Le Terrible Audit de Sécurité

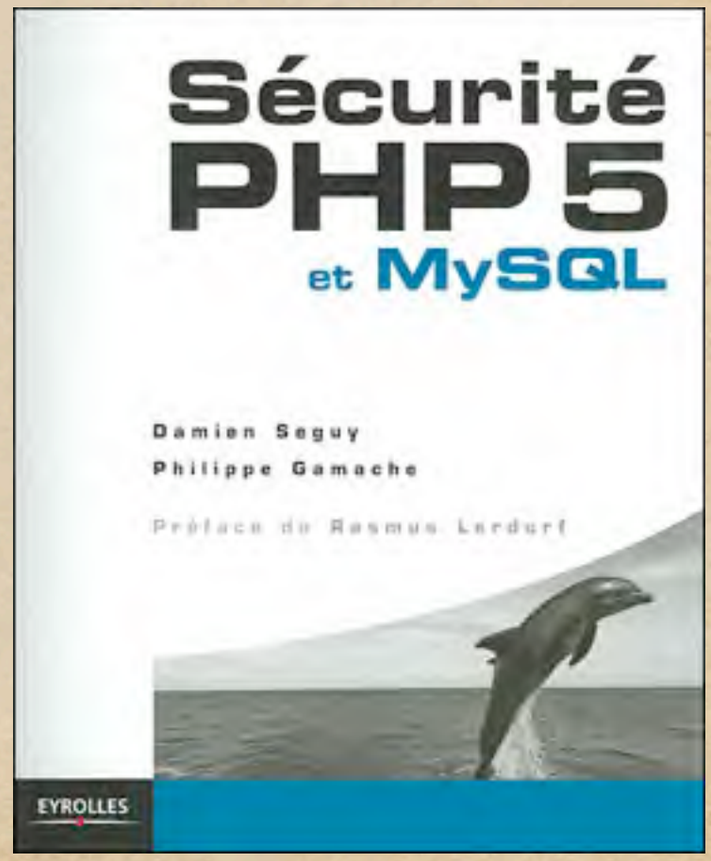
Ordre du jour

- Identifier les objectifs de sécurité
- Préparer un référentiel
- Vérifier la sécurité de son code

Qui parle?

- Damien Seguy
- Verbicruciste
- Alter Way Consulting

  L'expertise à coeur ouvert
- damien.seguy@alterway.fr



Référentiel de sécurité

Référentiel de sécurité

- Rappels du métier
- Liste des risques et vecteurs
- Matrice de sécurité
- Liste des détails des points de sécurité
- Références

Référentiel sécurité

- Liste des risques
  - Destruction, modification, lecture
  - DOS, détournement, image
- Liste des vecteurs
  - XSS, CSRF, injections, remplacement

Matrice de sécurité

	DOS	Destruction	Image
XSS			X
CSRF	X	X	X
headers	X		X

Points de sécurité

- Nom du point
- Description
- Risques courus
- Exemples et anti-exemples
- Méthode de vérification dans le code : automatique, manuel, méthode

Références

- OWASP
- PCI
- HIPAA
- ISO-27002
- ESSRII
- FISMA
- BASELII
- SOX

TOP 10 OWASP

- Injections
- XSS
- Session et identification
- Accès direct aux objets
- CSRF
- Configuration
- Stockage chiffré
- Restriction d'URL
- Couche de transport
- Redirections

TOP 10 OWASP

- Injections
- XSS
- Session et identification
- Accès direct aux objets
- CSRF
- Configuration
- Stockage chiffré
- Restriction d'URL
- Couche de transport
- Redirections

PIMCORE

- CMS
- PHP, MySQL
- Zend Framework
- Meilleur Projet OS Packt
- http://www.pimcore.org/

Méthode

- Prendre un point OWASP
- Trouver le point d'entrée
- Fouiller le code source
- Valider manuellement le point

Injections

Injections

- Points d'entrées SQL
  - mysql_query, pdo->query
    - query, execute, fetchAll, delete, update, select
- Injection de variables
  - getParams, getParam, $_GET/POST

Recherche

- Grep
  - Rapide, efficace
  - Trouve trop
- Tokenizer
  - PHP, sémantique
  - Implique le tri et la reconstruction

Tokenizer

```
<?php print ("hello $world! "); ?>
```

```
[1] => Array
    (
        [0] => 266
        [1] => print
        [2] => 1
    )

[2] => Array
    (
        [0] => 370
        [1] =>
        [2] => 1
    )

[3] => (
[4] => "
[5] => Array
    (
        [0] => 314
        [1] => hello
        [2] => 1
    )
```

```
[6] => Array
    (
        [0] => 309
        [1] => $world
        [2] => 1
    )

[7] => Array
    (
        [0] => 314
        [1] => !
        [2] => 1
    )

[8] => "
[9] => )
[10] => ;
```

```
[1] => Array
    (
        [0] => token PHP
        [1] => code PHP
        [2] => ligne
    )
[2] => "
```

```php
$this->db->fetchAll
  ("SHOW COLUMNS FROM documents_permissions");

$this->db->update
  ("documents_permissions", $data,
  "id='" . $this->model->getId() . "'");

$this->db->insert
  ("documents_permissions", array());

$this->db->delete
  ("documents_permissions",
   "id=" . $this->model->getId());

$this->db->fetchRow
  ("SELECT * FROM dp WHERE id = ?",
   $this->model->getId());
```

```
$data = json_decode($this->_getParam
("data"));
if (!empty($data->id)) {
    $nodes[] = $data;
} else {
    $nodes = $data;
}
//loop through store nodes  = documents
if (is_array($nodes)) {
    foreach ($nodes as $node) {
```

Bilan

- Pas de protections au niveau des requêtes SQL
- Transmission directe depuis le contrôleur au modèle
- Utilisation de valeurs sans contrôle

Bilan

- Pas de protections au niveau des requêtes SQL
- Transmission directe depuis le contrôleur au modèle
- Utilisation de valeurs sans contrôle

Sessions

Session et identification

- Utilisation des sessions standards
- Nécessite un arrimage plus fort
- Durée de vie courte recommandée
- User-Agent, IP, LANGAGE-ACCEPT, token aléatoire à mettre en session + via le Web

Bílan

- Utilisation standard des sessions PHP
- Pas de mécanisme spécifique d'arrimage

Bilan

- Utilisation standard des sessions PHP
- Pas de mécanisme spécifique d'arrimage

Redirections

Redirections

- Redirections mal validée
- Méthodes redirect ou _redirect
- Idéalement, interne au site, et fixe

Points d'entrée

```
$this->_redirect("/admin/");
$this->_redirect("/admin/login/");

$this->_redirect("/admin/login/
?auth_failed=true&inactive=".
$userInactive);
```

Bilan

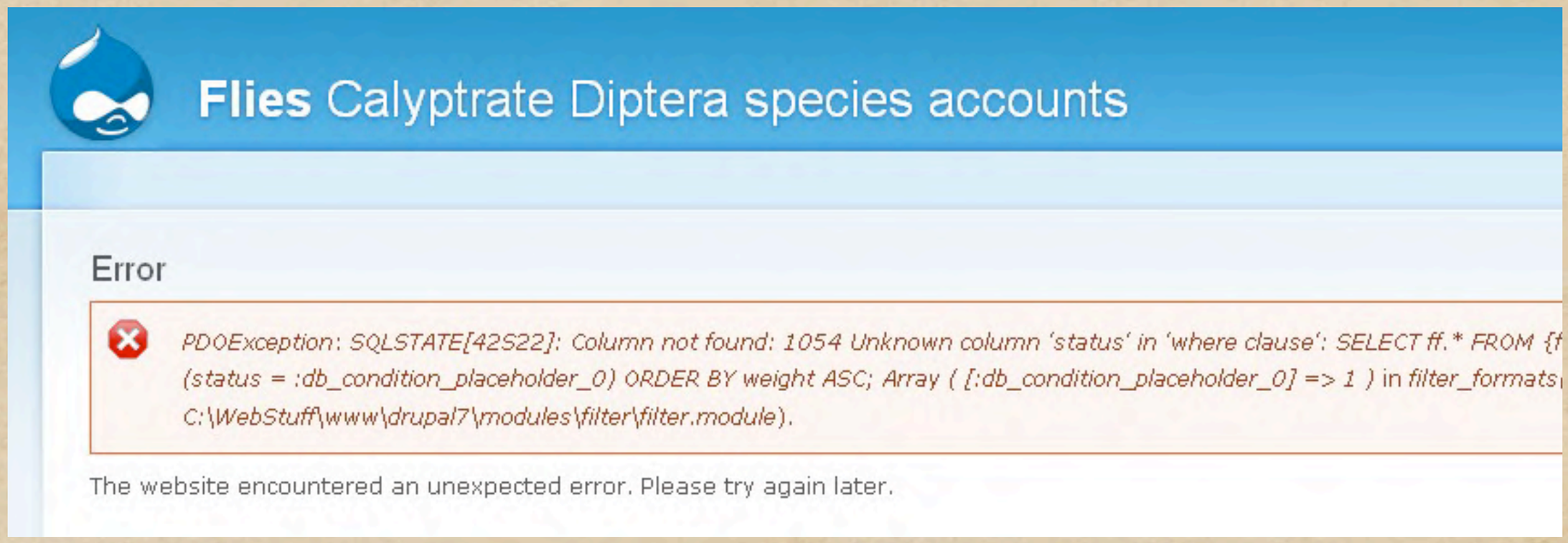
- Validation systématique
- Bonne discipline

Bilan

- Validation systématique
- Bonne discipline

Accès direct aux objets

Accès direct aux objets



Accès direct aux objets

- http://www.elysee.fr/president/les-actualites/les-actualites.4.html
- http://www.decathlon.fr/tee-shirt-manches-longues-id_8152082.html
- Les identifiants sont des auto_increment...

Par fois, c'est drôle

- http://www.decathlon.fr/surtout-n-allez-pas-a-l-afup-id_8152082.html

```
public function deleteAction() {
  $success = false;
   $document = Document::getById
        ($this->_getParam("id"));
   $document->getPermissionsForUser
        ($this->getUser());
   if ($document->isAllowed("delete")) {
      Element_Recyclebin_Item::create
            ($document, $this->getUser());
   } else {
      Logger::debug //****
   }
  $this->_helper->json(array
            ("success" => $success));
}
```

Accès direct aux objets

- Ne jamais exposer ses structures internes sur le site Web
- Faire une traduction, et stocker les vraies valeurs dans la session

Bilan

- Accès direct aux objets

Bilan

- Accès direct aux objets

Accès aux URL

- Les URL doivent bien porter des vérifications d'accès (type ACL)

```php
<?php
class Admin_AssetController
  extends Pimcore_Controller_Action_Admin {

    public function init() {
        parent::init();

        // check permissions
        $notRestrictedActions = array("get-i
        if (!in_array($this->_getParam("acti
            if (!$this->getUser()->isAllowed

                $this->_redirect("/admin/log
                die();
            }
        }
    }
?>
```

Accès aux URL

- 16 contrôleurs d'administration
- 16 dérivation de
  Pimcore_Controller_Action_Admin
- 7 utilisations de /admin/login
- Vérifier l'héritage ET parent::init

Bílan

- Pas de protection particulière
- Évite les outils ZF

Bilan

- Pas de protection particulière
- Évite les outils ZF

CSRF

CSRF

- Utilisation de Zend_Form et l'anti-csrf ?
  - Non
- Test sur /admin/login
  - Pas de vérification de token
- Sur deleteAction? Non
- Pas moyen de surveiller facilement

Bílan

- Pas de protection particulière
- Évite les outils ZF

Bilan

- Pas de protection particulière
- Évite les outils ZF

XSS

XSS

- Injection de code HTML/Javascript
- Etudier les Vues
  - Etudier les contrôleurs
- Grosse partie Javascript de présentation : protection par encodage

```
die($document->getPath() .
      $document->getKey());

$this->removeViewRenderer();

$this->_helper->json(
    array("docTypes" => $docTypes));
```

```
echo Zend_Json::encode(
    array( "error" => "plugin_dir_error" ));

readfile(PIMCORE_DOCUMENT_ROOT .
  $image->getThumbnail($thumbnail));
```

Bilan

- Peu de suivi des conventions Zend Framework
- Des die
- Utilisation intensive de javascript
- Difficile à auditer

Bilan

- Peu de suivi des conventions Zend Framework
- Des die
- Utilisation intensive de javascript
- Difficile à auditer

Injections		CSRF	
XSS		URL	
Sessions		Redirections	
Accès direct			

Récapitulatif

- Rédigez un référentiel
- Convertissez-le en code à éviter / recommander
- Vérifiez le vous-même

Merci