|  |
| --- |
| Mickaël BRENOIT | Michaël FUCHS  14/09/2017 |

|  |
| --- |
| UNIVERSITE DE HAUTE-ALSACE |
| Sécurisation bases de données |
| Mini-projet MIAGE M2 |



SOMMAIRE

[1. Présentation du mini-projet 2](#_Toc493173394)

[2. Création de la base de données 3](#_Toc493173395)

[2.1. Table « users » 3](#_Toc493173396)

[2.2. Table « accounts » 3](#_Toc493173397)

[2.3. Script SQL 3](#_Toc493173398)

[3. Les différentes failles traitées 4](#_Toc493173399)

[3.1. Les injections SQL 4](#_Toc493173400)

[3.1.1. Définition et comment les utiliser 4](#_Toc493173401)

[3.1.2. Comment se protéger 5](#_Toc493173402)

[3.1.3. Notre solution 5](#_Toc493173403)

[3.2. Cross-site scripting (XSS) 6](#_Toc493173404)

[3.2.1. Définition 6](#_Toc493173405)

[3.2.2. Comment éviter ce genre d’attaque 6](#_Toc493173406)

[3.2.3. Notre solution 7](#_Toc493173407)

[3.3. L’attaque dictionnaire et force brute 8](#_Toc493173408)

[3.3.1. Définition et comment s’en protéger 8](#_Toc493173409)

[3.3.2. Notre solution 8](#_Toc493173410)

[3.4. La faille « include » ou « remote file inclusion » 9](#_Toc493173411)

[3.4.1. Définition 9](#_Toc493173412)

[3.4.2. Comment éviter cette faille 9](#_Toc493173413)

[3.4.3. Notre solution 9](#_Toc493173414)

[3.5. La faille « input file … » 10](#_Toc493173415)

[3.5.1. Définition 10](#_Toc493173416)

[3.5.2. Les différentes protections 10](#_Toc493173417)

[3.5.3. Notre solution 11](#_Toc493173418)

# Présentation du mini-projet

Le mini-projet présenté dans ce rapport est le fruit de connaissances récoltées lors de nos recherches internet sur les différentes failles possibles sur un site internet. Il nous a été demandé de :

1. Créer une base de données qui contient deux tables :
   1. Une table « users » représentant les utilisateurs de notre application. Les utilisateurs auront un id, un login et un mot de passe.
   2. Une table « accounts » représentant les comptes bancaires que dispose un utilisateur. Les comptes auront un id, un type, un montant et une clé faisant référence à l’id de l’utilisateur à qui appartiennent les comptes.
2. Réaliser un formulaire en PHP qui se connecte à notre base de données et qui demande le login et mot de passe de l’utilisateur.
3. Rechercher les différentes failles importantes qui existent et les tester sur notre formulaire.
   1. Tester les failles « injections SQL » vues en cours
   2. Rechercher d’autres types de faille sur internet
4. Explorer les solutions sur le web et décrire au moins deux méthodes importantes de protection contre ces failles.
5. Illustrer les scénarios avec failles et sans failles.

# Création de la base de données

## Table « users »

La première table créée est « user ». Elle contient :

* Un champ « id » : identifiant unique d’un utilisateur, incrémenté automatiquement et non nul. C’est la clé primaire de cette table.
* Un champ « login » : pseudonyme de l’utilisateur, il est déclaré unique et non null
* Un champ « password » : mot de passe de l’utilisateur haché, non null.

De base, nous aurons deux entrées :

* Id : 1, login : mickael et password : md5(aA4\*7777)
* Id : 2, login : framboise et password : md5(strawberry)

## Table « accounts »

La seconde table créée est « accounts ». Elle contient :

* Un champ « id » : identifiant unique d’un compte, incrémenté automatiquement et non nul. C’est la clé primaire de cette table.
* Un champ « type » : intitulé du compte bancaire, unique et non null
* Un champ « amount » : montant représenté par un entier réel positif, non null
* Un champ « iduser » : identifiant de l’utilisateur qui détient ce compte, non null

De base, nous aurons quatre entrées :

* Id : 1, type : Livre bleu, amount : 1100 et iduser : 1
* Id : 2, type : Compte Courant, amount : 1600 et iduser : 1
* Id : 3, type : Livret Framboise 1, amount : 600 et iduser : 2
* Id : 4, type : Livret Framboise 2, amount : 750 et iduser : 2

## Script SQL

Image

# Les différentes failles traitées

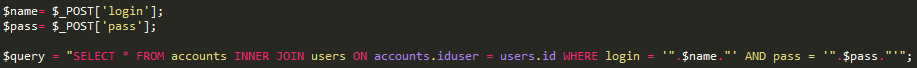
## Les injections SQL

### Définition et comment les utiliser

Les injections SQL (SQLi) se réfère à une attaque d'injection dans laquelle un attaquant peut exécuter des instructions SQL malveillantes qui contrôlent le serveur de base de données d'une application Web (également communément appelé système de gestion de base de données relationnelle - SGBDR). Étant donné qu'une vulnérabilité SQL Injection pourrait affecter n'importe quel site Web ou application Web qui utilise une base de données basée sur SQL, cette vulnérabilité est l'une des vulnérabilités les plus anciennes, les plus répandues et les plus dangereuses.

Pour exécuter des requêtes SQL malveillantes contre un serveur de base de données, un attaquant doit d'abord trouver une entrée dans l'application Web qui permet d’inclure une requête SQL. Un attaquant peut alors insérer une partie de code SQL qui sera incluse dans la requête SQL et s'exécuter en fonction du serveur de la base de données.

Le pseudo-code suivant du côté serveur sert à authentifier les utilisateurs sur l'application Web.



Le script ci-dessus est un exemple simple d'authentification d'un utilisateur avec un nom d'utilisateur et un mot de passe contre une base de données avec une table nommée utilisateurs et une colonne de nom d'utilisateur et de mot de passe. Le script ci-dessus est vulnérable à l'injection SQL, car un attaquant peut envoyer des entrées malveillantes de manière à modifier l'instruction SQL exécutée par le serveur de base de données. Un exemple simple d'une charge utile d'injection SQL pourrait être quelque chose d'aussi simple que le champ de mot de passe en password 'OR 1 = 1**.**

Cela entraînerait que la requête SQL suivante soit exécutée contre le serveur de base de données.

**SELECT id FROM users WHERE username=’username’ AND password=’password’ OR 1=1’**

Dans le cas où le contournement d'authentification est possible, l'application enregistrera probablement l'attaquant avec le premier compte à partir du résultat de la requête - le premier compte dans une base de données est habituellement un utilisateur administratif.

### Comment se protéger

Selon OWASP « Open Web Application Security Project (OWASP) est une communauté en ligne travaillant sur la sécurité des applications Web. Sa philosophie est d'être à la fois libre et ouverte à tous. Elle a pour vocation de publier des recommandations de sécurisation Web et de proposer aux internautes, administrateurs et entreprises des méthodes et outils de référence permettant de contrôler le niveau de sécurisation de ses applications Web. », la mise en place de trois défenses est obligatoire pour lutter contre les injections SQL.

Voici la liste des trois défenses :

* Utilisation des requêtes préparées
* Utilisation des procédures stockées
* Vérifier toutes les entrées utilisateurs

Les requêtes préparées garantissent qu'un attaquant ne peut pas modifier l'intention d'une requête, même si les commandes SQL sont insérées par un attaquant. Dans l'exemple de sécurité vu précédemment, si un attaquant devait entrer l'ID utilisateur de tom 'ou' 1 '=' 1, la requête paramétrée ne serait pas vulnérable et rechercherait un nom d'utilisateur qui correspondait littéralement à la chaîne entière tom 'ou' 1 '=' 1.

L’utilisation des procédures stockées est très similaire à l’utilisation des requêtes préparées. La seule différence entre les instructions préparées et les procédures stockées est que le code SQL pour une procédure stockée est défini et stocké dans la base de données elle-même, puis appelé à partir de l'application.

Vérifier toutes les entrées utilisateurs consiste à échapper les saisies des utilisateurs avant de les mettre dans une requête SQL. Pour cela on utilise des fonctions spéciales qui vont filtrer les données en prenant soin de virer les balises <elem></elem> ainsi que les apostrophes.

### Notre solution

Blabla

## Cross-site scripting (XSS)

### Définition

Cross-site Scripting, également appelé XSS, est un moyen de contourner le concept SOP. En anglais SOP signifie « standard operating procedure (SOP). D’après Wikipédia, « *SOP est une procédure de sécurité qui décrit comment affronter une menace et comment agir pour en diminuer le risque. Elle décrit les étapes à suivre pour réduire la possibilité qu'un incident se produise et s'il se produit ce qu'il faut faire pour en limiter les conséquences.* »

Chaque fois que le code HTML est généré dynamiquement et que l'entrée de l'utilisateur n'est pas « désinfectée » et qu'elle se reflète sur la page, un attaquant peut insérer son propre code HTML/JavaScript. Dans ce cas, un attaquant peut facilement insérer un code JavaScript. Ce faisant, l'attaquant peut accéder à d'autres pages sur le même domaine et peut lire des données comme les « CSRF-Tokens » ou les « cookies » définis.

Si les « cookies », qui contiennent généralement des informations d'identifiant de session, peuvent être lus par le JavaScript, l'attaquant peut les utiliser sur son propre navigateur et se connecter à l'application Web en tant que victime. Si cela ne fonctionne pas, l'attaquant peut encore lire des informations privées à partir des pages, telles que les jetons « CSRF » et faire des demandes au nom de l'utilisateur. En somme, usurper l’identité d’une personne.

### Comment éviter ce genre d’attaque

Dans certains cas, il pourrait suffire de coder les caractères spéciaux HTML, tels que l'ouverture et la fermeture des balises. Dans d'autres cas, un codage d'URL correctement appliqué est nécessaire. Les liens devraient généralement être refusés s'ils ne commencent pas par un protocole appartenant à une « whitelist » tel que « http: // » ou « https: // », empêchant ainsi l'utilisation de schémas URI tels que « javascript: // ».

Bien que la plupart des navigateurs Web modernes possèdent un filtre XSS intégré, ils ne doivent pas être considérés comme une alternative à la désinfection. Ils ne peuvent pas attraper toutes sortes d'attaques de scripts entre sites et ne sont pas stricts, sinon cela empêcherait certaines pages de se charger correctement. Le filtre XSS d'un navigateur Web ne doit être qu'une «seconde ligne de défense», la première étant la barrière qu’impose le développeur grâce aux filtrages des entrées utilisateurs.

Pour contrer ce genre d’attaque, le développeur peut utiliser par exemple la fonction « filter\_var() » qui permet de filtrer les données selon un filtrage spécifique. Heureusement, PHP met à disposition des filtres prêts à l’emploi qui sont efficaces et optimisés que nous allons voir dans la partie ci-dessous

### Notre solution

Blabla

## L’attaque dictionnaire et force brute

### Définition et comment s’en protéger

Ce genre d’attaque consiste simplement à tester chaque mot du dictionnaire pour un « login » donné. Les attaques de dictionnaires fonctionnent parce que de nombreux utilisateurs particulier ou en entreprise insistent sur l'utilisation de mots ordinaires comme mots de passe. Les attaques de dictionnaires sont rarement couronnées de succès contre les systèmes qui utilisent plusieurs mots et échouent contre les systèmes qui utilisent des combinaisons aléatoires de majuscules et minuscules mélangées avec des chiffres. Contre ces systèmes, la méthode d'attaque de la force brute (dans laquelle chaque combinaison possible de caractères et d'espaces est essayée jusqu'à une certaine longueur maximale) peut parfois être efficace, même si cette approche peut prendre beaucoup de temps pour produire des résultats.

La réussite d’un assaut de type dictionnaire peuvent être proche de zéro en limitant le nombre de tentatives autorisées dans une période de temps donnée et en choisissant judicieusement le mot de passe. Par exemple, si seulement trois tentatives sont autorisées, une période de 15 minutes doit s'écouler avant que les trois tentatives suivantes ne soient autorisées, et si le mot de passe est un énorme mélange de lettres et de chiffres sans importance, un système peut être rendu immunisé contre les attaques de dictionnaires et pratiquement immunisées contre les attaques de force brute.

### Notre solution

Blabla

## La faille « include » ou « remote file inclusion »

### Définition

L'inclusion de fichiers à distance (RFI) fait référence à une attaque d'inclusion dans laquelle un attaquant peut amener l'application Web à inclure un fichier distant (celui de l’attaquant). Les conséquences d'une attaque RFI réussie incluent la divulgation des informations du serveur, de la base de données, des personnes…

L'inclusion de fichiers à distance (RFI) se produit habituellement, lorsqu'une application reçoit le chemin d'accès d’un fichier dynamiquement par la variable « $\_GET[‘nom\_du\_fichier’] ». Cela permettrait d'envoyer une URL externe à l'instruction « include ».

### Comment éviter cette faille

La meilleure façon d'éliminer les vulnérabilités à l'inclusion de fichiers distants (RFI) est d'éviter d'inclure dynamiquement des fichiers en fonction de l'entrée de l'utilisateur. Si cela n'est pas possible, l'application devrait conserver une « whitelist » des fichiers pouvant être inclus afin de limiter le contrôle de l'attaquant sur ce qui est inclus.

En outre, dans le cas de PHP, la plupart des configurations PHP modernes sont configurées avec « allow\_url\_include » désactivé, ce qui n'autoriserait pas les utilisateurs malveillants à inclure des fichiers distants. Cela étant dit, l'inclusion de fichiers locaux (LFI) serait toujours possible.

### Notre solution

Blabla

## La faille « input file … »

### Définition

La vulnérabilité d’ « upload » de fichiers est un problème majeur avec les applications basées sur le Web. Sur de nombreux serveurs Web, cette vulnérabilité permet à un attaquant d’ « uploader » un fichier avec un code malveillant qui peut être exécuté sur le serveur. Un attaquant pourrait être en mesure de mettre une page d'hameçonnage dans le site Web.

Dans la plupart du temps, l’attaquant va utiliser cette faille en « uploadant » un fichier avec double extension comme « mon\_image.php.jpeg ». On devine ainsi que le fichier est bien un script PHP et non une image JPEG mais lors de l’ « upload », sans contre-mesure, le fichier est considéré comme une image.

L'attaquant peut ainsi révéler des informations internes du serveur Web à d'autres et, dans certaines occasions, des données sensibles peuvent être acquises comme celles existantes au sein d’une base de données, par des personnes non autorisées.

### Les différentes protections

Voici une liste des meilleures pratiques qui devraient être appliquées lorsque les « upload » de fichiers sont autorisés sur les sites Web et les applications Web. Ces pratiques aideront à sécuriser les fichiers « uploader » utilisés dans les applications Web :

* Définir un fichier « .htaccess » qui autorise uniquement l'accès aux fichiers avec des extensions autorisées.
* Ne placez pas le fichier « .htaccess » dans le même répertoire où les fichiers « uploader » seront stockés, placez-le dans le répertoire parent. De cette façon, le fichier « .htaccess » ne peut jamais être écrasé par un attaquant.
* Généralement, le fichier « .htaccess » devrait autoriser seulement les fichiers qui ont l’extension gif, jpg, jpeg et png. Le code qui va suivre permet d’éviter l’ « upload » de fichier à double extension :

**deny from all**

**<Files ~ “^w+.(gif|jpe?g|png)$”>**

**order deny,allow**

**allow from all**

**</Files>**

* Si possible, « uploader » les fichiers dans un répertoire en dehors de la racine du serveur.
* Ne comptez pas uniquement sur la validation côté client, car ce n'est pas suffisant. Idéalement, la validation côté serveur et côté client devrait être implémentée.

### Notre solution

Blabla