

## DIFFUSION RESTREINTE

# Version pédagogique du document



Villejuif le 8 janvier 2013

Le Délégué Général

A

Monsieur Philippe Volle

Directeur de l'Esiea

Objet : demande d'analyse du site [www.](http://www.) [redacted]

Je soussigné, [redacted] délégué général de l'association [redacted] donne l'autorisation à l'Esiea de mener une analyse du site [redacted]

[redacted]  
[Signature]  
[redacted]

**Ce rapport ne doit être diffusé qu'aux personnes ayant le besoin d'en connaître**

ESIEA	XXXXXXX
Philippe VOLLE	XXXXXXXXX

# DIFFUSION RESTREINTE

## Synthèse

Les vulnérabilités majeures suivantes ont été identifiées (par ordre de criticité) :

1. accès à une partie de l'espace d'administration sans authentification ;
2. flux réseau non chiffré ;
3. possibilité de lister le contenu des répertoires ;
4. nombre de tentatives de connexions non limité ;
5. cookies de session non sécurisés ;

Ces 5 vulnérabilités sont liées à des erreurs de configuration de service ou de conception du site.

La vulnérabilité la plus critique autorise l'accès à un espace d'administration du site sans aucune authentification au préalable. Un utilisateur mal intentionné peut donc modifier le site en production et ainsi, porter atteinte à l'image des organismes partenaires (E-réputation).

Ce document décrit la méthodologie exploitée. Pour chaque vulnérabilité découverte, une information est fournie permettant de couvrir le risque associé. Cette information est présentée avec le formalisme suivant :

- **recommandations X :** correction d'une vulnérabilité majeure
- **conseils X :** correction d'une vulnérabilité mineure
- commentaires : explication ou description simples

# DIFFUSION RESTREINTE

## Analyse de l'environnement du site

### Nom de domaine :

domain: XXXXXXXXXX	country: FR	notify: tech@ovh.net
status: ACTIVE	phone: +33 8 99 70 17 61	registrar: OVH
hold: NO	fax-no: +33 3 20 20 09 58	changed: 11/10/2006 tech@ovh.net
holder-c: E11067-FRNIC	e-mail: support@ovh.net	anonymous: NO
admin-c: E11067-FRNIC	website: http://www.ovh.com	obsoleted: NO
tech-c: OVH5-FRNIC	anonymous: NO	source: FRNIC
zone-c: NFC1-FRNIC	registered: 21/10/1999	
ns1-id: NSL53464-FRNIC	source: FRNIC	nic-hdl: E11067-FRNIC
registrar: OVH		type: ORGANIZATION
anniversary: 29/11	nic-hdl: OVH5-FRNIC	contact: [REDACTED]
created: 29/11/2011	type: ROLE	address: [REDACTED]
last-update: 29/11/2011	contact: OVH NET	address: [REDACTED]
source: FRNIC	address: OVH	address: [REDACTED]
	address: 140, quai du Sartel	country: [REDACTED]
ns-list: NSL53464-FRNIC	address: 59100 Roubaix	phone: [REDACTED]
nserver: dns20.ovh.net	country: FR	e-mail: [REDACTED]
nserver: ns20.ovh.net	phone: +33 8 99 70 17 61	registrar: OVH
source: FRNIC	e-mail: tech@ovh.net	changed: 29/11/2011 nic@nic.fr
	trouble: Information: http://www.ovh.fr	anonymous: NO
registrar: OVH	trouble: Questions: mailto:tech@ovh.net	obsoleted: NO
type: Isp Option 1	trouble: Spam: mailto:abuse@ovh.net	source: FRNIC
address: 2 Rue Kellermann	admin-c: OK217-FRNIC	
address: ROUBAIX	tech-c: OK217-FRNIC	

**Commentaires :** le nom de domaine « xxxxxxxxxx » a été acheté chez OVH. Les champs relatifs au demandeur sont renseignés (cf. lignes surlignées).

**Conseil 1 :** si l'anonymisation des enregistrements de contact est souhaitée, il suffit de la demander auprès du bureau d'enregistrement de domaines - « registrar » (OVH).

### Hébergement

```
XXXXXXXXXX      IN      A
XXXXXXXXXX.      85566  IN      A      XXX.XXX.33.3

3.33.186.213.in-addr.arpa.  IN      PTR
3.33.186.213.in-addr.arpa. 86399 IN      PTR      cluster015.ovh.net.
```

**Commentaires :** Le service est hébergé sur un serveur mutualisé par la société OVH (cluster015.ovh.net). Ce serveur héberge plusieurs milliers d'autres domaines (vérification sur le site « yougetsinal.com »)

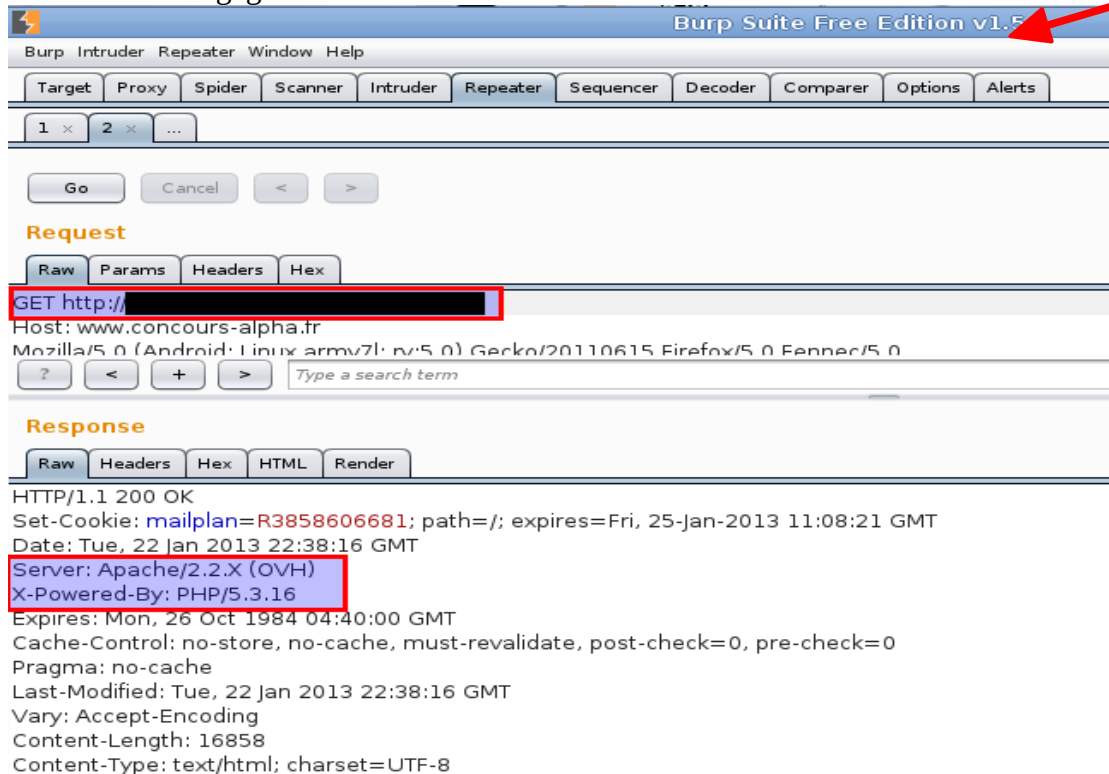
Au sein de ce serveur, l'aiguillage sur les autres domaines est réalisé par analyse de l'en-tête de la requête HTTP (virtualhosting).

Le serveur n'appartenant pas au propriétaire du site « xxxxxxxxxx », il ne peut être pris en compte dans la cible de l'étude. L'analyse de la sécurité du système d'exploitation et du serveur WEB est donc écartée.

**Seule l'analyse du contenu WEB lié au domaine « xxxxxxxxxx » peut être réalisée.**

# DIFFUSION RESTREINTE

Pour information, une analyse passive permet de déterminer que le serveur WEB est un apache 2.2 intégrant le module de langage PHP 5.3.16



## Analyse du site

### Fichiers disponibles en téléchargement

Commentaires : En analysant les métadonnées de quelques fichiers disponibles sur le site web, il est possible d'extraire des informations sur l'identité des auteurs.

Exemple sur des fichiers de type :

- documents PDF ;images Adobe XMP ;
- images Adobe PSD.

```
Create Date      : 2012:11:23 14:26:58+01:00
Modify Date     : 2012:11:23 14:26:58+01:00
Title           : CP20-11-2012 :
Creator        : PDFCreator Version 0.9.8
Author         : [REDACTED]
```

Une recherche sur les réseaux sociaux professionnels permet de rapidement retrouver certains profils.

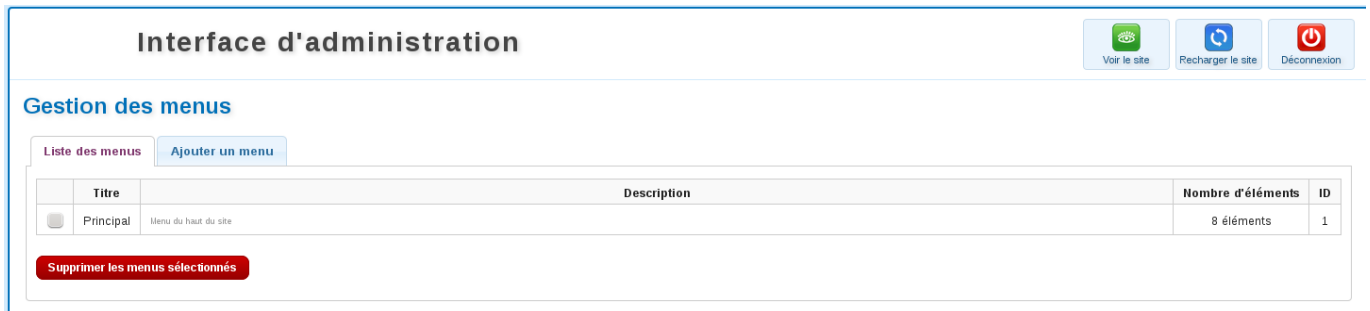
### Conseil 2 :

Afin d'éviter toute fuite d'informations, il est possible d'utiliser des applications supprimant les métadonnées des fichiers (FileMind, QuickFix). Le paramétrage correct des logiciels bureautiques permet aussi d'éviter cette fuite.

# DIFFUSION RESTREINTE

## Recherche d'entrées de site complémentaires

Commentaires : En exploitant la technique de « fuzzing » (recherche arbitraire) à partir d'une base de connaissance générique dédiée aux sites WEB, l'URL « /admin/menu.php » est apparue comme exploitable. Elle correspond à la page suivante :



**Interface d'administration**

Voir le site Recharger le site Déconnexion

**Gestion des menus**

Liste des menus Ajouter un menu

	Titre	Description	Nombre d'éléments	ID
<input type="checkbox"/>	Principal	Menu du haut du site	8 éléments	1

Supprimer les menus sélectionnés

Cette URL d'accès à l'interface d'administration (/admin/menu.php) est trop représentative. Elle est donc testée systématiquement par les outils de « fuzzing ».

**Conseil 3** : déplacer le répertoire contenant les pages d'administrations afin que l'URL d'accès ne soit pas représentative.

Commentaire : L'accès direct à l'interface d'administration constitue une vulnérabilité majeure. Le site devrait afficher une page de contrôle d'accès dès qu'une URL relative à sa zone d'administration est demandée.

**Recommandation 1** : activez l'authentification sur l'ensemble de la zone d'administration.

Commentaire : En cliquant sur l'icône « déconnexion », la page suivante apparaît :



**Accès à l'interface d'administration**

Identifiant :

Mot de passe :

S'identifier

Site créé avec Katapult 3.2, un produit conçu et géré par Créateur d'Image

Les informations contenues dans cette page permettent de récupérer le nom du moteur du site (Katapult 3.2) et la société éditrice de ce dernier (Créateur d'image). « Katapult » est un outil de gestion de contenu (CMS) générique. La connaissance du moteur et de sa version permet de récupérer sur les sites dédiés les vulnérabilités déjà référencées.

**Conseil 4** : supprimer les informations liées au nom et à la version du CMS.

# DIFFUSION RESTREINTE

Commentaires : L'analyse de l'URL de la page d'authentification montre que celle-ci n'est pas chiffrée. Les identifiants de connexion transitent en clair sur les réseaux. Ils peuvent être interceptés par un usager malveillant.

**Recommandation 2** : activer le chiffrement des flux sur la page d'authentification ainsi que sur toute la zone d'administration.

## Recherche d'identifiants valides

Commentaires : plusieurs essais de connexion avec différents couples (login,password) montrent que le nombre de tentatives n'est pas limité. Les outils de test automatique d'identifiants peuvent ainsi être exploités sans contrainte. Cette vulnérabilité vise la page d'authentification pour l'administration du site.

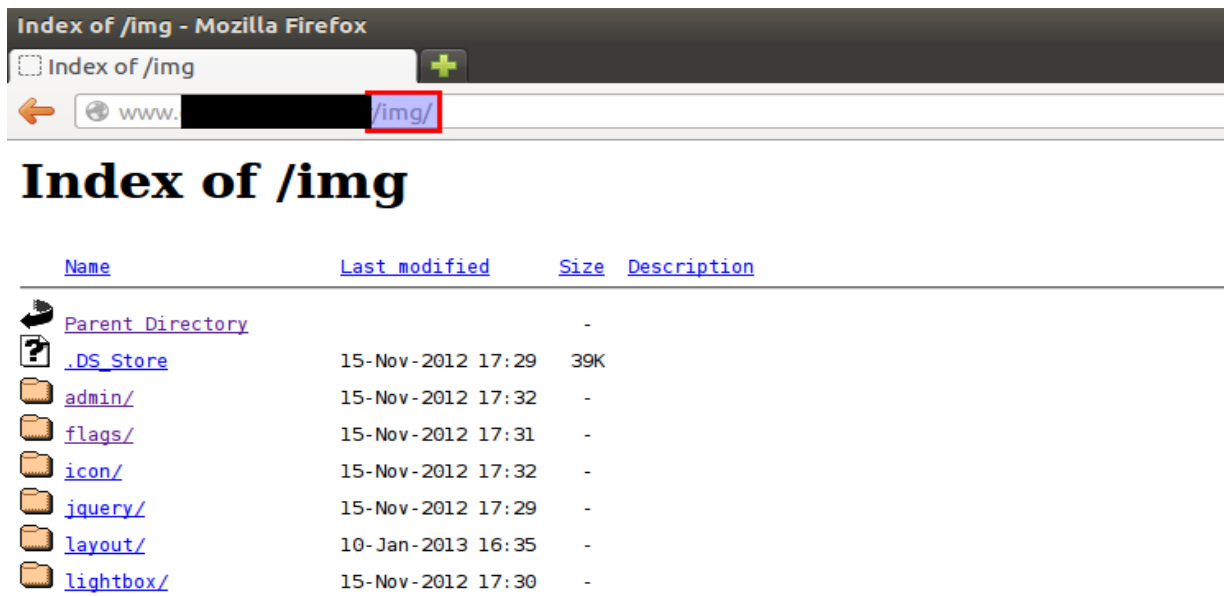
Il apparaît qu'elle est aussi présente sur la page d'authentification des clients.

**Recommandation 3** : activez un système permettant de limiter le nombre de tentatives de connexion à la fois sur la zone d'administration et sur le formulaire d'authentification des clients.

Il est possible par exemple d'intégrer un « captcha » qui doit être validé après un certain nombre d'essais de connexion infructueux. Cette méthode peut parfois être contournée par les robots de recherche si la technique du « captcha » n'est pas assez élaborée. Dans ce cas, on préférera la méthode qui consiste à activer un dispositif interdisant toute nouvelle connexion pendant un temps donné dès que le nombre d'essais infructueux a atteint une valeur définie.

## Récupération de la structure du site

Commentaire : En utilisant l'URL d'un répertoire du site, il est possible d'en afficher son contenu (ex. : avec un répertoire d'images :



# DIFFUSION RESTREINTE

De cette manière il est possible d'extraire de proche en proche la totalité de la structure du site. Cela permet souvent de récupérer des fichiers non prévus d'être diffusés (fuite d'information).

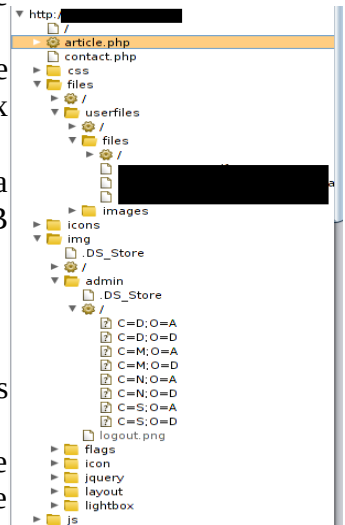
**Recommandations 4 :** bloquer la possibilité de lister les répertoires du site. Le blocage du parcours de répertoires d'un service WEB est possible selon deux méthodes :

- configurer le serveur WEB de manière à ce qu'il applique globalement la restriction sur l'ensemble du site. Exemple pour un serveur WEB APACHE :

```
<Directory"/var/www">  
    Options -Indexes  
</Directory>
```

- insérer dans les répertoires à protéger un fichier « .htaccess » définissant les restrictions à appliquer sur ce répertoire.

L'association des deux méthode permet par exemple de restreindre de manière globale tout en laissant la possibilité de lister un répertoire particulier (zone de téléchargement).



## Protection de l'internaute

**Commentaires :** le site délivre à chaque internaute un cookie de session non sécurisé. L'exploitation de cette faiblesse via l'exécution de script « Javascript » (« Cross-Site Scripting ») ou via l'écoute des trames réseau non chiffrées permet à un attaquant distant d'usurper la session d'un utilisateur légitime afin d'effectuer des actions sur le site avec ses privilèges.

**Recommandation 5 :** Sécuriser la gestion des cookies pour l'ensemble du site.

Lors de la description du cookie, il est possible de spécifier des options de gestion. Les deux options (drapeaux) « HttpOnly » et « Secure » permettent de sécuriser le cookie. Le drapeau « HttpOnly » permet d'éviter la manipulation du cookie au moyen de scripts locaux (« Javascript »). Le drapeau « Secure » permet d'éviter au cookie de transiter dans un flux réseau non chiffré (cf. Recommandation 2). La copie d'écran suivante montre que le cookie « mailplan » dont la valeur est « R363120753 » ne possède aucune des deux options de protection.

