Sécurité sous PHP

Ousmane NDIAYE

Module PHP-MySQL

Licence TDSI

- Introduction
- Identification
- Les attaques
- Les configurations
- Injections SQL
- Cross Site Scripting
- Détournement de session
- Protéger les dossiers

Introduction

- La sécurisation d'une application s'appuie sur plusieurs briques :

– l'identification : le login de l'utilisateur est vérifié ;

– l'habilitation : l'utilisateur doit disposer des droits adéquats pour accéder à un module ou à un sous-ensemble de données définies;

– la cohérence : les données introduites dans le système doivent être conformes à ce qui est attendu ;

– la sécurisation générale : la mise en œuvre de mécanismes adaptés rend les attaques plus difficiles à mener.

Identification

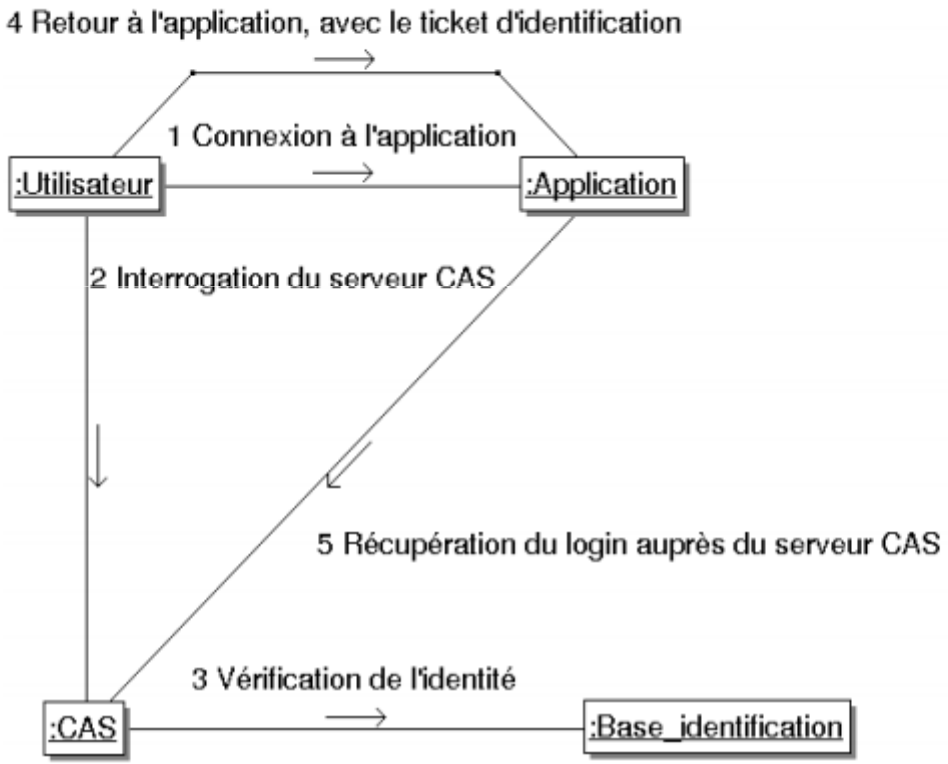
- Trois grands modes d'identification:

– La base de données contient une table Login, dont un des champs correspond au mot de passe utilisé.

– L'identification des utilisateurs est réalisée à partir d'une base de données centrale (Annuaire) et peut être réutilisée entre différentes applications.

– L'identification des utilisateurs est sous-traitée à une application dédiée à cet effet, un serveur CAS (Central Authentication Service - service d'authentification centralisé), qui traite de manière unique toutes les demandes de vérification de login.

Identification basée sur un serveur CAS



Identification

- Fonctionnement de l'interrogation du serveur CAS.

1 - L'utilisateur se connecte à l'application.

2 - L'application a besoin d'identifier l'utilisateur : elle redirige le navigateur vers le serveur CAS qui affiche un écran de saisie du login/mot de passe, en mode sécurisé via le protocole HTTPS.

3 - Au retour de la saisie du login/mot de passe, le serveur CAS vérifie l'identification auprès de sa base locale (annuaire LDAP, base de données...). Puis retourne (en mode HTTPS) au navigateur un cookie de session, spécifique au serveur CAS.

4 - Le serveur CAS redirige le navigateur de l'utilisateur vers l'application en lui joignant un ticket de session, utilisable une seule fois.

5 - L'application interroge le serveur CAS en lui fournissant le ticket de session et récupère, en retour, l'identifiant (le login) de l'utilisateur.

Identification

- La bibliothèque phpCAS
  - La communauté ESUP-Portail a mis au point une bibliothèque PHP pour gérer la communication avec des serveurs CAS.
  - Cette bibliothèque peut être téléchargée sur

http://www.ja-sig.org/wiki/display/CASC/phpCAS

Les attaques

- Contrairement aux applications basées sur un "client lourd", le programmeur ne maîtrise pas ce que l'internaute lui envoie comme information.
- N'importe qui peut créer des requêtes et les envoyer vers un serveur.
- Ces requêtes peuvent contenir n'importe quelle valeur et pas uniquement celles proposées dans l'interface.

Les attaques

- Attaques les plus connues:
  - Attaque par injection de code SQL
  - Attaque par cross-site scripting
  - Détournement de session.

Les configurations

- Apache

– Installation de PHP comme un module CGI

  - Chaque invocation d'un script php entraîne le démarrage d'un processus
  - Un binaire PHP est exécuté à chaque interprétation d'un script PHP
  - Le binaire peut être utilisé comme un interprête à partir de la ligne de commande

– Installation de PHP comme un module Apache

  - Le module PHP est démarré avec le serveur Apache et c'est Apache qui se charge des invocations de l'interprête à l'intérieur de son propre processus
  - Plus d'efficacité.

Les configurations

- PHP

– Le fichier de configuration de PHP (php.ini) est un fichier de propriétés:

  - name=value

– L'endroit où il se trouvent dépend des options de compilation

  - Dans le répertoire d'installation
  - Dans c:\WINNT pour windows 2000

Les configurations

- PHP
  - Directives
    - Plusieurs catégories de directives
      - Options pour le langage
      - Options pour la gestion des ressources
      - Options pour la gestion des variables
      - Options pour l'organisation des fichiers
      - Options pour l'upload de fichiers
      - Options pour le debugging

Les configurations

- PHP

– Pour le langage

  - short_open_tag et asp_tags pour les balise de début et de fin de scripts

– Pour les ressources

- memory_limit="8M"
  – Permet de limiter la mémoire utilisée pour l'exécution d'un script
  – Utile pour éviter à des scripts mal écrits d'écrouler le serveur
- max_execution_time=30
  – Temps maximum d'exécution d'un script
  – Pour éviter qu'un script consomme toutes les ressources CPU

Les configurations

- PHP

– Pour la gestion des erreurs

  - error_reporting = E_ALL
    – les erreurs à considérer
  - display_errors = on
    – Affiche les erreurs dans le navigateur
    – Mettre à off en production pour des raisons de sécurité
  - log_errors = off
    – Logging des erreurs dans un fichier
    – Mode On recommandé en production
  - error_log = filename
    – Fichier dans lequel les erreurs sont enregistrées

Les configurations

- PHP
  - Pour les données
    - track_vars= "on"
      - les variables d'env, get, post, cookies, server sont enregistrées dans les tableaux $_ENV, $_GET ...
      - toujours activé depuis 4.0.3
    - default_mimetype="text/html"
      - Type mime par défaut du résultat de l'exécution
    - default_charset ="iso88591"
      - Jeu de caractères par défaut
    - arg_separator.{input,output}='&'
      - Caractère utilisé pour séparer les arguments dans les urls
    - register_globals= "on" ou "off"

Les configurations

- PHP

– Pour les données

- Il est possible de forcer l'exécution d'un script avant ou après chaque script PHP.
  - auto_prepend_file
  - auto_append_file
- magic_quotes_gpc=on
  - Backslash automatiquement les ' " et \ dans les paramètres get, post et cookies.

Les configurations

- PHP
  - Pour les fichiers
    - include_path "/path1:/path2"
      - chemin de recherche des fichiers PHP pour les fonctions require() et include()
    - Doc_root
      - racine des fichiers PHP.
      - Si positionné, c'est le seul endroit où des fichiers PHP pourront être exécutés

Les configurations

- PHP
  - Pour le chargement (l'upload) de fichier
    - file_uploads = On
      - pour autoriser « l'upload » de fichiers
    - upload_tmp_dir string
      - le chemin vers lequel les fichiers sont transférés
    - upload_max_filesize 2M
      - la taille maximum des fichiers « uploadés »

Injections SQL

insertion de commandes SQL dans des données saisies au travers d'un formulaire

```
<? $user=$_POST['user']; $pass=$_POST['pass'];
  $query="SELECT * from users where uname='$user' AND upass='$pass'";
  $res=mysql_query($query); if (mysql_num_rows($res) >0 ) { $auth=1; …
…?>
```

Supposons $_POST['user'] = "admin' #"

Alors : $query = SELECT * from users where

uname='admin' #' AND upass="";

Cette requête retourne TOUJOURS une ligne !!!

Injections SQL

- Comment résister?
  - Config : Magic_quotes_gpc ON
    - admin ' # ➔ admin \' #
  - Protection locale : fonction mysql_escape_string ()
    - Ajoute des \ devant ', \, "
  - Contrôler les données fournies par l'utilisateur
  - Limiter et prévenir :
    - Ne jamais exposer le schéma de la base (dans les formulaires en particulier)
    - Ne pas afficher les erreurs
    - Limiter les droits de l'utilisateur qui accède à la base
    - Logger les requêtes

Cross Site Scripting

- Principe : insérer des balises html avec des scripts dans des données qui sont affichées par l'application

```
<?
        echo "votre recherche {$_POST['query']} a echoue <br>" ;
?>
```

- Dans le formulaire, on saisit :
  - "<script> alert("Coucou Bilou");</script>
  - Ou un script plus méchant !

Cross Site Scripting

- Comment résister?
  - Fonctions:
    - strip_tags() : retire TOUS les tags html d'une string
    - htmlspecialchars() : convertit les caractères spéciaux html en caractères affichables :
      - "<" ➔ &lt

```
<?php
$new = htmlspecialchars("<a href='test'>Test</a>", ENT_QUOTES);
echo $new;
// &lt;a href=&#039;test&#039;&gt;Test&lt;/a&gt;
?>
```

Détournement de session

- Pour pouvoir gérer la continuité de la connexion, les serveurs web mettent en place un mécanisme de session et transmettent au navigateur un identifiant de session, soit dans une variable, soit dans un cookie (cas le plus fréquent).
- Si un pirate récupère l'identifiant de session, il a alors la possibilité de faire exécuter du code en se faisant passer pour l'utilisateur.

Détournement de session

- il est fortement conseillé pour s'en protéger, de régénérer l'identifiant de session juste après l'identification de l'utilisateur.
- Pour ce faire, la fonction

  session_regenerate_id() est utilisée.

Protéger l'accès à certains dossiers

- Problème
  - Avec le principe du langage HTML, toute page est accessible nativement en indiquant le chemin complet d’accès.
  - Il est souhaitable de ne pas autoriser l’accès direct à certains dossiers comme celui qui contient les fichiers de paramètres ou ceux qui reçoivent des fichiers en téléchargement.

Protéger l'accès à certains dossiers

- Solution
  – Avec le serveur Web Apache, il suffit de créer un fichier nommé .htaccess à la racine du dossier à protéger et qui comprend les instructions

suivantes :

order deny,all

deny from all

– Ces deux lignes vont interdire l'accès direct au dossier depuis le navigateur.

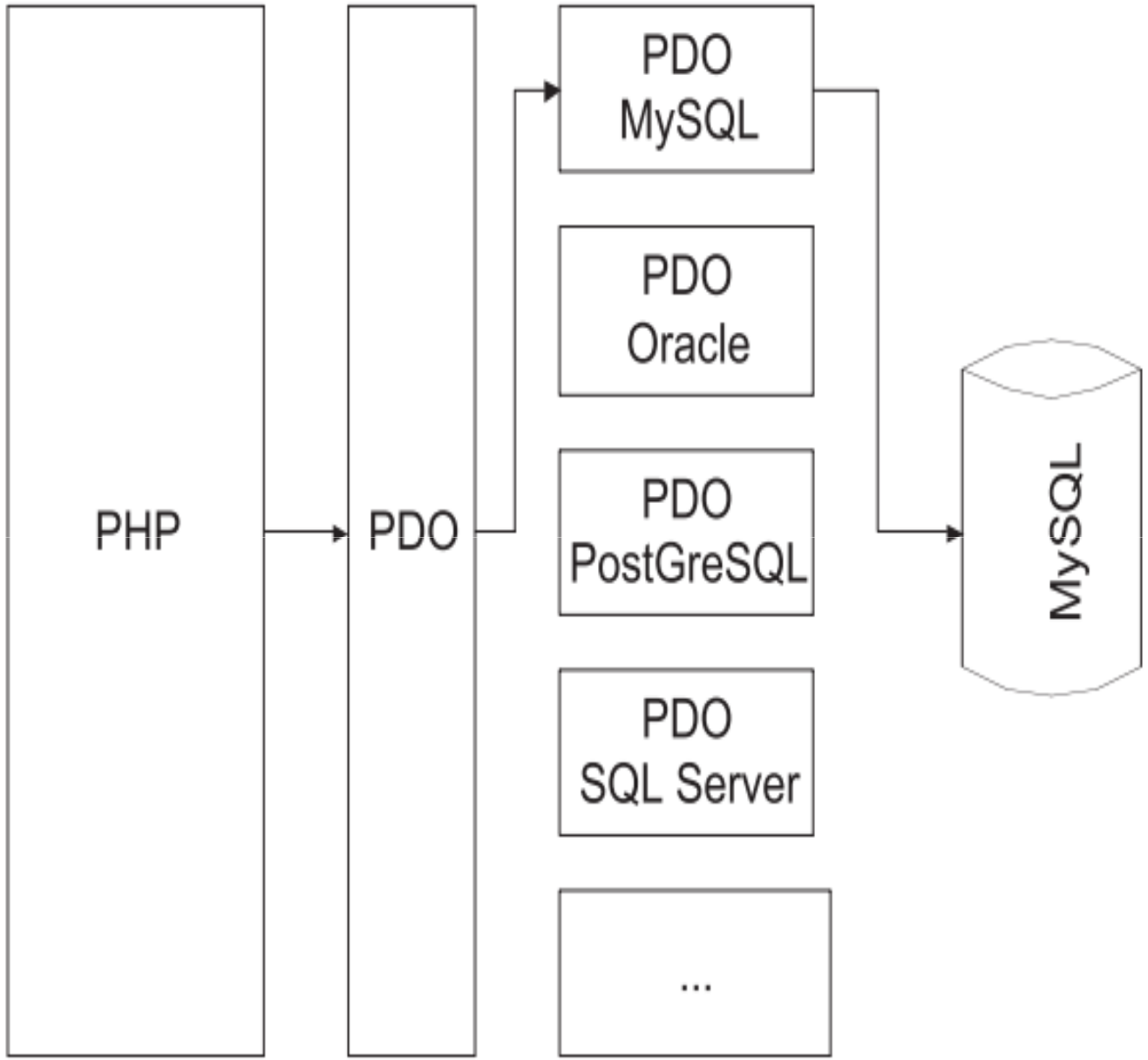
– Cela n'empêchera pas l'application d'y accéder par l'intermédiaire de la commande **include_once**.

TP

- PO PHP 5
- PDO (PHP Data Object): accès aux bases de données

Figure 18-1

Architecture des drivers PDO



- Biblio:

PROG° PHP 5 AVANCE (EYROLLES 2007).pdf