Projet 1 : Vulnérabilités web
IPL I317B Sécurité : labo

Olivier Choquet & Thibault Vanwersch

Date de remise : 7 novembre 2023 à 23H55

Objectif

Le but de ce projet est la mise en pratique des connaissances acquises en cours de labo sécurité : injection SQL. Vous devez réfléchir, faire des déductions et vous adaptez au fonctionnement interne du site internet que vous attaquez

Cible

Votre cible est un petit site web basique permettant de créer et gérer un petit wiki markdown :

https://labosecuipl.alwaysdata.net/23/yawiki/

Règles d'engagement

Le but de ce projet est de tester votre capacité à faire des injections SQL. Vous ne pouvez donc pas :

- ddos le site,
- faire du spam (ex: créer un nombre important de comptes ou de pages sur le site),
- utiliser des outils automatisés de scan (ex: sqlmap)
- ou mener tout autre type d'opérations destructives (ex: DROP, DROP cascade),…
- attaquer le système de connexion du site (çàd : la création de compte, le login, logout et le système de modification du mot de passe).
  Le système de connexion n'a pas vocation a être attaqué, il est là pour vous permettre de travailler dans des environnements séparés sans vous entraver les uns les autres.

Mise en œuvre

1. **Créez un compte sur le site**
   Vous n'avez besoin de créer qu'un seul compte pour ce projet. Utilisez un nom d'utilisateur explicite que vous mentionnerez dans votre rapport. Pour éviter que vos manipulations n'influent le projet d'autres étudiants, les comptes ont des bases de données indépendantes les uns des autres. Si vous créez deux comptes, ils n'auront pas accès l'un à l'autre.
   NB: Le formulaire de connexion/inscription n'a pas vocation à être attaqué !
2. **Explorez le site**
   Le site dispose de fonctionnalités simples. Familiarisez-vous avec elles et leurs fonctionnements. Cela sera utile pour produire l'inventaire des points d'interactions client-serveur demandé dans le rapport.
3. **Trouvez et exploitez la faille**

   Le site dispose d'au moins une vulnérabilité permettant des injections SQL.
   1. Trouvez où et comment faire l'injection
   2. Récupérer la liste des tables de la base de données
   3. Utilisez là pour récupérer l'id unique et le contenu des pages de votre cible[1]
   4. Récupérer la liste des utilisateurs et le hash de leur mot de passe
4. **Rédigez un rapport**

Rapport

Pour ce projet, vous devez remettre un rapport sur moodle sous la forme d'un document ODT ou d'un pdf. Si vous souhaitez placer plusieurs fichiers dans une archive, utilisez le format ZIP. Votre rapport doit contenir au moins l'information suivante :

- Votre login utilisateur.
- Un inventaire des points d'interactions client-serveur dans lequel vous reprendrez **toutes** les interactions possible avec le serveur.
  Pour clarifier les informations demandées, voici un exemple avec les fonctionnalités de login/logout :

Type de requête	**Path**	**Données soumises**	**Réponse**	**Description / vue par l'utilisateur**	**Injection possible (oui/non)**
		Qu'est-ce qui est envoyer vers le serveur ? Ex : des données postées par un formulaire ou des arguments dans l'url	*Note : parfois la réponse est formel (Ex : un json, des données précises,...) parfois c'est juste une réaction du site.*	*Une vue haut niveau de la fonctionnalité, où l'utilisateur clique ou quand le comportement du site a lieu.*	*Juste un oui/non, les détails au point suivant.*
POST	https://labosecuipl.alwaysdata.net/23/yawiki/	Login=<mon login>&password=<mon password>&type=login	Une 304 redirige vers la même page sur la quelle apparaît le contenu du site.	Le formulaire de connexion du site permet de s'authentifier.	Non

1 Un utilisateur cible est pré-généré et affiché sur la page d'accueil de votre wiki.

POST	https://labosecuipl.alwaysdata.net/23/yawiki/	type=logout	La session est invalidé et une 304 redirige vers la même page qui présente une page de connexion.	L'utilisateur peut se déconnecté en cliquant sur le bouton «logout » en haut à droite.	Non

- Les données extraites de la base de données.
- Pour chaque point d'injection mentionné dans l'inventaire comme étant injectable, vous préciserez dans votre rapport :
  - la manière de reproduire l'injection (quoi injecter, où et comment). Vous pouvez joindre du code pour illustrer ce point.
  - Pour l'injection SQL, quel est le code SQL supposé présent sur le serveur pour supporter l'usage normal de cette interaction ? Comment votre injection s'inclut-elle dans celui-ci ?
  - Quelles sont les risques de cette injection ?

Notes :

- Outre le compte cible, votre page d'accueil contient un utilisateur de test et son mot de passe. Ce compte se trouve dans la même instance que votre compte utilisateur.
- Si vous n'arrivez pas à trouver les points d'injections n'hésitez pas à en discuter avec les professeurs par e-mail ou le mardi matin pendant les cours pratique. Vous pouvez aussi expliquez en détail dans votre rapport vos différentes tentatives pour montrer votre compréhension de la matière même si vous n'avez pas trouvé une ou plusieurs vulnérabilités.
- N'oubliez pas l'existence de la pair de mot-clé LIMIT et OFFSET : https://www.sqlite.org/lang_select.html#the_limit_clause