Rapport de sécurité dev-web

Louis Arys Martin Perdaens Anh-Emile Pham

26 mai 2020

Table des matières

1 Points nécesssitant une protection

1.1 La base de données

— **L'accès aux données sensibles : les mots de passes et les comptes utilisateurs du site :** Il faut empêcher que des personnes non-autorisées

accèdent à ces informations, car elles leur permettraient de pouvoir s'approprier ou de mofifier le site ou les données personnelles des personnes à qui appartiennent les comptes. Une personne non-autorisée pourrait par exemple supprimer les données du site, ou alors altérer les information d'un utilisateur.

— **L'ajout, la modification ou la suppresion de données dans la base de données :** Il faut empêcher que des personnes non-autorisées puissent altérer les données contenues dans la base de données. Elles sont le coeur du site et sans elles plus rien ne fonctionnera correctement. Donc seuls les personnes privilégiées (administrateur ou développeurs) doivent y avoir accès.
— **l'accès aux données des utilisateurs :** ce sont des données privées, il ne faut donc pas que n'importe qui puisse y avoir accès. Ce genre de données comporte le domicile, le numéro de téléphone ou l'addresse mail des utilisateurs.

2 Vulnérabilités et menaces pour le site

2.1 Buffer Overflow

Lors de l'ajout ou la modification de données dans la base de données, une personne malveillante pourrait rentrer des textes de tailles supérieures à celui attendu par la base de données.

2.2 SQL Injection

Lors de l'ajout, la modification ou la suppresion de données dans la base de données, une personne malveillante pourrait mettre du code SQL comme paramètre.

2.3 Accès à la base de données

Une personne extérieur pourrait tenter d'accéder directementà la base de données, de manière à pouvoir accéder aux données ou les modifier.

2.4 Brutforce

Lors de la connexion d'un utilisateur au site, une personne mal intensionnée pourrait essayer de craquer le mot de passe de l'utilisateur à l'aide d'une attaque Brutforce.

2.5 DDOS

Le site pourrait ne plus fonctionner si une personne mal intentionnée surcharge le serveur de requêtes. Les utilisateurs n'auraient plus accès à aux données de la database, ni à de nouvelles pages web.

3 Risques associés aux menaces

3.1 Buffer Overflow

Dans le cas où l'input serait trop grand, la base de donnée va lancer une erreur, ce qui pourrait faire planter le site. Probabilité plutôt élevée car plusieurs requêtes de l'API sont des requêtes permettant de faire des inputs dans la base de données.

3.2 SQL Injection

Permettrait de récupérer des informations pouvant être sensible, et peut être confidentielle dans la base de données, comme par exemple l'id d'un utilisateur, sans devoir donner son mot de passe. La probabilité de ce type d'attaque est assez élevée, car plusieurs requêtes de l'api permettrait de faire ce genre d'attaque.

3.3 Brutforce

Permettrait d'obtenir le mot de passe d'un utilisateur ayant des permissions d'administrations, et ainsi de pouvoir altérer/modifier/insérer des données corrompues sur le site et dans la base de données. Permettrait aussi de récupérer des données sensibles. La probabilité de ce type d'attaque est élevée, car le site possède un système de login, pour accéder à une interface de gestion de la base de données.

3.4 DDOS

Pourrait rendre le serveur complètement inutile, ou provoquer de gros ralentissements de celui-ci. La probabilité de ce type d'attaque est assez élevée, car le serveur est en ligne, et est donc vulnérable à ce type d'attaque d'internet.

4 Classement des menaces

1. Brutforce
2. DDOS
3. Buffer Overflow
4. SQL Injection

5 Contre-mesures

5.1 Buffer Overflow

Vérifier systématiquement la taille des inputs, pour être sûr qu'ils correspondent bien à ce qui est attendu. En cas de problème renvoyer un message

d'erreur, ou alors ne rien faire.

5.2 SQL Injection

Utiliser le paramétrage plutôt que la concaténation de string lors du traitement des requêtes SQL sur le serveur. Le paramétrage permet de passer les paramètres et la requête séparément à la base de données, ce qui permet d'éviter que la requête soit mal interprétée.

5.3 Brutforce

Utiliser des mots de passes complexes, avec de longueurs supérieurs à 8, utilisant des chiffres, caractères et symboles. Ne surtout pas utiliser de mots du dictionnaire. De plus, bloquer l'accès au site lorsqu'un utilisateur essayer plus d'un certains nombre de fois d'accéder au site.

Le plugin express-brute est un module express permettant de mettre en place une protection contre le Brutforce.

5.4 DDOS

Limiter le nombre de connections/requêtes permisent pour un utilisateur à un certains nombre par minute/seconde.

Le module express-limit-rate permet d'avoir une protection contre de trop nombreuses requêtes.

6 Cadre Budgétaire

Budget nul, ce projet est fait en bénévola.