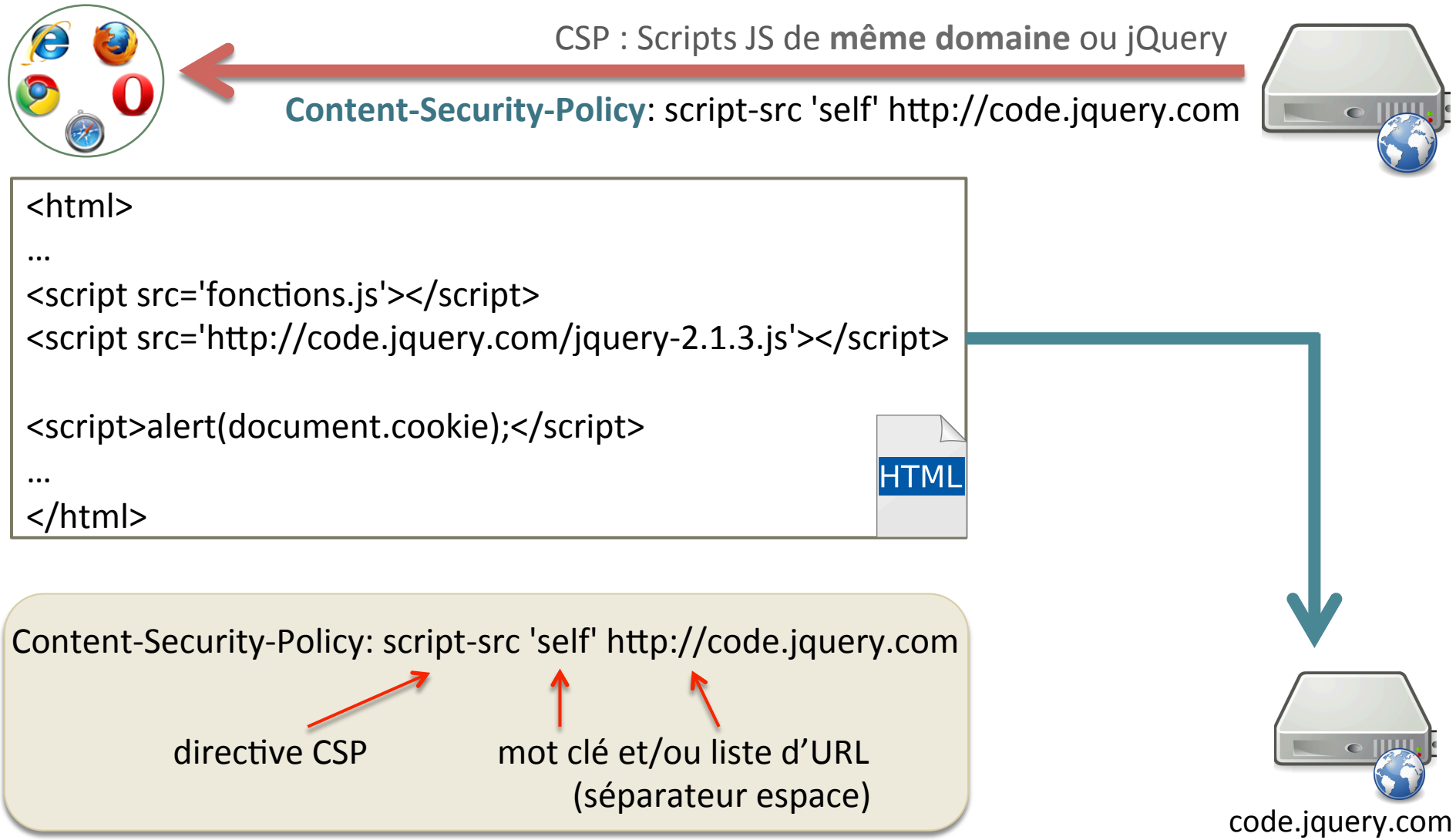
6. Champs d'en-tête HTTP de sécurité



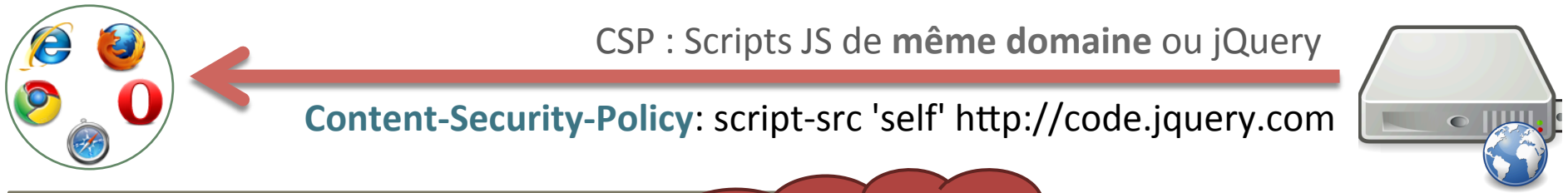
6. Champs d'en-tête HTTP de sécurité

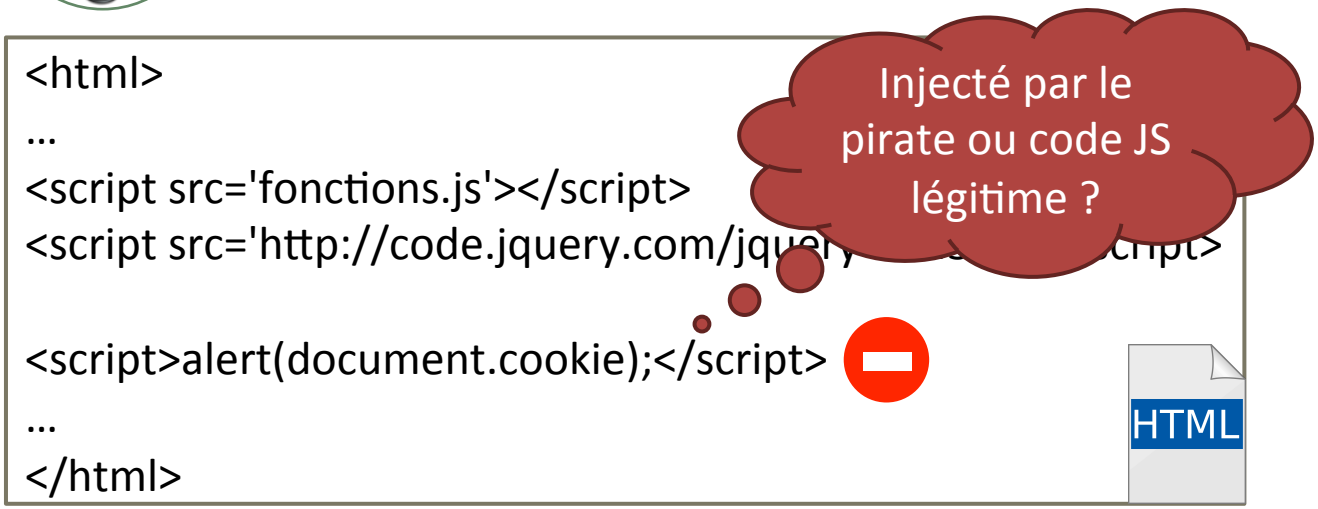


6. Champs d'en-tête HTTP de sécurité



6. Champs d'en-tête HTTP de sécurité



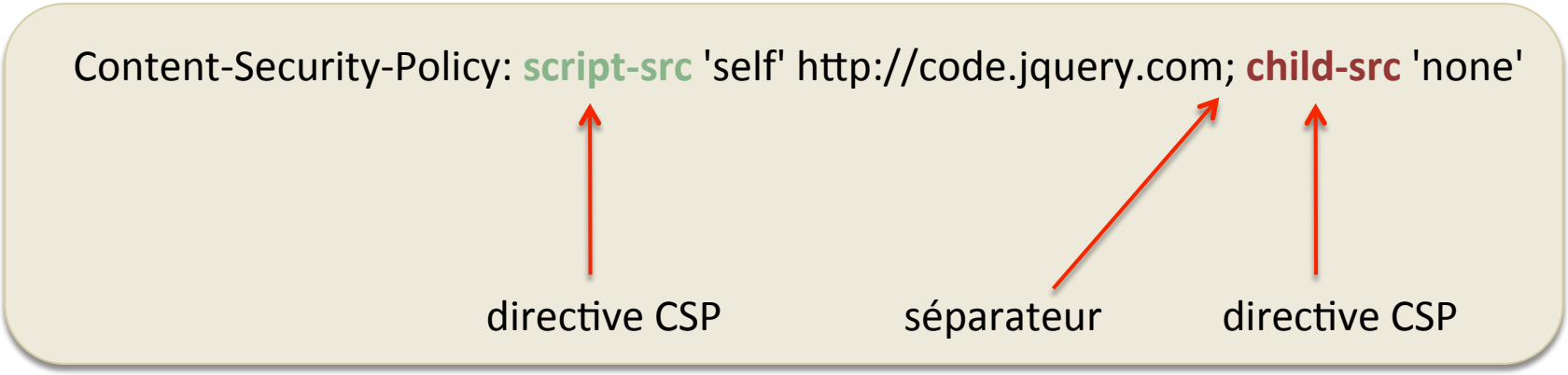


Refused to execute inline script because it violates the following Content Security Policy directive: "script-src 'self'". Either the 'unsafe-inline' keyword, a hash ('sha256-...'), or a nonce ('nonce-...') is required to enable inline execution.

Tout le code JS doit être placé dans des scripts externes

6. Champs d'en-tête HTTP de sécurité

Politique CSP = liste de directives séparées par ';'



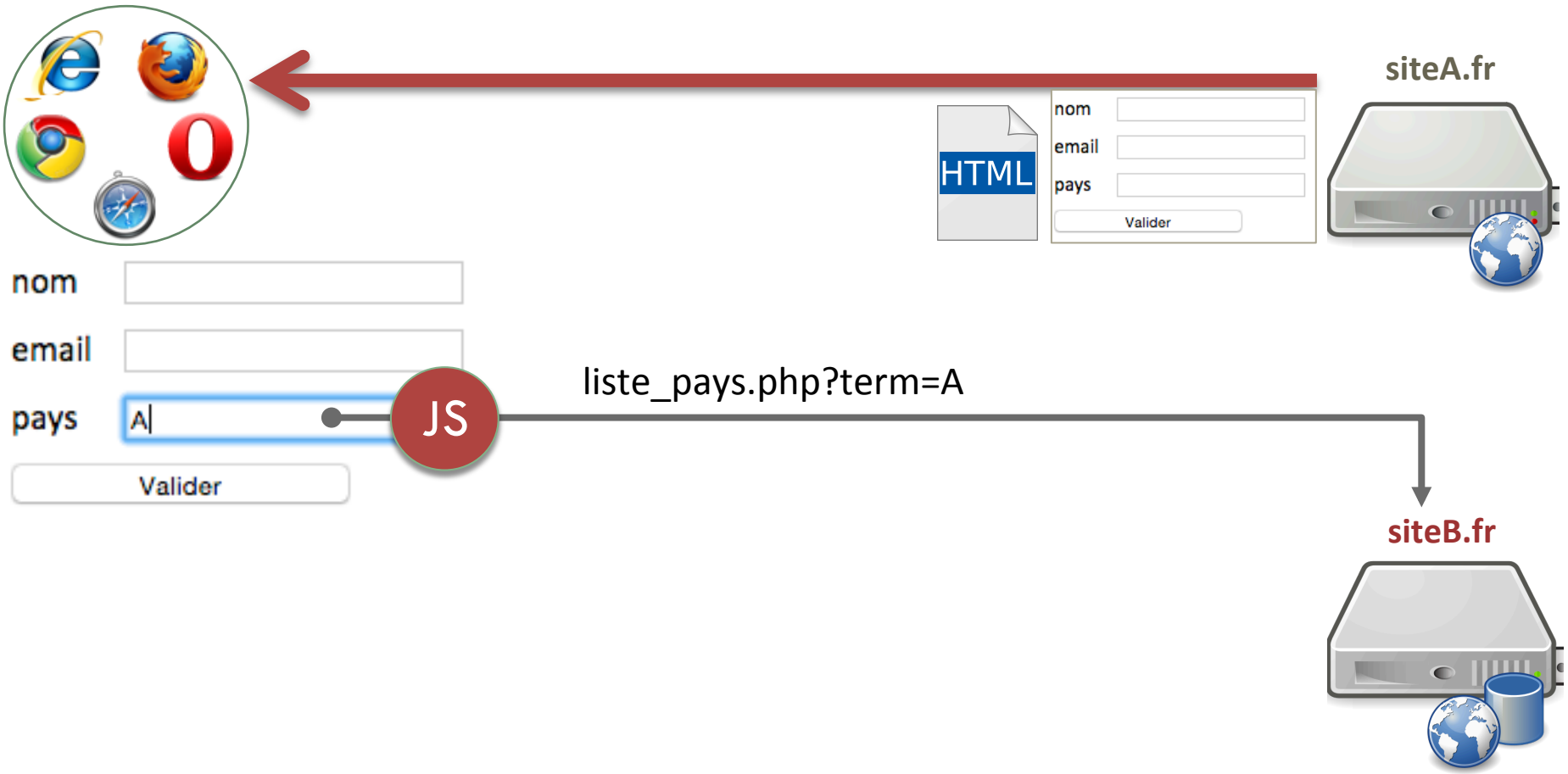
Scripts JS exécutés si même domaine ou jquery, pas de iframe

6. Champs d'en-tête HTTP de sécurité

Quelques directives CSP	Description
default-src	politique générale de téléchargement (liste utilisée par défaut)
script-src	liste blanche pour les scripts <script>
img-src	liste blanche pour les images <img>
style-src	liste blanche pour les styles CSS <style>
font-src	liste blanche pour les polices @font-face
form-action (CSP ≥ 1.1)	liste blanche des URL autorisées dans l'attribut action de <form>
media-src	liste blanche pour <video> et <audio>
object-src	liste blanche pour les plugin <object>
plugin-types (CSP ≥ 1.1)	liste blanche des types de plugin autorisés, ex application/pdf
frame-src (CSP 1) *obsolète*	liste blanche pour <frame>, <iframe>
child-src (CSP 2)	liste blanche pour <frame>, <iframe>

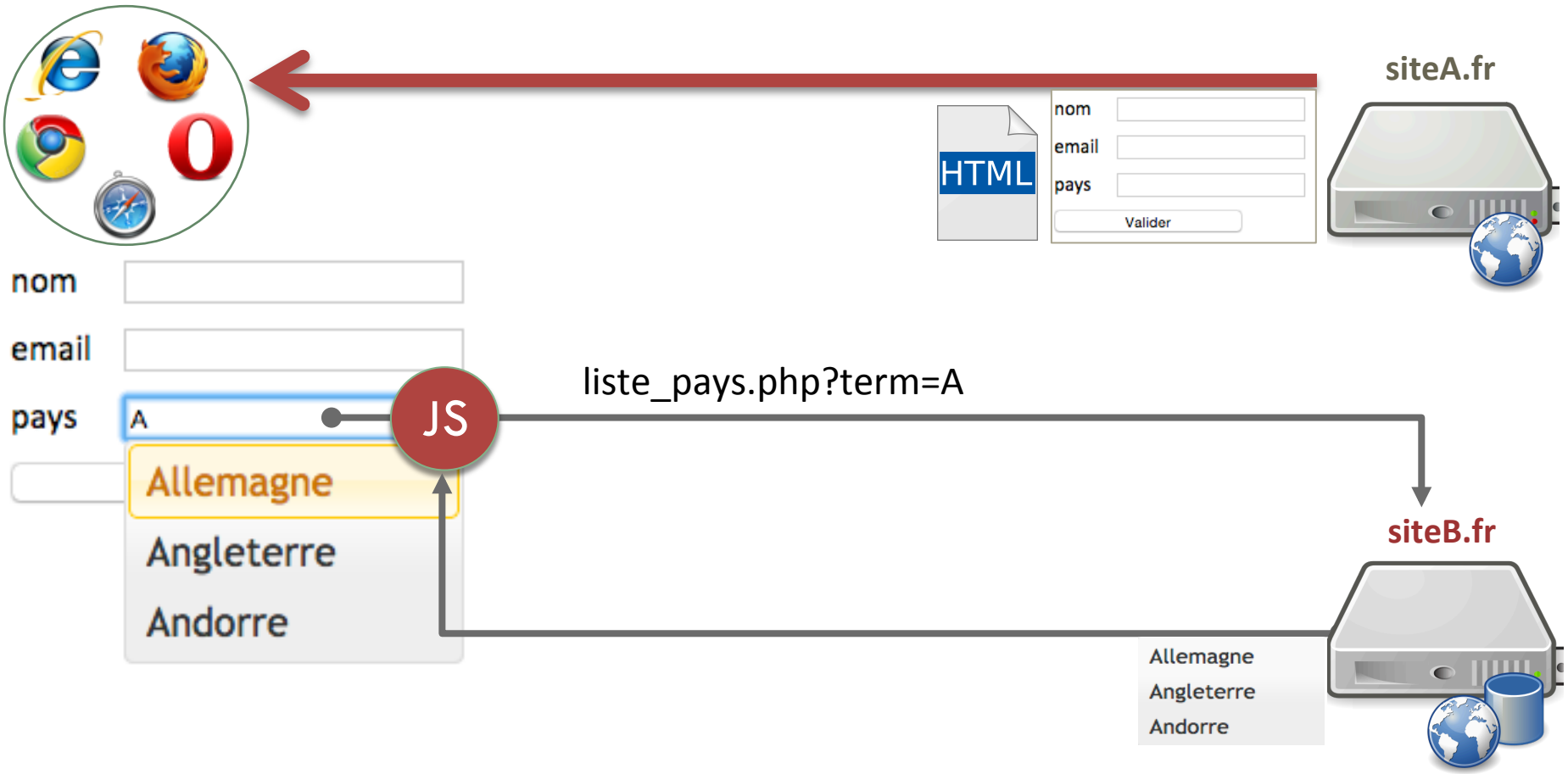
6. Champs d'en-tête HTTP de sécurité

Politique AJAX
cross domaine



6. Champs d'en-tête HTTP de sécurité

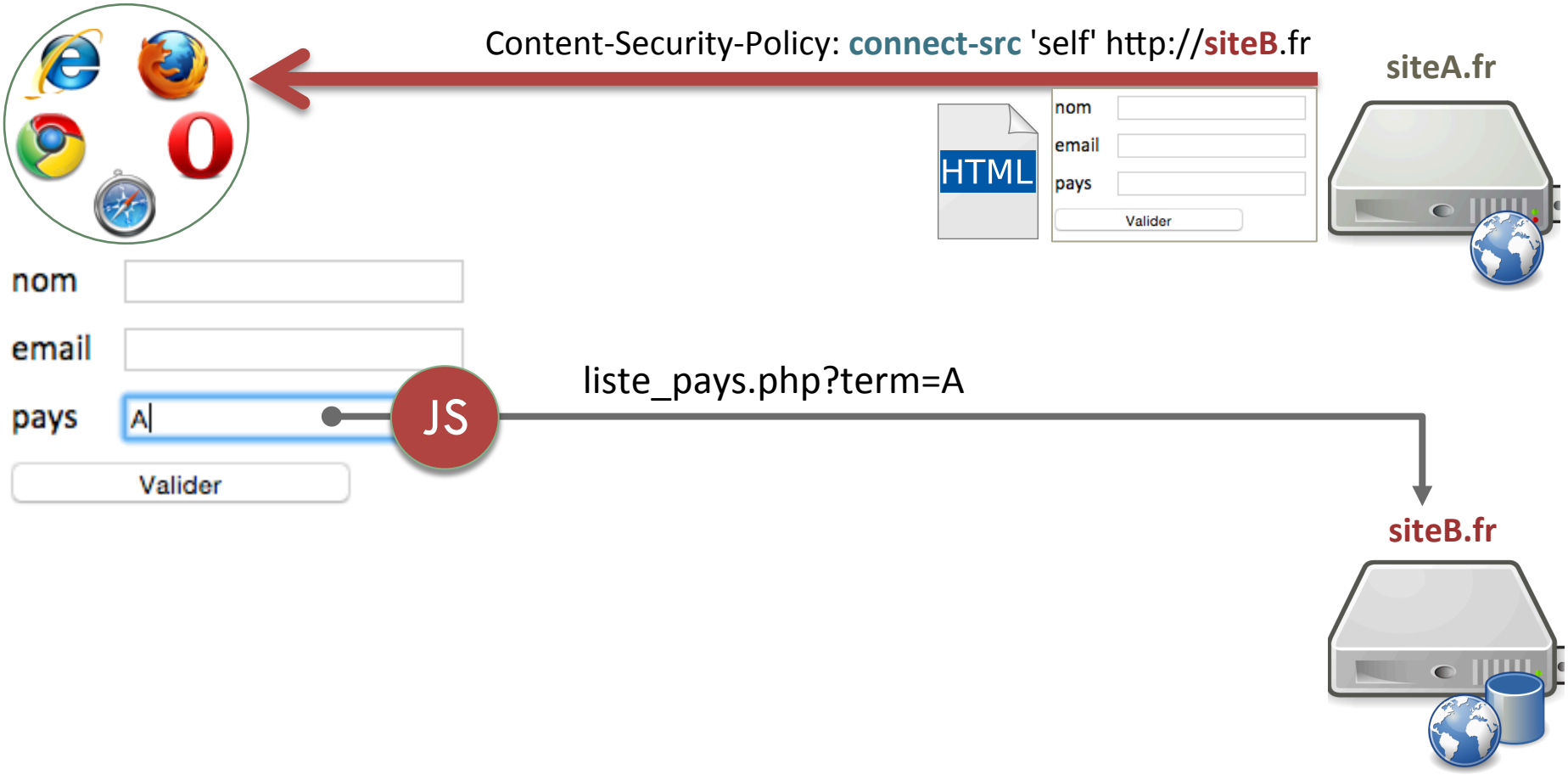
Politique AJAX
cross domaine



6. Champs d'en-tête HTTP de sécurité

Politique AJAX cross domaine

connect-src (CSP) : autoriser XHR vers sites de confiance A et B

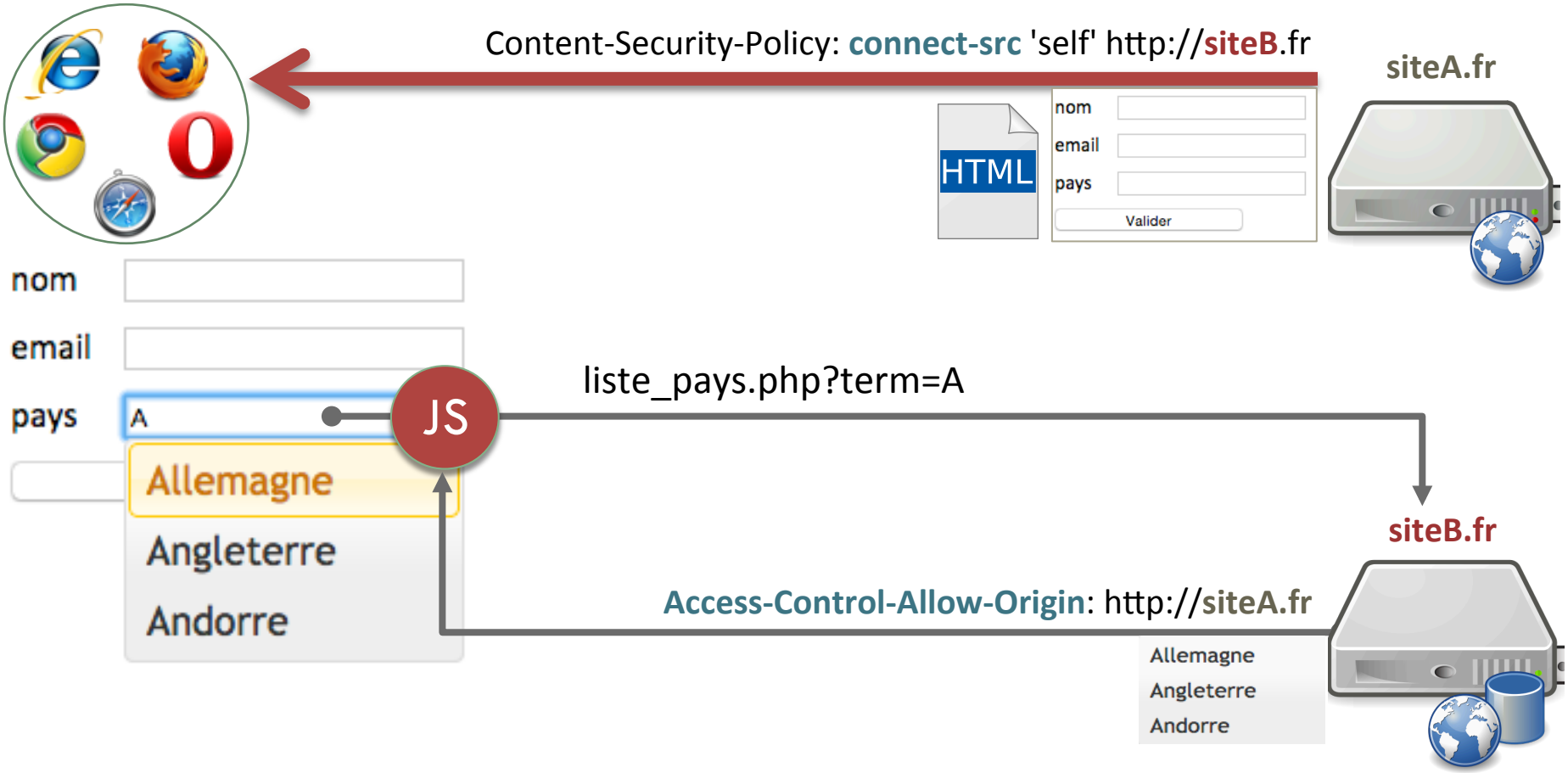


6. Champs d'en-tête HTTP de sécurité

Politique AJAX cross domaine

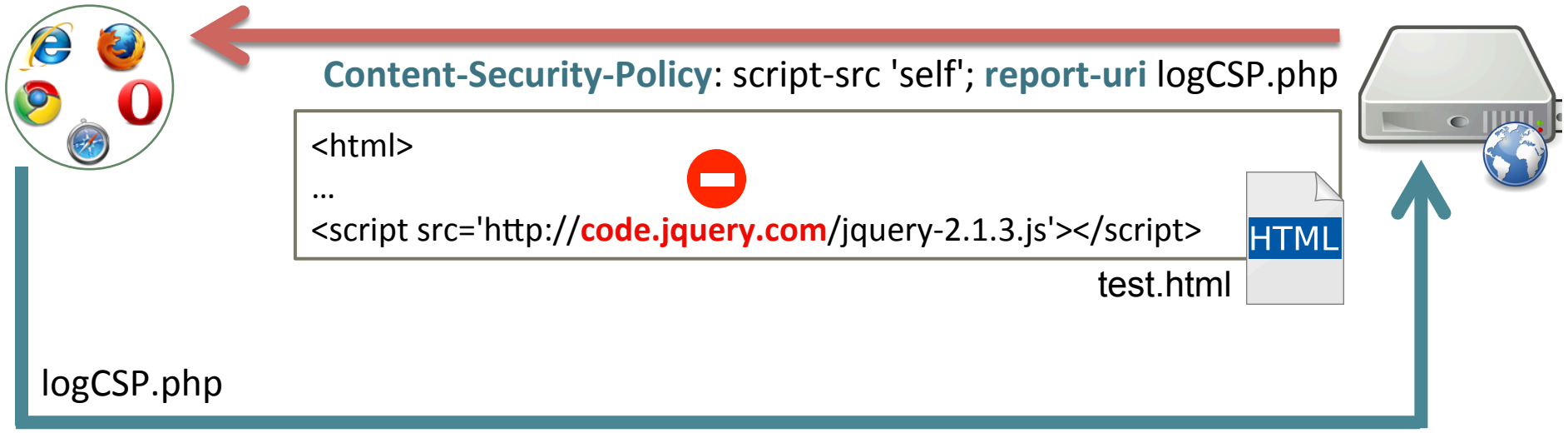
connect-src (CSP) : autoriser XHR vers sites de confiance A et B

Access-Control-Allow-Origin (CORS) : sites autorisés à demander une ressource



6. Champs d'en-tête HTTP de sécurité

Envoi au serveur d'un rapport de violation CSP au format JSON, par la méthode POST




```
{ "csp-report":
        {
            "document-uri": "http://localhost/test.html",
            "referrer": "http://localhost/accueil.html",
            "violated-directive": "script-src 'self' ",
            "original-policy": "script-src 'self'; report-uri logCSP.php"
            "blocked-uri": "http://code.jquery.com"
        }
}
```

6. Champs d'en-tête HTTP de sécurité

Attention à la fausse sensation de sécurité

- La politique peut être mal définie
- ou trop permissive.
- Si le navigateur ne supporte pas le champ d'en-tête, il l'ignore

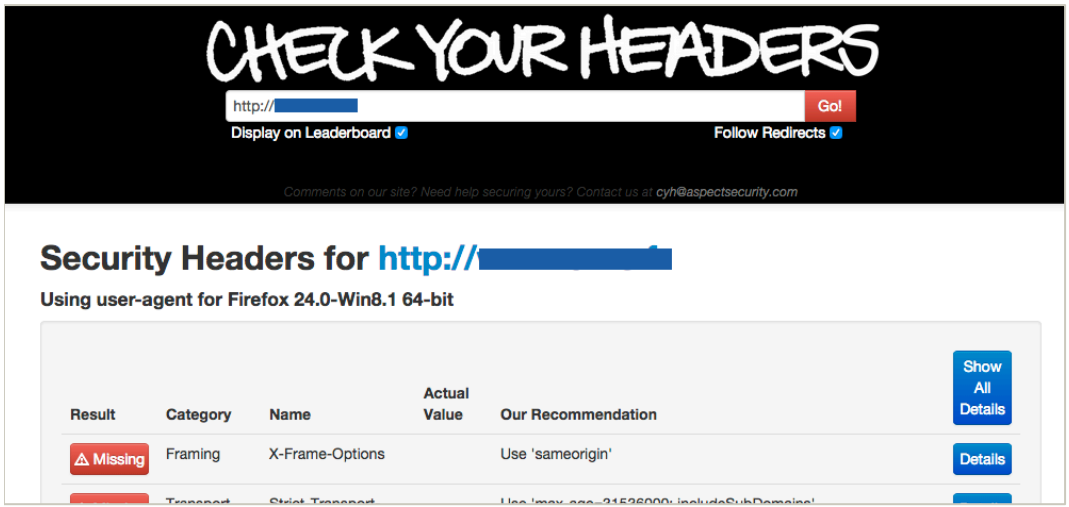
Utiliser comme protection supplémentaire, ne doit pas remplacer

- filtrage des entrées
- protection des sorties

Références

- Apache
  - http://httpd.apache.org/docs/trunk/misc/security_tips.html
  - https://www.owasp.org/index.php/List_of_useful_HTTP_headers
- PHP
  - http://php.net/manual/fr/security.php
  - http://www.php.net/manual/fr/ini.list.php
- CSP (content security policy)
  - http://www.w3.org/TR/CSP/
  - https://developer.mozilla.org/en-US/docs/Web/Security/CSP/CSP_policy_directives
  - http://caniuse.com/#feat=contentsecuritypolicy (support CSP)
- CORS
  - http://www.w3.org/TR/access-control/

Références



http://cyh.herokuapp.com/cyh

Références

Scanner de configuration PHP https://github.com/psecio/iniscan

```
pc6:iniscan-master magali$ bin/iniscan scan --path=/Applications/AMPPS/conf/php-5.6.ini
== Executing INI Scan [03.01.2015 21:56:22] ==

Results for /Applications/AMPPS/conf/php-5.6.ini:
============
Status | Severity | PHP Version | Key                      | Description
-------------------------------------------------------------------------
PASS   | ERROR    |             | session.use_cookies      | Accepts cookies to manage sessions
PASS   | ERROR    | 4.3.0       | session.use_only_cookies | Must use cookies to manage sessions, don't accept session-ids in a link
FAIL   | WARNING  |             | session.cookie_domain    | It is recommended that you set the default domain for cookies.
PASS   | ERROR    | 5.2.0       | session.cookie_httponly  | Setting session cookies to 'http only' makes them only readable by the browser
PASS   | ERROR    | 4.3.0       | session.bug_compat_42    | An undocumented feature/bug that allows initialize of a session in the global scope even if register_globals is disabled for PHP up to 5.3.22
PASS   | WARNING  | 4.3.0       | session.bug_compat_warn  | Disable warnings for session.bug_compat_42
FAIL   | WARNING  |             | session.hash_function    | Weak hashing algorithms in use. Rather use one of these: sha224, sha256, sha384, sha512, ripemd128, ripemd160, ripemd256, ripemd320, whirlpool, tige
r128,3, tiger160,3, tiger192,3, tiger128,4, tiger160,4, tiger192,4, snefru256, adler32, crc32, crc32b, fnv132, fnv164, joaat, haval128,3, haval160,3, haval192,3, haval224,3, haval256,3, haval128,4, haval160,4,
 haval192,4, haval224,4, haval256,4, haval128,5, haval160,5, haval192,5, haval224,5, haval256,5
PASS   | WARNING  |             | session.save_path        | Session save path should be set and writeable by only the web user
PASS   | ERROR    | 4.0.3       | session.use_trans_sid    | If used 'use_trans_sid' setting puts the session ID on the URL, making it easier to hijack
FAIL   | ERROR    | 4.0.4       | session.cookie_secure    | Cookie secure specifies whether cookies should only be sent over secure connections.
PASS   | WARNING  |             | session.entropy_file     | A file should be provided to help provide session entropy
N/A    | WARNING  | 5.5.2       | session.use_strict_mode  | Strict mode prevents uninitialized session IDs in the built-in session handling.
FAIL   | ERROR    | 4.0.3       | allow_url_fopen          | Do not allow the opening of remote file resources ('Off' recommended)
PASS   | ERROR    | 5.2.0       | allow_url_include        | Do not allow the inclusion of remote file resources ('Off' recommended)
FAIL   | WARNING  |             | display_errors           | Don't show errors in production ('Off' recommended)
PASS   | WARNING  |             | log_errors               | Log errors in production ('On' recommended)
PASS   | WARNING  |             | expose_php               | Showing the PHP signature exposes additional information
PASS   | ERROR    |             | register_globals         | The register globals setting is dangerous and has been deprecated ('Off' recommended)
PASS   | ERROR    |             | magic_quotes_gpc         | Magic quotes automatically adds quotes to incoming data ('Off' recommended)
PASS   | ERROR    |             | magic_quotes_runtime     | Magic quotes should be disabled at runtime in addition to being off for incoming data
PASS   | WARNING  |             | post_max_size            | A too large value for the maximum post size could allow for DoS against your application
PASS   | ERROR    |             | safe_mode                | It's not actually 'safe' ('Off' recommended)
PASS   | WARNING  |             | register_long_arrays     | Registering long arrays turns on the HTTP_*_VARS (Recommended Off)
PASS   | WARNING  |             | max_input_vars           | A maximum number of input variables should be defined to prevent performance issues
FAIL   | WARNING  |             | display_startup_errors   | Showing startup errors could provide extra information to potential attackers
FAIL   | WARNING  |             | open_basedir             | Restricting PHP's access to the file system to a certain directory prevents file-based attacks in unauthorized areas.
PASS   | WARNING  |             | error_reporting          | Error reporting should be different based on context, off in production
PASS   | WARNING  |             | upload_max_filesize      | A maximum upload size should be defined to prevent server overload from large requests
PASS   | WARNING  |             | upload_max_filesize      | The max upload size should not be too high, to prevent server overload from large requests
PASS   | WARNING  |             | post_max_size            | A maximum post size should be defined to prevent server overload from large requests
PASS   | WARNING  |             | post_max_size            | The max upload size should not be too high, to prevent server overload from large requests
PASS   | WARNING  |             | memory_limit             | A memory limit should be defined to prevent server overload from large processes
PASS   | WARNING  |             | memory_limit             | The standard memory limit should not be too high, if you need more memory for a single script you can adjust that during runtime using ini_set()
PASS   | WARNING  |             | asp_tags                 | Old versions of PHP allowed for ASP-style tags (<% %>) instead of <?php. This should be disabled.
PASS   | WARNING  |             | xdebug.default_enable    | Xdebug should be disabled in production
PASS   | WARNING  |             | xdebug.remote_enable     | Xdebug should not be trying to contact debug clients
FAIL   | WARNING  |             | disable_functions        | Methods still enabled - exec, passthru, shell_exec, system, proc_open, popen, curl_exec, curl_multi_exec
PASS   | WARNING  |             | soap.wsdl_cache_dir      | Checks to see if the SOAP WSDL cache directory is inside open_basedir for PHP before 5.3.22 and 5.4.x before 5.4.13
PASS   | WARNING  |             | upload_tmp_dir           | Checks to see if the upload_tmp_dir is inside the open_basedir folder

30 passing
2 failure(s) and 6 warnings
pc6:iniscan-master magali$
```

Annexe - Autres réglages de sécurité

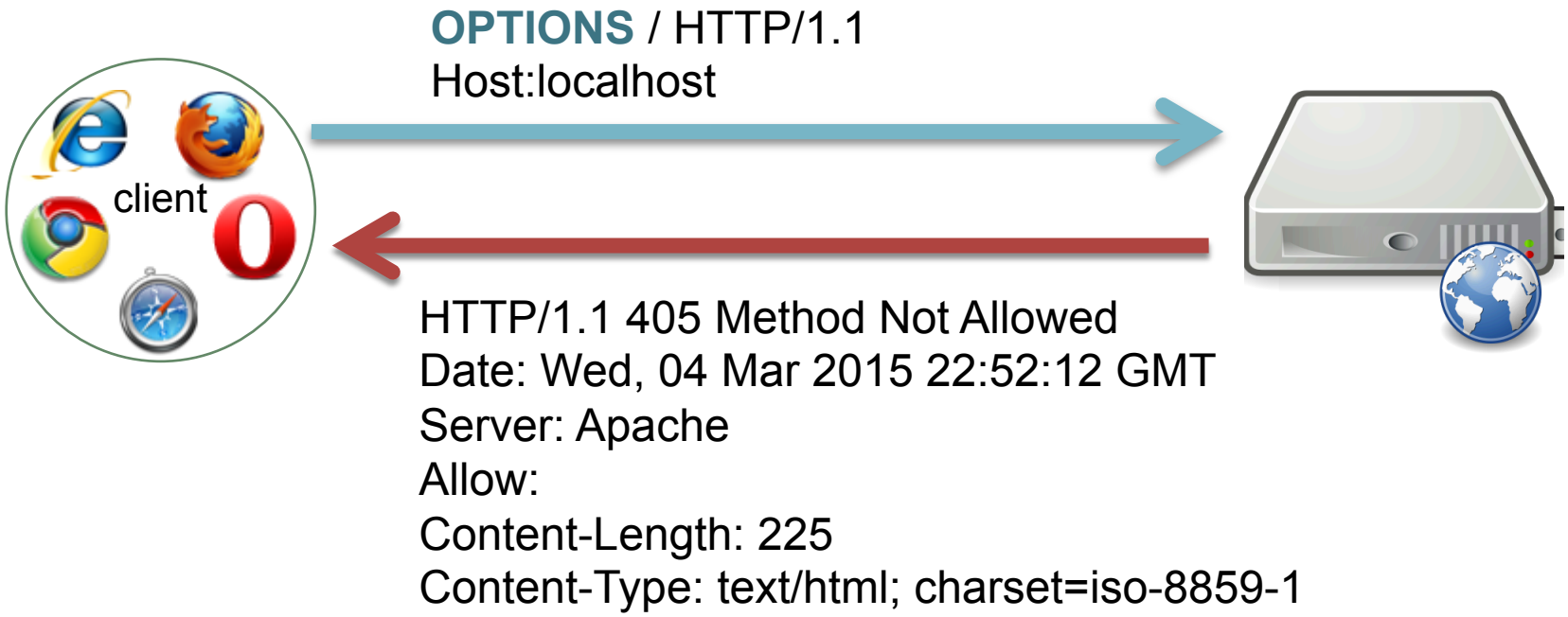

```
; ----  fichiers ----
allow_url_fopen = Off          ; pas d'URL dans fopen, …
allow_url_include = Off        ; pas d'URL pour require, include, …
file_uploads = Off             ; sauf si telechargement autorises
open_basedir = "/www/"         ; limiter chemin pour ouverture fichiers

disable_functions = "system, exec,shell_exec,phpinfo,phpversion,…"

; ---- contrôle des ressources -------
upload_max_filesize = xM       ; taille limite des fichiers téléchargés
post_max_size = yM             ; taille max données du POST (y > x)
max_execution_time = 45        ; durée max d'exécution du script (secondes, 0 = pas de  limite)
max_input_vars =1000           ; nombre max de variables GET/POST/COOKIE
max_input_time = 30            ; durée max d'analyse des variables POST/GET (sec.)
memory_limit = 50M             ; mémoire max qu'un script peut allouer (-1 = pas de limite)

register_globals = Off         ; n'existe plus en 5.4
enable_dl = Off                ; désactiver le chargement dynamique d'extension
```

Annexe - Autres réglages de sécurité

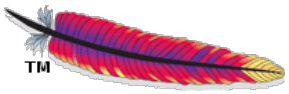
- Méthodes HTTP : interdire OPTIONS, PUT/DELETE (sauf si REST)

module expérimental mod_allowmethods

```
<Location />
    AllowMethods GET POST
</Location>
```



Annexe - Autres réglages de sécurité



- Déni de service

```
# --- DOS: limiter la taille des requêtes HTTP ----
LimitRequestBody 102400   # max corps = 100 Ko (0 : no limit, augmenter si upload)
LimitRequestLine 8190     # nb max octets dans la ligne contenant methode, URL, version
LimitRequestFields 50     # nb max de champs dans l'en-tête (0 : no limit)
LimitRequestFieldSize 8190 # nb octets max dans un champ d'en-tête
```

Module pour Apache 2.4 mod_qos

http://opensource.adnovum.ch/mod_qos/

http://devlog.cnrs.fr/jdev2015

T1 - Systèmes embarqués, réseaux de capteurs et objets communicants

T2 - Modélisation et ingénierie

T3 - Données massives scientifiques (Big data)

T4 - Transfert marchand et non marchand

T5 - Infrastructures et interopérabilité: Le cloud et les architectures orientées service

T6 - Les usines logicielles, le DevOps et la virtualisation

T7 - Javascript

T8 - Logiciels scientifiques et simulations: nouveaux modèles et enjeux

Merci

Questions ?

Licences icônes


Par RRZEicons (Travail personnel) [CC BY-SA 3.0 (http://creativecommons.org/licenses/by-sa/3.0)], via Wikimedia Commons

http://commons.wikimedia.org/wiki/File:Server-web.svg?uselang=fr
http://commons.wikimedia.org/wiki/File:Server-web-database.svg?uselang=fr

Par J.J. at the English language Wikipedia [GFDL (www.gnu.org/copyleft/fdl.html) or CC-BY-SA-3.0 (http://creativecommons.org/licenses/by-sa/3.0/)], from Wikimedia Commons

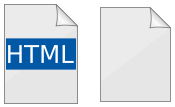
http://commons.wikimedia.org/wiki/File:Piratey_transparent_background.svg

By Everaldo Coelho; see upload log (based on File:Crystal personal.png) [LGPL (http://www.gnu.org/licenses/lgpl.html)], via Wikimedia Commons

http://commons.wikimedia.org/wiki/File%3ACrystal_personal.svg

© 2007 Nuno Pinheiro & David Vignoni & David Miller & Johann Ollivier Lapeyre & Kenneth Wimer & Riccardo Iaconelli / KDE / LGPL 3, via Wikimedia Commons

http://commons.wikimedia.org/wiki/File:Oxygen480-apps-preferences-web-browser-cookies.svg



https://openclipart.org/detail/171856/icon-html---a-cone

https://openclipart.org/detail/83893/file-icon

http://www.apache.org/foundation/press/kit/

http://php.net/download-logos.php