Rapport d’audit ICT-183



David Dieperink, Stefan Petrovic – CID3A

CFPV

Table des matières

[1 INtroduction 3](#_Toc117592773)

[2 authentification 3](#_Toc117592774)

[2.1 Description 3](#_Toc117592775)

[2.2 Eléments audités 3](#_Toc117592776)

[2.3 Corrections à apporter 4](#_Toc117592777)

[3 xSS 5](#_Toc117592778)

[3.1 Description 5](#_Toc117592779)

[3.2 Eléments audités 5](#_Toc117592780)

[3.3 Corrections à apporter 5](#_Toc117592781)

[4 CSRF 6](#_Toc117592782)

[4.1 Description 6](#_Toc117592783)

[4.2 Eléments audités 6](#_Toc117592784)

[4.3 Corrections à apporter 6](#_Toc117592785)

[5 injection sql 7](#_Toc117592786)

[5.1 Description 7](#_Toc117592787)

[5.2 Eléments audités 7](#_Toc117592788)

[5.3 Corrections à apporter 7](#_Toc117592789)

[6 Protection des informations 8](#_Toc117592790)

[6.1 Description 8](#_Toc117592791)

[6.2 Eléments audités 8](#_Toc117592792)

[6.3 Corrections à apporter 8](#_Toc117592793)

# INtroduction

Ce document regroupe les différentes failles de sécurités trouvées sur le site d’e-commerce. Il décrit les failles de sécurité, explique leur fonctionnement et décrit différentes corrections mises en place avec leurs avantage et désavantages.

# authentification

## Description

L’authentification permet à un utilisateur de prouver son identité au site. Cela lui permet d’avoir des droits et des accès à des données du site.

## Eléments audités

Voici les fonctions utilisées dans l’application pour l’authentification :

Figure



Figure

Une image contenant texte

Description générée automatiquement

1. ***Figure 1 :*** Un utilisateur est connecté à l’application quand il est trouvé directement dans la base de données en faisant une condition qui prend en compte le nom d’utilisateur et le mot de passe.

* Il n’y a pas de vérification du mot de passe avec un sel, cela crée des failles. Une Rainbow table peut être utilisé.
* Une vérification de la longueur du mot de passe n’existe pas, donc des **mots de passe par défaut** peuvent être utilisés (ex : admin, root).

1. ***Figure 2*** : La fonction utilisée pour effectuer la requête des informations de l’utilisateur dans la base de données fait un hachage avec le **MD5** mais ne prend en compte aucun sel.

## Corrections à apporter

* Une vérification plus complète peut être effectuée en vérifiant si l’utilisateur existe en faisant une condition avec son nom d’utilisateur dans la requête SQL (fonction **findOne**) puis en utilisant la fonction PHP **password\_verify** qui vérifie le hachage d’un mot de passe avec un sel. Cela permet de contourner la Rainbow table.

Une image contenant texte

Description générée automatiquement

* Une vérification sur la longueur du mot de passe doit également être implémentée pour éviter les mots de passe par défaut.

Une image contenant texte

Description générée automatiquement

* Pour contourner une attaque de **force brute**, la fonction PHP **sleep()** peut être utilisé pour mettre un délai lors de chaque tentative de connexion.



* Pour forcer HTTPS dans le serveur, un fichier **.htaccess** peut être ajouté dans la racine de l’application avec le contenu suivant :

Une image contenant texte

Description générée automatiquement

# xSS

## Description

XSS veut dire Cross-Site-Scripting. Une attaque XSS consiste à insérer un code malveillant dans un champ de formulaire par exemple. Si un code malveillant est inséré dans un champ de formulaire, le site va exécuter le code.

## Eléments audités

Le site possède plusieurs formulaires. Ces formulaires sont sensibles aux attaques XSS. Lorsque cette ligne (<script>alert(‘XSS’)</script>) est rentrée dans un champ de formulaire et que le formulaire est envoyé le script s’exécutera.

## Corrections à apporter

* Pour éviter que cela se produise, une des solutions est de filtrer les informations reçues lors de l’envoi du formulaire. Si les informations reçues ne sont pas conformes à nos attente, l’envoi du formulaire est refusé.

Une image contenant texte

Description générée automatiquement

# CSRF

## Description

CSRF veut dire Cross-Site request forgery. Une attaque CSRF consiste à prendre le contrôle d’une session autorisée par l’utilisateur et grâce à cette session, les attaquants peuvent exécuter des actions malveillantes. Cette attaque par le biais de requête HTTP.

## Eléments audités

Le site possède plusieurs formulaires qui sont sensible. Aucun champ ne permet réellement de prouver que c’est la bonne personne qui rentre les informations et qui exécute les requêtes HTTPS.

## Corrections à apporter

* Pour éviter que cela se produise, une des solutions est d’utiliser un framework comme Laravel qui prend en charge automatiquement les attaque CSRF. Il existe également une autre option, celle-ci consiste à générer un token aléatoire avec un délai d’expiration.

Une image contenant texte

Description générée automatiquement

# injection sql

## Description

Une injection SQL est un type d’attaque assez courant. Cette attaque consiste à faire passer une requête SQL dans un champ de formulaire. Par exemple dans un formulaire de connexion, cela permet de bypass l’authentification si le formulaire est malm protégé.

## Eléments audités

Dans plusieurs formulaires du site, les champs n’étaient pas vérifiés donc les injection SQL passaient. Ces formulaires sont celui du login, de l’insertion d’un article et de l’update d’un article.

## Corrections à apporter

* Pour éviter que des injections SQL se produisent, pour la vérification du login nous allons check si les informations reçues contiennent des simple guillemets « ‘’ ». Si le champ « login » et le champ « password » ne contiennent pas de simples guillemets, la personne arrive à se connecter.

Une image contenant texte

Description générée automatiquement

* Nous effectuons la même vérification sur le formulaire d’insertion des articles. On vérifie que les champs « name », « description », « prix » et « quantité » ne possède pas de simples guillemets.



# Protection des informations

## Description

Les informations que possède un site web sont très peut sécuriser, par exemple les images, les fichiers que possède le site, etc. Les images sont très peu sécurisées car avec un simple screenshot l’image peut être volée.

## Eléments audités

Les images ne possèdent pas de filigrane (watermark en anglais), ce qui permet à des utilisateurs mal intentionnés de potentiellement voler nos images à l’aide de screenshot.

De plus certain formulaire ne sont pas immuniser contre les upload de fichier mal veillant. Apache exécute tous les fichiers qui possèdent l’extension « .php ». Donc si une image s’appelle « image.php.png » Apache va exécuter le code php que possède l’image.

Il y’a également un autre problème dans la page de contact, l’adresse mail est écrite en dur, cela permet à des scrappeur web de récupérer l’adresse mail et d’envoyer des spam.

## Corrections à apporter

* Tout d’abord il faut mettre un filigrane sur nos images. Cela se fait à l’aide d’un fichier PHP qui génère du texte et qui le met sur l’image de base. On récupère l’image, ont défini une couleur pour le texte du filigrane et ensuite ont défini sa position et son texte. Si l’image est valide on l’affiche.

Une image contenant texte

Description générée automatiquement

* Pour l’affichage on doit mettre ce lien, on transmet le lien de l’image au fichier qui va générer le filigrane.

Une image contenant texte

Description générée automatiquement

* Pour l’upload d’image, il faut supprimer le « .php » du nom du fichier, cela permet d’éviter l’exécution de se fichier par Apache. Pour le supprimer, une des manières est la suivante, je remplace le « .php » par une chaîne de caractère vide :

Une image contenant texte

Description générée automatiquement

* Pour contrer les spam mail à cause d’un scrappeur web, il suffit d’utiliser un bouton qui lorsqu’il est appuyé, il affiche l’adresse mail bout par bout grâce à un script JavaScript.

Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

* Une autre solution peut être envisageable, il s’agirait d’implémenter un formulaire de contact qui serait envoyé que lorsque le captcha de vérification est vérifié, cela évite aussi les spam car validé les captchas avec un BOT est compliqué.